Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования Московский физико-технический институт (государственный университет)

МФТИ

60

60-я НАУЧНАЯ КОНФЕРЕНЦИЯ МФТИ

Москва,
Долгопрудный,
Жуковский
2017

ТРУДЫ 60-Й ВСЕРОССИЙСКОЙ НАУЧНОЙ КОНФЕРЕНЦИИ МФТИ

20-26 ноября 2017 года

Радиотехника и компьютерные технологии

Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)»

Труды
60-й Всероссийской научной конференции МФТИ

20 - 26 ноября 2017 года

Радиотехника и компьютерные технологии

Москва Долгопрудный Жуковский
МФТИ
2017

УДК 621.396+004
ББК 32.84+32.973
Т78

Т78 **Труды 60-й Всероссийской научной конференции МФТИ.**
20–26 ноября 2017 г. Радиотехника и компьютерные технологии. -
М.: МФТИ, 2017. - 198 с.
ISBN 978-5-7417-0648-0

Включены результаты оригинальных исследований студентов, аспирантов, преподавателей и научных сотрудников МФТИ и дружественных учебных и научных организаций. Статьи представляют интерес для специалистов, работающих в области радиотехники и компьютерных технологий

УДК 621.396+004
ББК 32.84+32.973

ISBN 978-5-7417-0648-0

Оглавление

Программный комитет конференции

Н.Н. Кудрявцев, ректор МФТИ – председатель

В.А. Баган, директор по развитию – заместитель председателя

А.А. Воронов, проректор по учебной работе и довузовской подготовке

А.В. Дворкович, директор ФРКТ

В.В. Киселев, директор ФФПФ

С.С. Негодяев, директор ФАКТ

В.В. Иванов, директор ФЭФМ

А.М. Райгородский, директор ФПМИ

С.В. Леонов, директор ФБМФ

П.К. Кашкаров, директор ИНБИКСТ

Организационный комитет конференции

М.В. Милов, руководитель направления «Образование» ЦУП – председатель

С.О. Русскин, представитель ФРКТ

Е.Ю. Чиркина, представитель ФФПФ

Ю.О. Алексеева, представитель ФАКТ

В.Б. Макарова, представитель ФАКТ

В.А. Яворский, представитель ФЭФМ

С.А. Зайцев, представитель ФЭФМ

Е.Г. Молчанов, представитель ФПМИ

В.Н. Логинов, представитель ФПМИ

К.А. Коньков, представитель ФПМИ

К.И. Агладзе, представитель ФБМФ

В.Г. Орлов, представитель ИНБИКСТ

М.В. Костелева, представитель УНЦ ГСН

А.С. Гупаисова, начальник пресс-службы

Е.Д. Жебрак, директор аналитического центра

Секция микропроцессорных технологий и высокопроизводительных вычислительных систем

УДК 004.41

Использование технологии аппаратной поддержки вложенной виртуализации для ускорения сценариев моделирования гипервизоров

Е.А. Юлюгин, Г.С. Речистов

Intel Corporation

Моделирование — важнейшая часть процесса производства вычислительных систем, позволяющая начать разработку программного обеспечения задолго до производства аппаратуры, тем самым существенно сокращая время, необходимое для выхода конечного продукта на рынок. Для того чтобы быть применимой для отладки сложных сценариев, таких как загрузка гипервизоров, модель должна демонстрировать высокую скорость работы. Если целевая архитектура совпадает с хозяйской, то необходимая производительность может быть достигнута через прямое исполнение, которое в случае архитектуры Intel® 64 может быть реализовано с помощью технологии аппаратной поддержки виртуализации Intel VT-x [1].

Загрузка гипервизоров, таких как VMware ESXi, KVM, а также виртуальных машин, запущенных под их управлением, является практически важным классом сценариев программного моделирования. Задача поддержания таких сценариев может быть сформулирована как задача о вложенной виртуализации (англ. nested virtualization) [2], так как программная модель сама по себе является виртуальной машиной. Наиболее частыми операциями, совершаемыми любым гипервизором, моделирующим архитектуру Intel 64, являются манипуляции со структурой VMCS (Virtual Machine Control Structure) [1]. Данная структура контролирует различные аспекты поведения процессора в режиме прямого исполнения VMX non-root, в том числе определяя события, которые должны быть перехвачены монитором виртуальных машин. Обращения к этой структуре возможны с помощью двух инструкций VMREAD и VMWRITE, которые изначально рассматривались как служебные (англ. sensitive) согласно классификации Попека — Голдбера [3]. То есть при попытке выполнения данных инструкций в режиме прямого исполнения происходит передача управления гипервизору (VM exit), который моделирует их поведение. Данные переключения являются медленными, и важной задачей является минимизация их количества.

При исследовании производительности сценариев загрузки VMware ESXi и KVM под управлением симулятора Wind River® Simics® [4] было обнаружено, что доля выходов из режима прямого исполнения из-за инструкций VMREAD/VMWRITE составляет 58% и 40% соответственно. В процессорах четвертого поколения Intel Core™ была добавлена функциональность, направленная на увеличение производительности сценариев вложенной виртуализации — технология теневых VMCS (англ. shadow VMCS). Задача данной работы состоит в разработке алгоритма прямого исполнения инструкций VMREAD и VMWRITE, использующего данную технологию. При разработке алгоритма следует учитывать, что Simics — программный симулятор, задачей которого является моделирование отсутствующих на рынке вычислительных систем. Поэтому следующие условия должны быть учтены.

1. Расположение полей структуры VMCS в памяти моделируемого процессора может отличаться от хозяйской. По этой причине прямое отображение гостевой VMCS на хозяйскую невозможно.

2. Набор полей структуры VMCS моделируемого процессора может отличаться от хозяйского. Некоторые поля могут быть недоступны в гостевой системе, другие могут отсутствовать в хозяйской. Прямой доступ должен быть разрешен только к полям, существующим в обеих структурах. Предполагается, что если поле присутствует в обеих структурах VMCS, то оно имеет одинаковую кодировку, ширину и свойства. Единственный параметр, который может отличаться, — смещение от начала структуры.

Процессор, поддерживающий теневые структуры VMCS, использует два региона памяти размером 4 кбайт каждый в качестве битовых карт для управления поведением инструкций VMREAD и VMWRITE в режиме VMX non-root. Каждое поле структуры VMCS связано с одним битом карты. Если бит, соответствующий определенному полю структуры VMCS, выставлен, то попытка доступа к нему приводит к VM exit. Иначе исполнение происходит без прерываний.

Для обеспечения корректной работы необходимо гарантировать, что результат исполнения инструкций VMREAD и VMWRITE не зависит от режима моделирования. Для этого необходимо орагнизовать синхронизацию структуры VMCS между режимами прямого исполнения и программного моделирования. Это было сделано через массив, содержащий все поля структуры, доступ к которым возможен из обоих режимов. Каждый элемент массива содержит индекс поля, его значение, а также дополнительные флаги. Порядок полей в массиве не имеет значения. При переключении в режим прямого исполнения необходимо заполнить этот массив, если моделируемый процессор находится в режиме гипервизора VMX root. Значения полей массива затем используется для обновления значений полей теневой структуры VMCS. При переходе в режим программного моделирования необходимо аналогично заполнить массив, основываясь на значениях полей теневой структуры VMCS хозяйской системы.

При прямом исполнении VMREAD и VMWRITE используется следующий алгоритм.

1. Перед входом в режим VMX non-root теневая структура VMCS обновляется в соответствии со значениями в синхронизационном массиве. Все поля, содержащиеся в массиве, помечаются как доступные для чтения и недоступные для записи в битовых картах.
2. При первой попытке записи в некоторое поле гостевой структуры VMCS происходит VM exit, обработчик которого проверяет возможность прямых обращений к данному полю. Если прямой доступ к заданному полю невозможен, то происходит переход в режим программного моделирования. В противном случае это поле помечается разрешенным для записи в битовой карте, а также измененным в массиве гостевых полей структуры VMCS. После чего происходит переход в режим прямого исполнения. Все дальнейшие обращения к запрошенному полю будут происходить без прерывания режима прямого исполнения.
3. При переходе в режим программного исполнения все поля гостевой контрольной структуры, помеченные как измененные, должны быть обновлены в соответствии со значениями в теневой VMCS.

Исследование производительности проводились на рабочей станции Lenovo ThinkPad T540p, 8 GB RAM, Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz. Управление энергопотреблением было отключено для обеспечения постоянной частоты работы процессора. Результаты измерений производительности симулятора Simics при моделировании загрузки гипервизоров (стадия 1) и виртуальных машин под их управлением (стадия 2) приведены на рис. 1.

В текущей реализации первая запись в некоторое поле структуры VMCS всегда вызывает выход из режима прямого исполнения. При этом первый доступ зачастую является и последним в текущем цикле прямого исполнения. Это приводит к большому количеству выходов, вызванных инструкцией VMWRITE. Дальнейшая работа над поставленной задачей должна состоять в улучшении протокола синхронизации состояния структуры VMCS между режимами программного моделирования и прямого исполнения

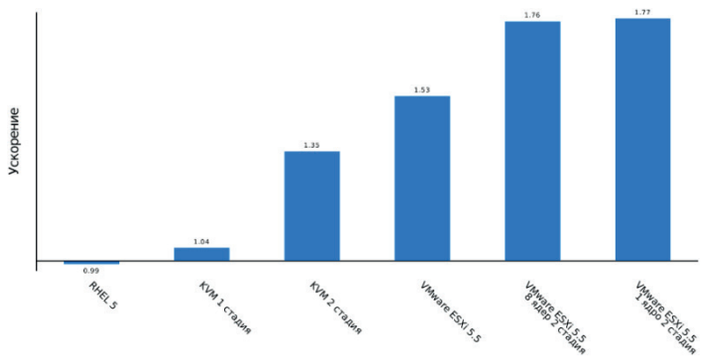


Рис. 1. Ускорение, полученное за счет прямого исполнения обращений к структуре VMCS

Литература

1. Intel® 64 and IA-32 Architectures Software Developer's Manual, Intel Corporation, 2017.
2. *Muli Ben-Yehuda* [*et al.*]. The Turtles Project: Design and Implementation of Nested Virtualization // 9th USENIX Symposium on Operating Systems Design and Implementation. 2010. P. 423 – 436.
3. *Popek G.J., Goldberg R.P.* Formal requirements for virtualizable third generation architectures// Communications of the ACM. 1974.
4. *Aarno D., Engblom J.* Software and System Development using Virtual Platforms – Full System Simulation with Wind River Simics. Morgan Kaufmann Publishers. 2014.

УДК 004.052.3

Тестирование высокоскоростных интерфейсов передачи данных и оптимизация их настроек

И.Е. Билялетдинов[1], А.Е. Ометов[2], Л.С. Тимин[1,2]

[1]ОАО «Институт электронных управляющих машин им. И.С. Брука»
[2]ЗАО «МЦСТ»

В современных процессорах семейства «Эльбрус» используются высокоскоростные каналы передачи данных – каналы памяти DDR3/ DDR4 и каналы межпроцессорных связей и ввода-вывода, реализованные на базе физического уровня PCI Express.

Физический уровень каналов памяти имеет большое число различных настроек и параметров, это и сопротивления (например, выходные сопротивления сигналов), и настройки временных характеристик, и параметры внутренних блоков и механизмов.

Один из наиболее применяемых способов, позволяющих выяснить качество выбранных настроек, заключается в том, чтобы запустить длительный прогон на нескольких вычислительных комплексах. Другой – в том, чтобы, используя очень точный осциллограф, следить за изменениями сигналов и их параметрами. Однако при реализации в оптимальном варианте оба они требуют большого количества дополнительного оборудования и временных затрат. Если же проводить настройки неоптимальным образом, то с большой вероятностью может снизиться надежность вычислительного комплекса (возрастает вероятность сбоя) или скорость его работы (для обеспечения надежности снижается частота).

Для решения задачи следует обзавестись численной характеристикой настройки, которая будет отражать работоспособность канала и которую можно получить быстро. Такой характеристикой является ширина области работоспособности [1] на глазковой диаграмме для шины данных DDR3/DDR4.

С целью определения ширины глаза без помощи осциллографа авторами предлагается перемещать точку захвата данных. При сдвиге за границы глаза система окажется неработоспособной, что позволит найти эту границу. Захват данных в системе памяти DDR происходит по фронту строба DQS. Внутри физического уровня канала памяти есть несколько управляемых блоков задержек BDL и LCDL сигналов строба DQS.

Начальные значения задержек выставляются во время процедуры инициализации физического уровня памяти внутренними механизмами подстройки, однако они доступны для чтения и записи пользователю. При этом управлять задержками можно отдельно для каждого байта и отдельно для режимов чтения и записи (при процессорном чтении данными и стробом управляет модуль памяти, а при записи – процессор). Алгоритм определения окна работоспособности следующий.

1. Установка начальной задержки.
2. Увеличение задержки.
3. Запуск теста, определяющего работоспособность.
4. Если тест прошел успешно, то следует далее увеличивать задержку и запускать тест.
5. Если тест завершился с ошибкой, то строб вышел из зоны работоспособности, следует запомнить последнюю рабочую задержку – это правая граница окна работоспособности.
6. Установка начальной задержки, ее уменьшение.
7. Запуск теста, определяющего работоспособность.
8. Если тест прошел успешно, то следует дальше уменьшать задержку и запускать тест.
9. Если тест завершился с ошибкой, то строб вышел из зоны работоспособности, следует запомнить последнюю рабочую задержку – это левая граница окна работоспособности.
10. Установка начальной задержки.

Отдельное управление задержкой позволяет определять окна работоспособности для каждого байта и каждого режима отдельно, что, в свою очередь, дает возможность оценить возможный технологический разброс характеристик каналов памяти.

В качестве теста на работоспособность можно использовать широкий набор тестов, однако для сокращения времени исполнения разумно использовать внутренние механизмы физического уровня памяти [2]. Таких механизмов два: встроенное самотестирование (BIST) и встроенный модуль управления (DCU).

Механизм встроенного самотестирования позволяет записывать псевдослучайный код в память по программируемым адресам. Недостатком является возможно тестировать только один байт памяти. С одной стороны, это позволит снимать характеристики для каждого байта, с другой – исключается влияние соседних байтов друг на друга и уменьшаются шумы в системе питания, которые могут повлиять на работоспособность вычислительного комплекса в дальнейшем.

Внутри физического уровня памяти также находился внутренний командный модуль, который позволяет управлять памятью в обход контроллера памяти. Он может исполнять все внутренние команды памяти (в том числе команды управления) и настройки модуля памяти, однако есть ограничения, обусловленные размерами кэшей управления: всего можно исполнить 16 команд. Также к недостаткам можно отнести относительно длительное заполнение кэшей и трудность программирования на языке памяти (например, простая запись одного значения занимает четыре команды из 16 доступных). Преимущество командного модуля относительно встроенного механизма самотестирования только одно – возможность управлять всеми байтами одновременно.

Связи в вычислительных комплексах на базе микропроцессоров семейства «Эльбрус» реализованы на основе физического уровня PCI Express. Каждый микропроцессор соединен с каждым четырьмя связями, которые состоят из четырех двунаправленных линий. Пропускная способность этих линий достигает 6 Гб/с, поэтому очень важно правильно подобрать настройки физуровня так, чтобы сигнал не затухал (линии на серверной плате достаточно длинные) и не искажался.

Межпроцессорные связи имеют следующий настраиваемый набор параметров.

1. Выходная амплитуда передатчика.
2. Величина pre-emphasis и equalisation.
3. Пропускная способность канала.

Их правильная настройка необходима для обеспечения повышенной отказоустойчивости комплекса.

С целью проверки корректности набора параметров необходимо провести тестирование линий. Одним из известных решений является стандарт IEEE 1149.6, однако

его методика не позволяет протестировать интерфейс на рабочей частоте, так как частота JTAG не превосходит 10 – 30 МГц [4]. Поэтому для проверки набора параметров следует использовать встроенный механизм самотестирования PCIe [3].

Этот механизм состоит из двух частей: генератора тестовых данных и механизма сравнения. Первый встроен в передатчик и может посылать кодовые последовательности типа PRBS7, PRBS15, PRBS23 и PRBS31, а также пользовательские данные. Механизм сравнения размещен в приемнике и может синхронизоваться с генератором, принимать значения и подсчитывать количество ошибок.

Управление этим механизмом, изменение параметров связей, их инициализация производятся с помощью управляющих регистров, которые доступны с использованием JTAG интерфейса.

Порядок тестирования набора параметров предполагает следующие действия.

1. Выбор набора настроек и инициализацию физического уровня передатчика и приемника с применением этих настроек.
2. Выбор режима работы генератора в передатчике и включение компаратора в приемнике в аналогичном режиме.
3. Синхронизация механизма сравнения с генератором. После этого сбрасывается значение счетчика ошибок и начинается тестирование.
4. Чтение значения счетчика ошибок каждой линии.
5. Выключение генератора и механизма сравнения.
6. Анализ полученных данных, вывод о работоспособности настроек.

В результате на основании данных счетчика ошибок можно определить окно работоспособности межпроцессорной связи, проанализировать работу каждой линии и выбрать наилучшую точку для повышения отказоустойчивости системы.

Литература

1. *Guy Foster*. Anatomy of an Eye Diagram – A Primer. Syn the Sys Research, Inc. 2004. P. 9.
2. *Laung-Tern Wang, Charles E. Stroud, Nur A. Touba*. System-on-Chip Test Architectures: nanometer design for testability. – Burlington: Morgan Kaufmann Publishers. 2008. P. 856.
3. *Laung-Terng Wang, Cheng-Wen Wu, Xiaoqing Wen*. VLSI Test Principles and Architectures: Design for Testability. – San Francisco: Morgan Kaufmann Publishers. 2006. P. 777.
4. IEEE Std 1149.1-2001: IEEE Standard Test Access Port and Boundary-Scan Architecture. – New York: Institute of Electrical and Electronics Engineers, 2001. P. 208.

УДК 004.056.53

Фильтрация сетевых пакетов на основе мандатных меток в операционной системе «Эльбрус»

А.А. Имкенов

Московский физико-технический институт (государственный университет)
АО «МЦСТ»

Обеспечение защищенности информации является одной из важнейших задач при разработке операционной системы. В операционной системе «Эльбрус» применяется мандатное разграничение доступа на действия субъектов над объектами. Всем пользователям (субъектам) и файлам (объектам) назначаются метки (уровни) доступа, например, «несекретно», «секретно», «совершенно секретно». На основе сравнения меток субъекта и объекта принимается решение о предоставлении доступа. Сетевые пакеты, отправляемые процессами, наследуют метки этих процессов. Мандатная метка устанавливается в дополнительное поле заголовка IPv4-пакета по стандарту RFC 1108.

В целях защиты информации при межсетевом взаимодействии применяется межсетевой экран (МЭ) – комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в

соответствии с заданными правилами. В ядре операционной системы «Эльбрус» фильтрация сетевых пакетов реализована на основе подсистемы Netfilter [2].

Целью работы являлось исследование и расширение схемы фильтрации сетевых пакетов в системе Netfilter для поддержки мандатных меток сетевых пакетов. Рассмотрена схема фильтрации сетевых пакетов в ядре операционной системы «Эльбрус». Основу работы Netfilter составляют цепочки – упорядоченные наборы правил. Сетевой пакет, принятый/отправленный системой, последовательно проходит серию цепочек. Правила состоят из критериев и действий. Если сетевой пакет удовлетворяет критерию правила, к нему будет применено соответствующее действие [1].

В схеме фильтрации применяются 3 цепочки: INPUT – входящие пакеты, FORWARD – исходящие пакеты, OUTPUT – исходящие пакеты. (рисунок 1).

В качестве критериев выступают поля заголовков сетевых пакетов: адрес отправителя/получателя, номер сетевого интерфейса, тип транспортного протокола и др. Допустимыми действиями являются ACCEPT – принять пакет и DROP – отклонить пакет [1].

Результатом работы стало создание модуля ядра xt_LABEL, предназначенного для фильтрации сетевого трафика по мандатным меткам. Модуль xt_LABEL осуществляет разбор заголовков сетевых пакетов в цепочках INPUT, FORWARD и OUTPUT для выделения мандатной метки (Рисунок 2). На основе сравнения этой метки и метки хоста, которому предназначается пакет, принимается решение о принятии либо блокировке.

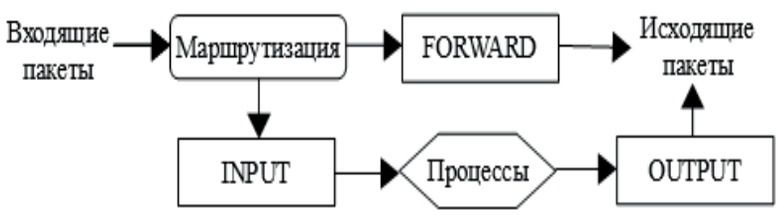


Рис. 1. Схема фильтрации Netfilter

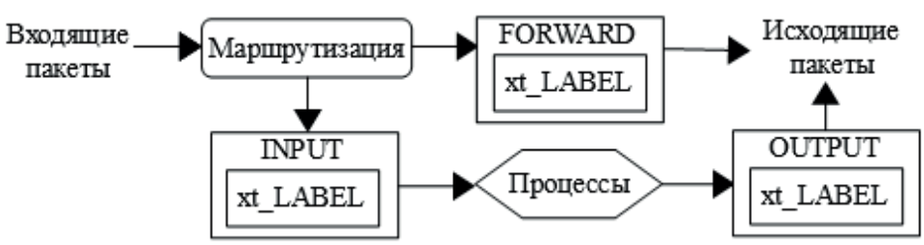


Рис. 2. Разработанная схема фильтрации

Литература

1. *Engelhardt J., Bouliane N*. Writing Netfilter modules. Netfilter Core Team, 2012.
2. *Russel R., Welte H.* Linux netfilter hacking. Netfilter Core Team, 2012.

УДК 004.454

Развитие поддержки формата Device Tree в ОС «Эльбрус»

И.В. Прусов, А. А. Мухин

ЗАО «МЦСТ»

В вычислительных комплексах (ВК), выпускаемых АО «МЦСТ», используются устройства, которые подключаются шинами I2C и SPI, повсеместно внедренными в мировой проектной практике. Примерами являются температурные датчики, контроллеры GPIO, часы реального времени и ряд других функциональных абонентов ВК.

Одной из существенных проблем построения систем на этих шинах является инициализация подключаемых устройств, требующая данных об адресах и параметрах. До недавнего времени в ОС «Эльбрус» для регистрации устройств на шинах I2C и SPI была частично реализована поддержка формата Device Tree, позволяющего хранить информацию об устройствах, которые не могут быть обнаружены автоматически во время загрузки ВК. Этот формат позволяет по определённым правилам составить текстовое описание устройств, допускающая преобразование в двоичное представление – Device Tree Blob (DTB) [1]. Ядро Linux содержит функции для работы с описанием в виде DTB и позволяет использовать его с целью получения информации об устройствах.

Существующая реализация обладала определёнными недостатками, ухудшающими гибкость и переносимость решения. Загрузка описания из ПЗУ производилась ядром по фиксированному адресу, разбор описания и регистрация I2C- и SPI-устройств выполнялась в драйверах соответствующих контроллеров, а для архитектуры SPARC на старых версиях ядра подсистема, работающая с Device Tree, использовала дерево структур tree_entry, объявленных в исходном коде вместо разбора описания.

Для решения проблемы с фиксированным адресом чтением описания устройств авторами было принято решение выполнять чтение DTB файла из ПЗУ в программе начальной загрузки ВК и передавать ядру указатель на уже загруженное описание в оперативной памяти. Это позволяет более рационально использовать ПЗУ и избежать проблем при изменении ёмкости ПЗУ на будущих ВК. Правила описания I2C- и SPI-устройств были изменены для того, чтобы соответствовать разрабатываемой спецификации Device Tree[2]. Это позволяет исключить из кода драйверов I2C- и SPI-контроллеров регистрацию устройств, описанных в Device Tree, и использовать для этого встроенные механизмы ядра Linux. Для обеспечения поддержки Device Tree на ВК с процессорами архитектуры SPARC в старые версии ядра были внесены правки, позволяющие динамически строить дерево структур tree_entry на основании описания Device Tree и использовать существующие механизмы работы с этим деревом.

По результатам работы формат описания и механизм Device Tree были успешно использованы для работы ОС «Эльбрус» на ВК с уникальными наборами I2C- и SPI-устройств, что раньше требовало внесения правок в исходный код ядра.

Литература

1. *Gibson D. Herrenschmidt B.* Device trees everywhere. 2008.
2. The Devicetree Specification [Электронный ресурс] URL: http://www.devicetree.org/specifications/ (на 03.10.2017)

УДК 004.4

Способ построения симулятора архитектуры «Эльбрус» с поддержкой функционального и потактового режимов моделирования инструкций

П.А. Порошин[1], А.Н. Мешков[1,2], С.В. Черных[2]

[1]ОАО «Институт электронных управляющих машин им. И.С. Брука»
[2]ЗАО «МЦСТ»

Программные модели вычислительных систем, или симуляторы, являются важным инструментом при разработке аппаратуры, новых микропроцессоров и программного обеспечения для них. При этом разные задачи формируют отличающиеся требования к симулятору: для каких-то задач важна функциональная корректность и скорость моделирования, для других требования к производительности ниже, но необходима возможность получения точной информации о времени исполнения каждой из операций. Первым требованиям удовлетворяют функциональные симуляторы, вторым – потактово-точные (потактовые).

Одновременно разрабатывать и поддерживать два разных симулятора (функциональный и потактовый) очень непросто и трудоемко. Поэтому имеет смысл найти способ, который бы позволил минимизировать дополнительные усилия на поддержку каждого из них. Помимо этого, в случае наличия рабочего функционального симулятора, целесообразно выработать подход к построению потактовой модели с переиспользованием кода функциональной модели.

В данной работе описываются решения, примененные к построению потактового симулятора микропроцессоров семейства «Эльбрус» с архитектурой VLIW [1] на основе существующего функционального симулятора.

Чтобы сократить усилия, необходимые для поддержки обеих моделей, было решено разработать симулятор, способный работать как в функциональном, так и в потактовом режимах. В первом режиме должна обеспечиваться функциональная корректность моделирования и высокая скорость работы, во втором, за счет сниженной производительности, также должны моделироваться задержки между операциями и различные блокировки конвейера. Основная идея совмещения двух режимов заключается в том, что один из них (в данном случае функциональный) реализуется полуавтоматическим способом из другого, более детального режима (потактового). Это и позволяет сократить общий объем работы, так как, в сущности, необходимо вести поддержку только более детального, потактового, режима моделирования.

Особенностью оригинального функционального симулятора является двухстадийное исполнение операций. Каждая операция описана псевдостадиями чтения и записи (рис. 1а), напрямую не связанными с конвейерными стадиями процессора и реализованными как функции. Это упрощает реализацию прерываний при исполнении широкой команды и других особенностей архитектуры «Эльбрус». Потактовая модель разработана на основе оригинального функционального симулятора главным образом путем уточнения и «дробления» псевдостадий операций на стадии, соответствующие моделируемым стадиям конвейера (рис. 1б). Уточненные стадии являются основным описанием поведения операций в новом симуляторе и непосредственно используются при потактовом режиме работы. Для функционального режима работы необходимо восстановить псевдостадии чтения и записи оригинального функционального симулятора, что достигается путем автоматической «склейки» конвейерных стадий в соответствующие им псевдостадии на этапе компиляции (рис. 1в).

Тест производительности нового симулятора, работающего в функциональном режиме, не показал существенного замедления по сравнению оригинальным функциональным симулятором, что позволяет говорить о перспективности выбранного подхода.

Рис. 1. Примеры описания операций с помощью стадий (стадии B, R, E0, E1 – моделируемые потактовым симулятором стадии конвейера)

Литература

1. *Ким А.К., Перекатов В.И., Ермаков С.Г.* Микропроцессоры и вычислительные комплексы семейства «Эльбрус». СПб.: Питер, 2013. 272 с.

УДК 004.451.87

Реализация состояния глубокого сна микропроцессора «Эльбрус-4С» при помощи средств ядра Linux

А.А. Демидов

Московский физико-технический институт (государственный университет)
ЗАО «МЦСТ»

Общепринятый подход к снижению энергопотребления вычислительных комплексов (ВК) сформулирован в стандарте ACPI [1], согласно которому для данного ВК определяется несколько наборов состояния энергосбережения, где C0-Cn — состояния сна для процессорного ядра, одним из которых является состояние глубокого сна. Алгоритм перевода вычислительного ядра в состояние глубокого сна согласно спецификации целевых микропроцессоров «Эльбрус» содержит следующие шаги.

Инвалидацию регистров подготовки перехода (позволяет избежать слабоконтролируемых спекулятивных обращений в память).

Гашение кеш-памятей (требуется из-за невозможности поддержания когерентности памяти отключенного ядра).

Занесение кода отключения ядра в IB (Instruction Buffer) без его исполнения (позволяет избежать слабоконтролируемых спекулятивных обращений в память от незавершенной предподкачки прямой ветви кода).

Отключение ядра (запись в регистр st_core).

Этот алгоритм реализован автором в составе энергосберегающей подсистемы ядра Linux – cpuidle [2], переводящей ядра микропроцессора в различные состояния сна в период простоя процессора (рис. 1). Подсистема включает в себя архитектурнозависимый компонент driver, содержащий функцию e2k_enter_idle(), которая непосредственно переводит ядра микропроцессора в различные состояния сна. При решении поставленной задачи эта функция была модифицирована с целью добавления возможности перевода в (ранее не предусматриваемое) глубокое состояние сна. Политика, позволяющая переводить ядро в оптимальное при данном состоянии процессора состояние сна, определяется компонентом governor, управляя которым через sysfs интерфейс можно собрать статистику вхождений ядер в различные состояния сна или изменить политику перевода.

Эти возможности были введены в модифицированный модуль ядра Linux cpuidle-e2k. Тестирование проводилось на вычислительном комплексе «Эльбрус-401» в течение 30 с, состоянии простоя ВК (idle). При включении модуля наблюдалось снижение

энергопотребления вычислительного комплекса на базе микропроцессора «Эльбрус-4С» с 50.6 Вт до 41.8 Вт (на 17%).

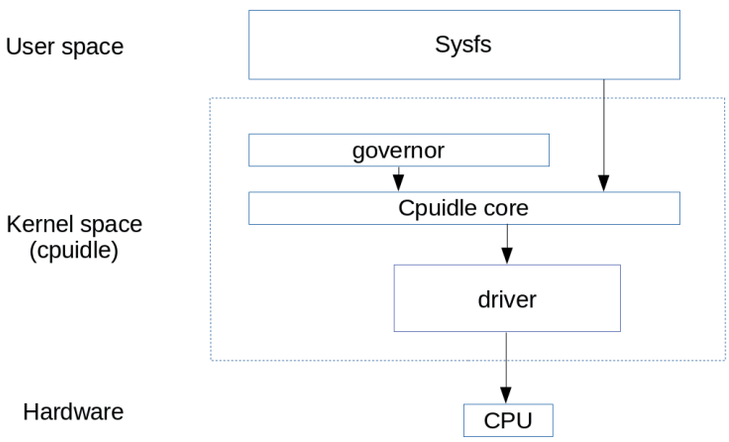


Рис. 1. Структурная схема подсистемы cpuidle

Литература

1. Hewlett-Packard Corporation, Intel Corporation, Microsoft Corporation, Phoenix Technologies Ltd, Toshiba Corporation. Advanced Configuration and Power Interface Specification, Revision 4.0a. 2010.
2. *Venkatesh P., Shaohua L., Belay A.*. «Cpuidle — Do nothing, efficiently … » // Proceeedings of the Linux Symposium. 2007. V. 2. P. 119.

УДК 004.318

Об аппаратной поддержке виртуализации системы прерываний в многоядерных микропроцессорах семейства «Эльбрус»

Р.В. Деменко[1,2], В.Б. Трофимов[2]

[1] Московский физико-технический институт (государственный университет)
[2] ЗАО «МЦСТ»

Рост производительности современных компьютерных платформ и необходимость иметь гибкую инфраструктуру вычислительных средств обуславливают эволюцию технологий виртуализации. Реализация средств аппаратной поддержки виртуализации позволяет получить значительный прирост производительности виртуальных машин. В современных многоядерных микропроцессорах такая аппаратная поддержка реализуется, помимо прочего, для виртуализации операций ввода/вывода и системы прерываний [1], [2]. В данной работе предложены принципы реализации аппаратной поддержки виртуализации системы прерываний МП «Эльбрус», которые являются частью общего подхода к созданию этих средств для архитектуры «Эльбрус» [3] и подразумевают:

- виртуализацию обращения к регистрам контроллера прерываний,
- обеспечение доставки прерываний нужному гостевому ядру.

Обращения к регистрам контроллера прерываний

Как правило, управляющая структура виртуальной машины, включающая состояние системы прерываний (копии регистров контроллера прерываний), хранится в памяти машины. В отсутствие аппаратной поддержки каждое обращение гостевого ядра к регистрам контроллера прерываний перехватывается гипервизором и обрабатывается программно.

Такой перехват для каждого ядра можно не делать, если реализовать дублирующий набор управляющих регистров, который используется гостевым ядром, активным на данном физическом ядре в текущий момент. При постановке гостевого ядра гипервизор

заполняет эти регистры значениями из управляющей структуры. При снятии гостевого ядра значения регистров откачиваются в управляющую структуру.

Доставка прерываний нужному гостевому ядру

Для поддержки многопроцессорной конфигурации контроллер прерываний в МП «Эльбрус» имеет распределенную структуру. Элементы системы прерываний взаимодействуют через аппаратно формируемые сообщения (сообщения о прерываниях, служебные сообщения). Введение гостевого набора регистров приводит к появлению в аппаратуре гостевых сообщений о прерываниях, которые необходимо изолировать как от сообщений хоста, так и от сообщений других гостей. С этой целью сообщения сопровождаются номером гостевой машины, поскольку три параметра <номер гостевой машины, номер гостевого ядра, тип (и вектор) прерывания> позволяют однозначно идентифицировать сообщение.

Чтобы доставить прерывания нужному гостевому ядру, пара <номер гостевой машины, номер гостевого ядра> преобразуется в физический номер ядра (если данное гостевое ядро активно) с использованием аппаратной таблицы соответствия, управляемой гипервизором. Ее состояние должно быть одинаковым во всех процессорах многопроцессорной системы, это свойство гарантируется аппаратной схемой синхронизации, реализованной через служебные сообщения.

В случае, если гостевое ядро неактивно, это прерывание фиксируется в управляющей структуре соответствующей гостевой машины, аппаратно генерируемой атомарной DMA-операцией записи.

При заполнении гостевых регистров во время процедур снятия/постановки гостевого ядра необходимо гарантировать, что уже сформированные сообщения о прерываниях не будет потеряны. Такая потеря может возникнуть вследствие гонок между сообщениями о прерываниях, служебными сообщениями и DMA-операциями, связанными с доставкой прерываний отложенному гостевому ядру. Для исключения ситуаций гонок аппаратура предоставляет системному ПО возможность точно определить момент завершения процесса синхронизации таблиц соответствия и завершения всех соответствующих DMA-операций.

Для прерываний от внешних устройств, отданных под непосредственный контроль гостевой ОС («проброс» устройства в виртуальную машину), стоит проблема определения номера гостевой машины. В самом распространенном случае внешнее прерывание приходит в виде Message Signaled Interrupt (MSI), представляющем собой с точки зрения процессора особый DMA-запрос. Содержащийся в нем виртуальный адрес проходит процедуру трансляции в физический адрес. Применительно к MSI соответствующие поля в таблице трансляции можно использовать для хранения параметров прерывания внешнего устройства, отданного гостевой ОС, в нашем случае — номера гостевой машины.

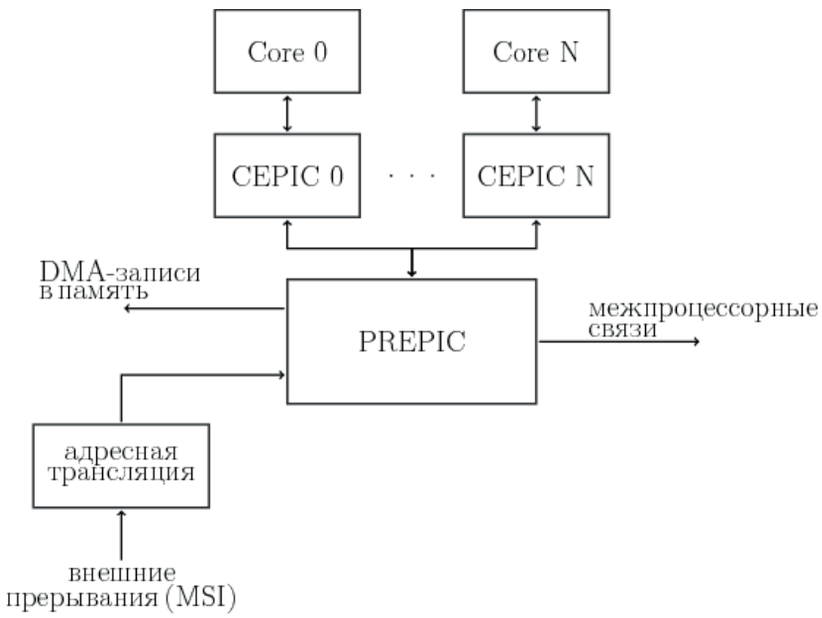


Рис. 1. Упрощенная схема контроллера прерываний (Elbrus Programmable Interrupt Controller, EPIC)

Условные обозначения
Core 0, Core N — ядра микропроцессора,
CEPIC 0, CEPIC N — Core EPIC, локальная для каждого ядра часть контроллера прерываний,
PREPIC — Processor EPIC, общая для процессора часть контроллера прерываний, содержит таблицу соответствия физических и виртуальных ядер.

Литература

1. Intel Virtualization Technology for Directed I/O, Architecture Specification, 2016.
2. ARM Generic Interrupt Controller Architecture Specification. V2.0, 2013.
3. *Знаменский Д.В*. Выбор вариантов реализации средств аппаратной поддержки виртуализации архитектуры «Эльбрус». //Вопросы радиоэлектроники, сер. ЭВТ. 2014. Т. 3.

УДК 004.4'422

Удаление немёртвых процедур, не влияющих на результат программы

В.Е. Шампаров, А.Л. Маркин

ЗАО «МЦСТ»

Одной из задач оптимизирующей компиляции является удаление так называемого мёртвого кода, результаты выполнения которого не используются. Алгоритм выявления и удаления мёртвых инструкций внутри процедуры известен [1] и применяется в популярных оптимизирующих компиляторах [2], [3].

Процедуру назовём мёртвой, если она не содержит побочных эффектов и все операции её вызова также мертвы. Удаление мёртвых процедур выполняется по правилам, аналогичным классическому алгоритму DCE.

В рамках данной работы выявлены такие процедуры, которые работают со статическими объектами, имеющими ограниченную процедурой лексическую область видимости, и не влияют на результат исполнения программы при любых входных данных. Классический метод не позволяет удалять подобные процедуры, так как формально они не мертвы. Поэтому был разработан охарактеризованный ниже алгоритм выявления и удаления немёртвых процедур, не влияющих на результаты программы. Он реализован в рамках компилятора LCC для микропроцессоров семейства «Эльбрус».

Алгоритм предполагает два прохода по представлению программы. В первом проходе каждая процедура преобразуется к виду без возвращаемого значения, если оно не используется после всех вызовов процедуры. Во втором проходе удаляются вызовы всех процедур, соответствующих следующим условиям.

1. На процедуру не был взят адрес.
2. Процедура листовая, иными словами не вызывает других процедур.
3. Процедура не имеет возвращаемого значения.
4. Внутри процедуры нет записей по указателю, volatile чтений и записей.
5. Все записи по имени работают с локальными или статическими объектами процедуры.

Измерение изменения производительности при применении оптимизации проводилось на наборе бенчмарков SPEC CPU2006 [4], причём компиляцию выполнили на машине с архитектурой процессора x86-64 с пиковым набором опций, а исполнение — на машине с архитектурой процессора «Эльбрус». В таблице 1 показаны результаты измерения. В колонках «отношение времён компиляции» и «отношение времён выполнения» показаны отношения времён соответствующей работы без преобразования к времени работы с преобразованием. В порядке строк приводятся только результаты четырёх тестов с наибольшими отклонениями от 1 по скорости компиляции, результаты двух тестов с наибольшими отклонениями от 1 по скорости исполнения и геометрическое среднее от результатов всех тестов.

Данные таблицы 1 показали, что ускорение компиляции достигает 1,18, замедление — 0,83, и при этом доля времени работы алгоритма не превышает 0,5%. Из этого можно сделать вывод, что применение данного алгоритма меняет контекст для применения других оптимизаций.

Для сравнения была выполнена попытка измерить те же отношения на компьютере с архитектурой процессора x86-64 с компилятором gcc версии 7.1.0 с опциями -flto -O3. Установлено, что в ходе LTO оптимизаций этот компилятор не удаляет процедуры, которые были удалены реализованным алгоритмом.

Дальнейшее улучшение алгоритма возможно в следующих направлениях: адаптация алгоритма для сборки в помодульном режиме и добавление анализа нелистовых процедур.

Таблица 1.

Ускорение работы тестов из набора SPEC-2006 (больше 1 – ускорение, меньше 1 – замедление)

Название теста	Отношение времён компиляции	Отношение времён выполнения	Доля времени работы дополнения
400.perlbench	0,91	1,00	0,001%
403.gcc	0,83	1,00	0,06%
444.namd	1,13	1,00	0,005%
462.libquantum	1,03	1,01	0,02%
483.xalancbmk	1,18	1,00	0,4%
433.milc	0,98	0,99	0,01%
Gmean	0,99	1,00	0,02%

Литература

1. *Muchnick S.* Advanced compiler design and implementation. Morgan Kaufman. – San Francisco, 1997. P. 592-593.
2. *Lattner C.* LLVM: An infrastructure for multi-stage optimization. University of Illinois. 2002. P. 26.
3. *Novillo D.* GCC. An Architectural Overview, Current Status and Future Directions // Proceedings of the

Linux Symposium, Tokyo. 2006. P. 185 – 200.
4. http://www.spec.org/ [Электронный ресурс]

УДК 004.94

Оценка перспектив использования вычислительной техники с процессором «Эльбрус-8С» для решения задач робототехнического комплекса

Н.А. Бочаров

ЗАО «МЦСТ»

Микропроцессор (МП) «Эльбрус-8С» относится к пятому поколению VLIW-микропроцессоров с архитектурой «Эльбрус». Пиковая производительность МП «Эльбрус-8С» на операциях с одинарной и двойной точностью составляет 250 и 125 GFLOPS соответственно. Это в пять раз превышает вычислительную мощность ранее выпущенного четырехъядерного МП «Эльбрус-4С», дизайн которого был взят за основу [1].

В рамках общего комплекса работ, проводимых для оценки возможности использования вычислительных средств семейства «Эльбрус» и, в частности микропроцессора «Эльбрус-8С», при создании робототехнических комплексов, решались задачи моделирования движения робота и обработки системы стереозрения [2]. В первой задаче движение робота было сведено к поиску пути на графе и соответственно проведен анализ алгоритмов поиска пути на графе, разработана программа, моделирующая поведение робота во время движения с учетом как характеристик робота, таких как скорость, радиус поворота, радиус обнаружения препятствий, так и параметров местности, таких как проходимость местности и заранее неизвестные препятствия [3]. В ходе решения второй задачи разработана программа для моделирования виртуальной трехмерной среды с использованием набора базовых трехмерных моделей, таких как дерево, куст, холм, трава, человек и т.д. Кроме того, разработана программа, реализующая алгоритм калибровки стереопары с использованием шахматного паттерна, и алгоритм трехмерной реконструкции исходной сцены по паре изображений с правой и левой камер, причем в качестве входных изображений могут использоваться изображения, полученные как с реальной стереопары, так и с помощью разработанной программы моделирования трехмерной среды.

Было проведено сравнительное тестирование разработанных моделей на «Эльбрус-4С», «Эльбрус-8С» и «Intel Core i7 4700». На рис. 1 и 2 соответственно представлены зависимости времени построения графа проходимости и поиска пути роботом от количества узлов в графе. На рис. 3 приведена диаграмма затрат времени на стереореконструкцию по стереопаре изображений размером 640 × 480 px.

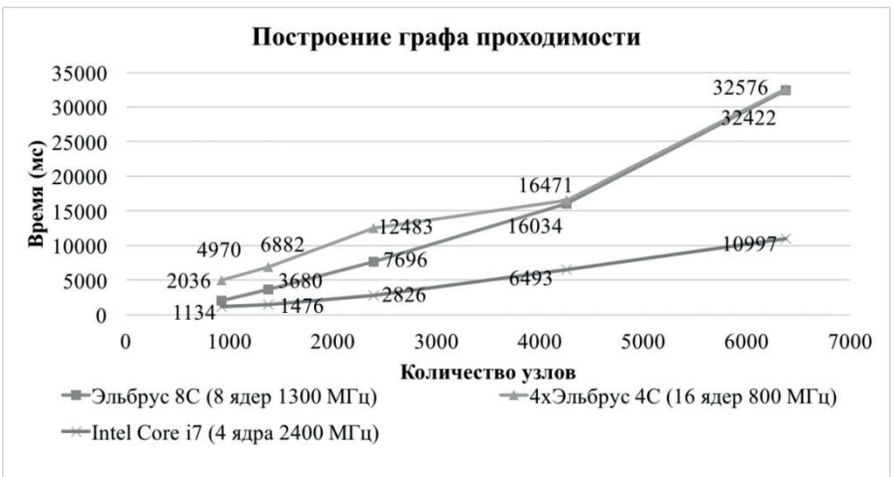


Рис. 1. Зависимость времени построения графа проходимости от количества узлов в графе

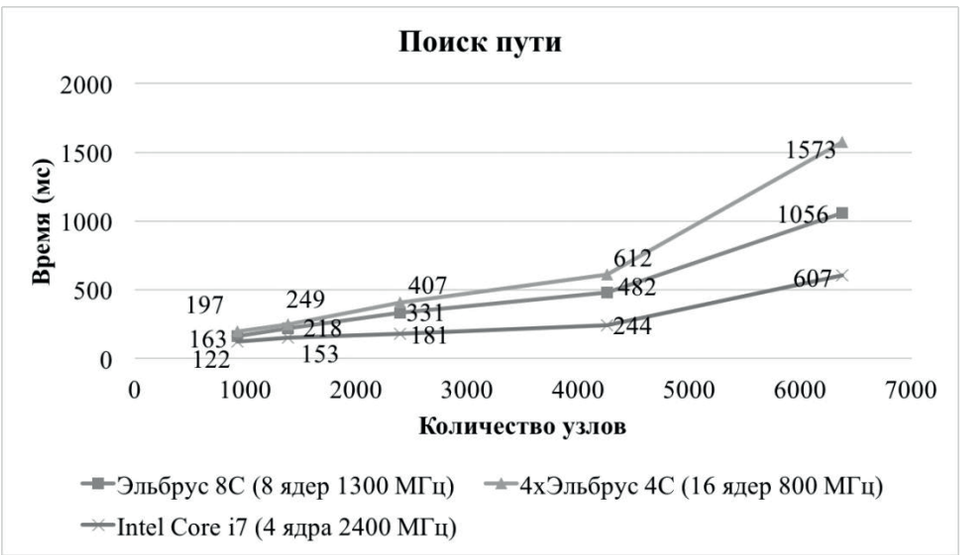


Рис. 2. Зависимость времени поиска пути роботом от количества узлов в графе

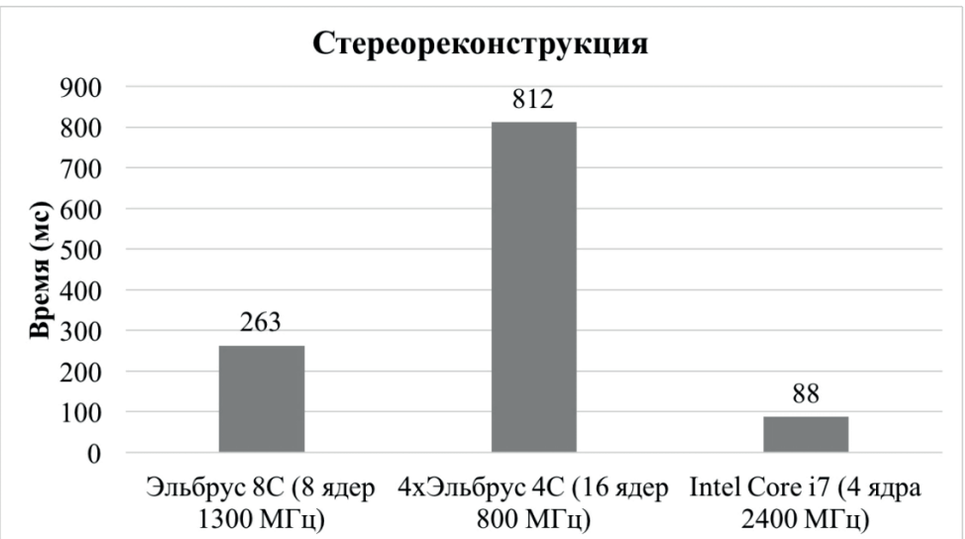


Рис. 3. Затраты времени на стереореконструкцию по стереопаре

Проведенное моделирование показало возможность применения общего программного обеспечения и средств вычислительной техники на основе микропроцессора «Эльбрус-8С» для решения задач движения робота и обработки системы технического зрения.

Новизна данной работы заключается в следующих положениях и результатах: разработаны тестовые программы для моделирования задач движения робота и системы стереозрения, получены временные характеристики для процессора «Эльбрус-8С».

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект №17-29-03297).

Литература

1. *Альфонсо Д.М., Деменко Р.В., Кожин А.С., Кожин Е.С., Колычев Р.Е., Костенко В.О., Поляков Н.Ю., Смирнова Е.В., Смирнов Д.А., Смольянов П.А., Тихорский В.В*. Микроархитектура восьмиядерного универсального микропроцессора «Эльбрус-8С» // Вопросы радиоэлектроники. 2016. Т. 4. № 3. С. 6–13.
2. *Бочаров Н.А., Сапачев И.Д., Парамонов Н.Б.* Макеты задач робототехнических комплексов на языке Java в среде ОС «Эльбрус» // Москва: Наноиндустрия. Спецвыпуск 2017(74). Издательство «Техносфера» С. 122 – 127.

3. *Бочаров Н.А., Парамонов Н.Б., Сапачев И.Д.* Реализация алгоритмов группового управления на языке Java в среде ОС «Эльбрус» // Современные информационные технологии и ИТ-образование. 2016, Т. 12, № 1, С. 108 – 115.

УДК 004.318

Исследование эффективности аппаратного сжатия хранимых в кэш-памяти данных на раннем этапе проектирования микпропроцессора

П.И. Крюков, А.И. Титов

Московский физико-технический институт (государственный университет)
АО «Интел А/О»

Аппаратное сжатие данных — перспективный способ увеличения вместимости кэш-памяти в современных микропроцессорах. В литературе данный подход предлагается как более эффективная альтернатива непосредственному увеличению площади, занимаемой кэш-памятью на кристалле [1]. Однако аппаратное сжатие имеет существенные накладные расходы, которые могут сделать его применение нецелесообразным. В данной работе предлагается подход для быстрой оценки эффективности аппаратного сжатия по сравнению с непосредственным увеличением кэш-памяти с такими же накладными расходами на площадь, не требующий полноценной реализации сжатия в потактовой модели процессора.

Положительный эффект от аппаратного сжатия состоит в том, что одна ячейка кэш-памяти может вместить больше сжатых блоков памяти. Наиболее простой способ состоит в хранении в одной физической ячейке кэш-памяти сжатых данных из двух блоков стандартного размера (cache line) вместо одного несжатого в случае, если возможно сжатие каждого из блоков в два раза. При такой организации кэша каждая ячейка должна быть расширена полями для второго тега, MESI-состояния и другими контрольными битами, но не полями данных (рис. 1). Другими накладными расходами на введение аппаратного сжатия становятся оборудование, производящее распаковку и упаковку данных, и вносимое им увеличение времени доступа в кэш-память.

В первом приближении эффект от сжатия данных эквивалентен увеличению размера кэш-памяти пропорционально усреднённому коэффициенту компрессии K, определённому как отношение количества блоков, сжатых в два раза, к общему количеству блоков. Чтобы оценить увеличение IPC от внедрения аппаратного сжатия, такой коэффициент был получен для каждой исследуемой трассы с использованием алгоритмов C-Pack 2 [2] (наибольшая эффективность), FPC [3] и BDI [4]. Далее, для каждой трассы при потактовом моделировании исходный размер кэш-памяти второго уровня 1,75 МБ был увеличен в соответствии с измеренным коэффициентом в диапазоне от 1,75 МБ при K = 0 % до 3,5 МБ при K = 100 %. Дополнительно на 2 такта было увеличено время чтения данных из кэш-памяти для моделирования распаковки. Усреднение результатов по всем трассам показало средний прирост IPC, соответствующий увеличению кэша до 2,25 МБ.

Накладные расходы на оборудование, требуемое непосредственно для логики сжатия и распаковки, были учтены в оценке площади. Согласно нашим оценкам теги, MESI-состояние и другие контрольные биты занимают 20 % ячейки, таким образом, удвоение этих полей увеличит площадь кэш-памяти на 20 %. Если бы эта площадь была использована для непосредственного наращивания кэш-памяти, её размер составил бы 2,125 МБ.

Для оценки эффективности аппаратного сжатия при неизменном количестве доступного оборудования необходимо сравнить приросты IPC, полученные при увеличении количества хранимых в кэш-памяти данных сжатием и непосредственным расширением, либо соответствующие им размеры кэша. Для рассматриваемой в данной работе модели процессора предлагаемый подход показал целесообразность использования аппаратного сжатия, так как оно позволяет в среднем увеличить размер кэша на 128 КБ без увеличения занимаемой площади. Метод может быть развит как для анализа частичного

использования сжатия в кэш-памяти (например, для половины ячеек), так и исследований при фиксированном значении энергопотребления или других характеристик.

Теги	MESI	Данные
0xf410	M	0000......0000
0xb510	E	ffff......ffff
0x3610	E	1b23......2acc

Теги	MESI	Данные		Теги	MESI
0xf410	M	{00..00}	{FF..FF}	0xb510	E
0x3610	E	1B23......2ACC		*X*	I
X	I	*X*		*X*	I

Рис. 1. Пример размещения данных в обычном кэше (слева) и в кэше со сжатием данных (справа)

Литература

1. *Ahn E., Yoo S.-M., Kang S.-M. S.* Effective Algorithms for Cache-Level Compression // Proceedings of the 11th Great Lakes Symposium on VLSI. 2001. P. 89–92.
2. *Chen X., Yang L., Dick R. P., Shang L, Lekatsas H.* C-pack: a high-performance microprocessor cache compression algorithm // IEEE Transactions on VLSI Systems. 2010. VIII. P. 1196–1208.
3. *Alameldeen A. R., Wood D. A.* Frequent Pattern Compression: A Significance-Based Compression Scheme for L2 Caches // Technical Report 1500, Computer Sciences Department, University of Wisconsin-Madison. 2000. IV.
4. *Pekhimenko G., Seshadri V., Mutlu O., Gibbons P. B., Kozuch M. A., Mowry T. C.* Base-delta-immediate compression: practical data compression for on-chip caches // Proceedings of the 21st International Conference on PACT. 2012. P. 377–388.

УДК 004.318

Анализ и оптимизация использования физического регистрового файла в современном суперскалярном микропроцессоре

А.А. Шишпанов[1,2], К.Р. Гарифуллин[2]

[1]Московский физико-технический институт (государственный университет)
[2]АО «Интел А/О»

Современный суперскалярный микропроцессор использует модель внеочередного исполнения инструкций и механизм переименования архитектурных регистров в физические. Переполнение физического регистрового файла приводит к временной приостановке загрузки новых инструкций и ожиданию высвобождения ресурсов, снижающему производительность. Увеличение размера регистрового файла не всегда оказывается возможным из-за физических ограничений и требований по энергоэффективности. Единственным способом улучшения производительности является повышение эффективности использования физического регистрового файла. В данной работе предлагается метод раннего освобождения регистров, позволяющий повысить эффективность использования регистрового пространства.

Предварительно проведённое исследование показало, что большую часть времени физические регистры используются неэффективно. Только 10% времени физические регистры используются по назначению, т.е. хранят вычисленные значения от момента записи в них вычисленного значения до его последнего использования, 16% времени ожидают записи готового результата. Около 74% времени физические регистры избыточно удерживаются после последнего чтения данных из них до момента последовательной фиксации архитектурного состояния и последующего высвобождения.

Существующие методы раннего освобождения физических регистров предлагают сохранять архитектурное состояние только для некоторых инструкций, что позволяет освободить часть физических регистров раньше. Для отслеживания того, какие архитектурные состояния необходимо сохранить для дальнейших вычислений, некоторые методы раннего освобождения физических регистров предлагают учёт их использований в других инструкциях с помощью счётчиков [1]. Такой подход позволяет точно отслеживать зависимости по данным, но ведёт к дополнительным аппаратным расходам для реализации

счётчиков. Другие методы раннего освобождения сохраняют физические регистры только для некоторых инструкций [2], [3]. Эти инструкции являются контрольными точками восстановления архитектурного состояния и помечаются специальным образом в процессе помещения их в промежуточные буферы согласно ранее определённым эвристикам. Некоторые физические регистры могут использоваться для восстановления архитектурного состояния при возникновении событий, приводящих к переисполнению инструкций. Так как заведомо неизвестно, какие именно инструкции вызовут эти события, при использовании описанных методов не все необходимые контрольные точки могут быть сохранены, и физические регистры могут быть освобождены преждевременно. В такой ситуации для восстановления всех потерянных данных вынужденно производится переисполнение затронутых инструкций [4], что негативно сказывается на производительности. Разработанный метод раннего освобождения регистров производит виртуальную, аналогичную обычной, фиксацию архитектурного состояния, но не влияющую на фактическое архитектурное состояние процессора. Виртуальная фиксация, в отличие от обычной, не замедляется на незавершённых инструкциях, высвобождает уже использованные физические регистры и сохраняет только необходимые в дальнейшем архитектурные состояния. Такой метод позволяет высвобождать регистры заведомо безопасно, не приводит к дополнительным расходам на переисполнение и легко масштабируется под имеющиеся ресурсы в силу своей итеративности.

Сравнение производительности процессора при удвоении размера физического регистрового файла и при использовании предложенного метода раннего освобождения физических регистров изображено на рис. 1. Использование раннего освобождения даёт прирост производительности, сопоставимый с удвоением размера физического регистрового файла.

Удвоение размера физического регистрового файла	+2,8%
Использование раннего освобождения физических регистров	+2,1%

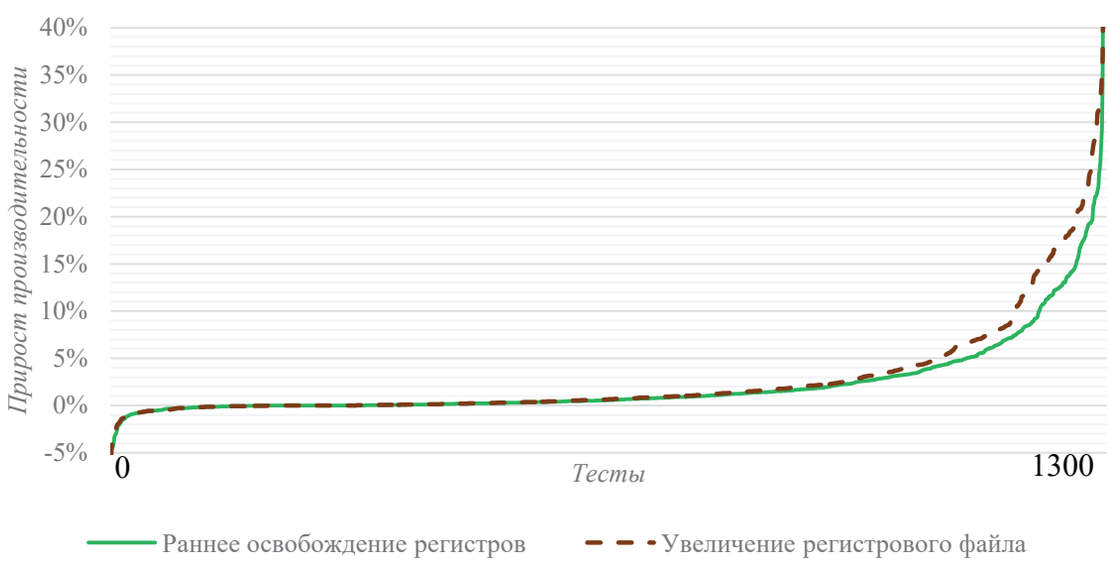


Рис. 1. Прирост производительности при использовании раннего освобождения регистров и при удвоении размера физического регистрового файла

Литература

1. *Moudgill M., Pingali K., Vassiliadis S.* Register Renaming and Dynamic Speculation: An Alternative Approach // Proc. 26th Ann. Int'l Symp. Microarchitecture (MICRO '93). 1993. P. 202 – 213.

2. *Akkary H., Rajwar R., Srinivasan S. T.* Checkpoint Processing and Recovery: An Efficient, Scalable Alternative to Reorder Buffers // IEEE Micro. 2003. 23, 6. P. 11 – 19.
3. *Akkary H., Rajwar R., Srinivasan S. T.* An analysis of a resource efficient checkpoint architecture // ACM Trans. Archit. Code Optim. 2004. 1, 4. P. 418 – 444.
4. *Srinivasan S. T., Rajwar R., Akkary H., Gandhi A., Upton M.* Continual flow pipelines // SIGARCH Comput. Archit. News. 32, 5. October 2004. P. 107 - 119.

УДК 004.318

Механизм выборочного переиспользования запросов подкачки инструкций для суперскалярного микропроцессора

О.И. Ладин[1,2], А.Ю. Сивцов[2]

[1]Московский физико-технический институт (государственный университет)
[2]АО «Интел А/О»

В современных микропроцессорах для сокращения времени доступа к памяти используются системы кэшей [1]. Данная система строится по принципу пирамиды, согласно которому наименьшее время доступа обеспечивается лишь для небольшого объёма данных. Самый быстрый и, соответственно, самый компактный кэш первого уровня обычно разделяется на кэш инструкций и кэш данных, для исключения конфликтов между используемыми данными и инструкциями. Кэши более высоких уровней являются общими (рис. 1).

Для подкачки инструкций в кэш первого уровня, из кэша второго уровня, используется буфер предподкачки инструкций [2]. Он представляет собой временное хранилище для адресов запросов, а также для подкаченных данных, которые не были доступны в кэше инструкций.

Буфер предподкачки служит интерфейсом между инструкционным кэшем и кэшем второго уровня. Конечные размеры этого буфера могут стать причиной приостановки конвейера микропроцессора, когда невозможно выделить место для нового запроса. Данные блокировки могут значительно повлиять на производительность микропроцессора в случае ошибок предсказания ветвлений, если отсутствует возможность запросить правильные инструкции, следующие за переходом.

Невозможность стирания ненужных запросов в память обусловлена сложностью определения и корректного восстановления состояния системы памяти при отмене запроса. Однако предложенный в [3] механизм виртуализации буфера предподкачки позволяет обойти это ограничение, вводя наряду с физическими (реальными ячейками буфера) виртуальные ячейки, которые являются указателями на выделенную для этого запроса физическую ячейку. В случае ошибки предсказания появляется возможность освободить физические ячейки, сбросив указатель в соответствующей виртуальной ячейке. Сами же запросы всё время остаются активными, но при возвращении данных игнорируются.

В случае неправильного предсказания переходов часть запросов является валидной для обоих направлений предсказания. Предложенный ранее механизм будет отправлять запросы по правильному пути, включая совпадающие с только что отменёнными. Эффективный размер буфера предподкачки будет меньше начального значения (часть виртуальных ячеек занята), что также может приводить к остановкам конвейера.

В данной работе предлагается метод, позволяющий в некоторых случаях избежать повторной отправки раннее отменённого запроса. Метод основан на том, что раннее отправленный активный запрос вернёт данные, поэтому его можно переиспользовать, достаточно убедиться в соответствии адресов. Это позволяет сэкономить виртуальную ячейку буфера предподкачки, сократить время ожидания данных, снизив число отправок излишних запросов в систему памяти.

В программном потактовом симуляторе микропроцессора был имплементирован механизм, позволяющий отменять запросы в случае ошибок предсказания переходов, а также переиспользовать раннее отменённые, но ещё активные запросы в случае

совпадении их адресов. Общее количество запросов было снижено на 3%. Время простоя конвейера микропроцессора, обусловленное переполнением буфера предподкачки было сокращено на 75%. Среднее значение прироста производительности от применения данной техники оценивается в +0.1%.

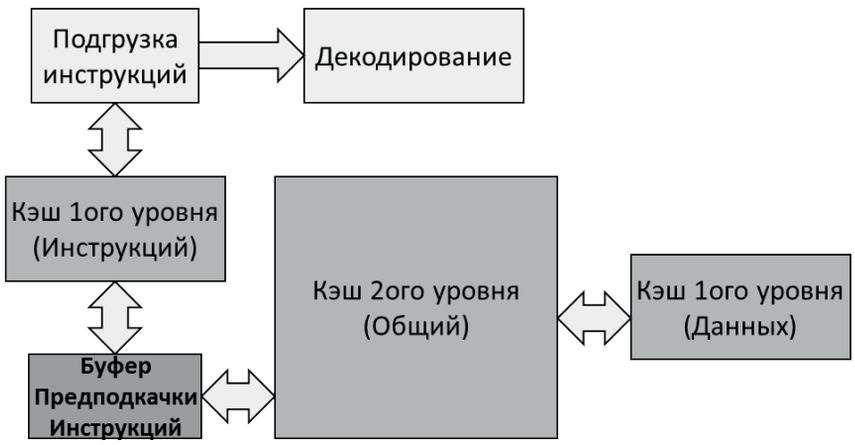


Рис. 1. Блок-схема первых стадий конвейера с системой памяти ядра микропроцессора

Литература

1. *Hennessy J.L., Patterson D.A.* Computer Architecture: A Quantitative Approach 5th Edition. San Francisco: Morgan Kaufmann Publishers Inc., 2011. P. 857.
2. *Jouppi N.P.* Improving direct-mapped cache performance by the addition of a small fully-associative cache and prefetch buffers // ISCA '90 Proceedings of the 17th annual international symposium on Computer Architecture. 1990. P. 364–373.
3. *Mowry T.C., Lam M.S., Gupta A.* Design and evaluation of a compiler algorithm for prefetching // ASPLOS V Proceedings of the fifth international conference on Architectural support for programming languages and operating systems. 1992. P. 62–73.

УДК 004.318

Методология измерения производительности микропроцессора в режиме одновременной многопоточности

Г.М. Корепанов, О.В. Шимко

Московский физико-технический институт (государственный университет)

Потактовое моделирование является одним из основных инструментов разработки современных процессоров, и его точность принципиально важна для принятия микроархитектурных решений. При моделировании используются эталонные тестовые наборы, большая часть которых предназначена для потактового моделирования однопоточного (single-threaded, ST) режима. В то же время инфраструктура для моделирования работы процессора в режиме одновременной многопоточности (simultaneous multithreading, SMT) развита хуже. Разумной альтернативой разработке тестов, предназначенных для SMT-моделирования, является адаптация существующей ST-инфраструктуры. Таким образом, возникает принципиальная задача измерения производительности многопоточного режима с помощью тестовых наборов, предназначенных для работы в однопоточном режиме.

Существующая методология моделирования многопоточного исполнения основывается на моделировании одновременного исполнения нескольких однопоточных трасс тестового набора. Несмотря на простоту такого подхода, он обладает существенными недостатками:

- недостаточная репрезентативность выборки комбинаций трасс, исполняемых в многопоточном режиме. Поскольку количество возможных комбинаций экспоненциально

растет с количеством потоков, случайная выборка поднабора для моделирования оказывается недостаточно репрезентативной [1];

- отсутствие моделирования совместного использования кода (code sharing). При исполнении нескольких трасс одной и той же программы общий код может быть переиспользован разными потоками. Эта функциональность не моделируется в силу специфических ограничений однопоточных трасс, что приводит к заниженному значению производительности. При этом ошибка может в среднем достигать 5%.

Таким образом, для точного моделирования многопоточного исполнения необходимо, во-первых, решить задачу репрезентативной выборки комбинаций трасс и, во-вторых, решить проблему моделирования и оценки влияния на производительность совместного использования общего кода. При решении этих задач мы рассматривали случай одновременного исполнения двух потоков, однако результаты могут быть обобщены и на большее число потоков.

При выборе комбинаций трасс использовался метод кластеризации для набора пар с уникальным поведением на основании анализа исходных трасс и данных моделирования [2]. Однако в данной работе для получения наиболее репрезентативной выборки использовалось существенно большее число исходных тестов по сравнению с предыдущими работами. Поэтому для сокращения количества комбинаций мы предварительно провели детальную кластеризацию исходных однопоточных трасс, выбрав по одному представителю из групп близких по параметрам тестов. Кроме того, чтобы повысить репрезентативность выборки пар трасс, при кластеризации были использованы дополнительные характеристики, специфичные для многопоточного режима исполнения, такие как доля общего кода между потоками и чувствительность потоков к уменьшению доли ресурсов машины. Наконец, при определении веса выбранных пар использовались не только количество пар трасс со сходными характеристиками, но и доля изначальной программы, представленная каждой трассой. В результате была получена выборка, отражающая исходное множество пар значительно точнее, чем случайные выборки. Это проверено прямым сравнением средних значений производительности на выборках и на большом наборе случайных пар.

В существующем подходе пару однопоточных трасс невозможно запустить в многопоточном режиме с корректным моделированием совместного использования общего кода, так как в разных трассах физические адреса одних и тех же инструкций могут оказаться различными. Мы решили эту проблему, реализовав совмещение физических адресов с помощью инструмента для объединения образов памяти двух тестов в единый образ с общим адресным пространством. Однако данный подход имеет ограничения. В частности, он не может быть применен для некоторых пар из-за несоответствия размеров страниц в их образах памяти. Для оценки эффекта совместного использования кода на всех парах трасс мы предложили интерполяционный метод, основываясь на механизме влияния этой функциональности на производительность. Поскольку линии, использующиеся в каждом из потоков, не дублируются, освобождается часть кеша инструкций, что эквивалентно увеличению его эффективного размера (рис. 1) и, следовательно, производительности. Поэтому, интерполировав зависимость эффективного размера кеша от доли общего кода на все пары, мы рассчитали изменение производительности на каждой комбинации трасс.

Для валидации рассчитанных значений прироста производительности мы воспользовались отдельным набором точек, полученных при моделировании совместного использования кода для пар трасс с подходящими образами памяти. Проверка на этих парах показала хорошую точность полученных значений, что и доказывает состоятельность нового подхода. Данная методология была апробирована для моделирования многопоточного исполнения с 2 и 4 потоками на потактовом симуляторе микропроцессора суперскалярной микроархитектуры.

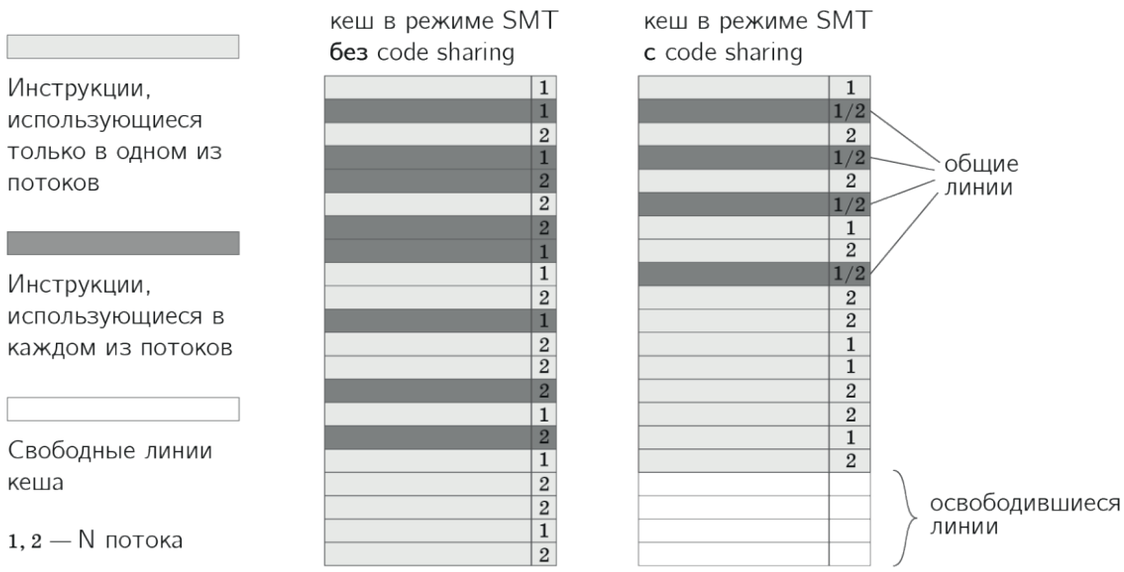


Рис. 1. Механизм увеличения эффективного размера кеша при использовании потоков общих линий

Литература

1. *Ricardo A. Velasquez, Pierre Michaud, Andr´e Seznec*. Selecting Benchmark Combinations for the Evaluation of Multicore Throughput// International Symposium on Performance Analysis of Systems and Software, Apr. 2013, Austin, United States. 2013.
2. *Eeckhout L., Vandierendonck H. and De Bosschere K.* Workload design: selecting representative program-input pairs//International Conference on Parallel Architectures and Compilation Techniques. 2002. P. 83–94.

УДК 004.272.34

Влияние баланса вычислительной производительности и скорости доступа к памяти на эффективность расчетов электронной структуры: сравнение процессоров Intel, AMD и Nvidia

***В.С.Вечер*[1,2], *В.В. Стегайлов*[2,1]**

[1]Московский физико-технический институт (государственный университет)
[2]Объединённый институт высоких температур РАН

Задачи вычислительного материаловедения являются крайне популярным и ресурсоемким направлением вычислительной науки, например, расчеты одного только популярного квантового пакета VASP потребляют 15–20% времени всех суперкомпьютеров мира. Решение таких задач требует значительных вычислительных мощностей суперкомпьютеров, при достаточно высокой их стоимости. Поэтому вопросы снижения стоимости закупки суперкомпьютеров путем эффективного их ко-дизайна и снижения стоимости их эксплуатации являются актуальными. Многие высокопроизводительные системы известны тем, что демонстрируют в реальных приложениях малую долю своей пиковой производительности, что особо касается многоядерных и многосокетных узлов. Недавняя работа Stanisic и др. [1] подчеркивает большое количество подводных камней при попытке характеризовать производительность современных машин с точки зрения интерконнекта и подсистемы памяти.

В настоящее время доступен широкий ассортимент серверных процессоров от Intel и AMD, кроме того, в данный сегмент постепенно приходят и новые игроки, например, Nvidia с их архитектурой Denver. Они различаются между собой количеством ядер и тактовой частотой, размером и латентностью системы кэшей, скоростью работы памяти [2]. В первой части доклада авторы продемонстрируют способ сравнения различных платформ и наличие универсальной тенденции $t_{\mathrm{solve}} * R_{\mathrm{peak}} = F(N_{\mathrm{cores}}, \mathrm{Balance})$. Будет

продемонстрирован способ напрямую измерить эффективность использования вычислительного оборудования, и показано, как эффективность работы подсистемы памяти влияет на скорость расчета кодов VASP и GROMACS.

С другой стороны, большая вычислительная нагрузка порождает существенное тепловыделение и энергопотребление компонентов суперкомпьютеров. Достижение экзафлопсного уровня сопряжено с необходимостью демонстрировать производительность не менее 50 GFLOP/s на каждый затрачиваемый в расчетах Ватт, в то время как у самых лучших суперкомпьютеров из списка Green500 такой параметр достигает значения 10–14 GFLOPs/Watt [3]. Кроме того, высокое энергопотребление и тепловыделение суперкомпьютеров оборачивается дополнительными статьями расходов. Во второй части доклада авторы покажут сравнение нескольких архитектур по их энергопотреблению в кодах вычислительного материаловедения, и продемонстрируют существование оптимальных с точки зрения энергозатрат режимов расчета.

Работа поддержана грантом РНФ №14-50-00124.

Литература

1. *Stanisic L.* [*et al*]. Characterizing the Performance of Modern Architectures Through Opaque Benchmarks: Pitfalls Learned the Hard Way // IPDPS 2017-31st IEEE International Parallel & Distributed Processing Symposium (RepPar workshop). 2017.
2. *Stegailov V.V., Vecher V.S.* Efficiency analysis of Intel and AMD x86_64 architectures for ab-initio calculations: a case study of VASP // Суперкомпьютерные дни в России: Труды международной конференции (25–26 сентября 2017, г. Москва). 2017. С. 904.
3. http://www.teratec.eu/library/pdf/forum/2014/Presentations/SP04_C_Zeller_NVIDIA_Forum_Teratec_2014.pdf

УДК 004.318

Повышение энергоэффективности микропроцессора за счёт уменьшения спекулятивного исполнения

К.А. Королев, О.В. Шимко, И.В. Смирнов

Московский физико-технический институт (государственный университет)
АО «Интел А/О»

Сегодня одним из основных микроархитектурных способов улучшения производительности микропроцессора является повышение параллелизма на уровне инструкций за счет увеличения глубины внеочередного исполнения. В свою очередь это приводит к увеличению спекулятивного исполнения в направлении, выбранном предсказателем ветвлений кода. При неправильно предсказанном направлении ветвления результаты спекулятивного исполнения являются неверными и очищаются. Такую спекулятивность называют ошибочной. В современных процессорах ошибочная спекулятивность составляет более 20% и продолжает расти, так как несмотря на постепенно увеличивающуюся точность предсказателей ветвлений, более высокие темпы роста глубины внеочередного исполнения приводят к итоговому увеличению ошибочной спекулятивности. Таким образом, ошибочная спекулятивность является значительной проблемой, и ее снижение имеет большой потенциал для увеличения энергоэффективности и производительности микропроцессора.

Современные методы снижения ошибочной спекулятивности основываются на ограничении спекулятивного исполнения [1 – 3]. Предметом исследования является баланс между точностью определения ошибочной спекулятивности и ее покрытием. Точность важна для минимизации задержек в исполнении полезных инструкций, приводящих к снижению производительности. Покрытие важно для максимального снижения энергопотребления микропроцессора и повышения его производительности за счет лучшей энергоэффективности. Отличия предложенных методов заключаются в алгоритме

определения ошибочной спекулятивности, а также в использовании полного или частичного ограничения исполнения.

Предложенные исследования рассматривают снижение ошибочной спекулятивности в однопоточном режиме. Данная работа изучает универсальный метод ограничения спекулятивного исполнения инструкций как для однопоточного, так и для многопоточного режима исполнения инструкций. Для принятия решения об остановке исполнения используется кумулятивная статистическая оценка точности предсказаний ветвлений. Статистика предсказаний ветвлений накапливается в буфере истории ветвлений и позволяет оценить точную вероятность правильного предсказания для каждого отдельного ветвления. Вероятность правильной спекулятивности оценивается как произведение вероятностей правильного предсказания всех предшествующих ветвлений, исполняемых в данный момент. Остановка исполнения спекулятивных инструкций происходит, когда вероятность правильной спекулятивности оказывается ниже порогового значения. Исполнение возобновляется при превышении порогового значения вероятностью правильной спекулятивности, которая повышается при каждом завершении исполнения ветвления. При этом если предсказание ветвления было неправильным, то происходит снижение энергопотребления микропроцессора за счет остановки ошибочного спекулятивного исполнения. Снижение энергопотребления приводит к росту тактовой частоты, что приводит к увеличению производительности (IPS, Instructions Per Second), если достаточно мало снижение IPC (Instructions Per Cycle) из-за ограничения исполнения полезных спекулятивных инструкций.

В многопоточном режиме остановка спекулятивного исполнения происходит отдельно для каждого потока. При этом буфер истории ветвлений статически разделяется между потоками. В отличие от однопоточного режима снижение ошибочной спекулятивности в многопоточном режиме может привести не только к уменьшению энергопотребления, но и к увеличению IPC. Остановка спекулятивного исполнения одного потока позволяет достичь большего использования свободных ресурсов аппаратуры внеочередного исполнения другими потоками и увеличить их производительность. Также стоит отметить, что потенциал для применения данной техники в многопоточном режиме ниже по сравнению с однопоточным режимом, так как ошибочная спекулятивность меньше в режиме многопоточного исполнения (10% в многопоточном режиме против 20% в однопоточном режиме).

Данный подход был реализован в программном потактовом симуляторе архитектуры микропроцессора. Результаты моделирования показали снижение энергопотребления на 0.6 – 0.7%, снижение IPC на 0.1 – 0.2% и увеличение итоговой производительности на 0.1%. В многопоточном режиме в среднем не наблюдается ожидаемого роста IPC. Анализ работы метода выявил, что основная причина отсутствия роста IPC – недостаточная точность остановок исполнения на группе тестов.

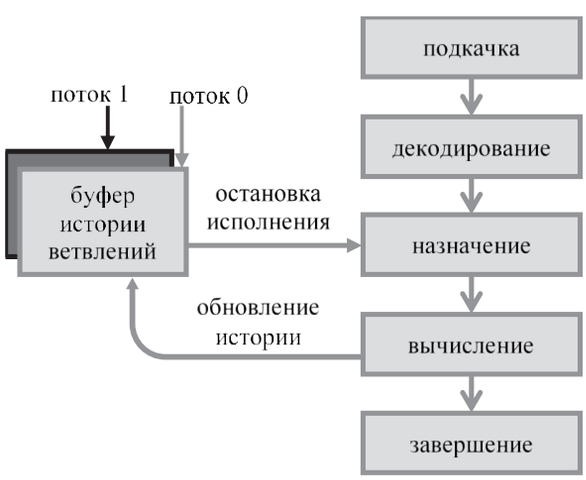


Рис. 1. Схема остановки конвейера микропроцессора по истории предсказаний ветвлений

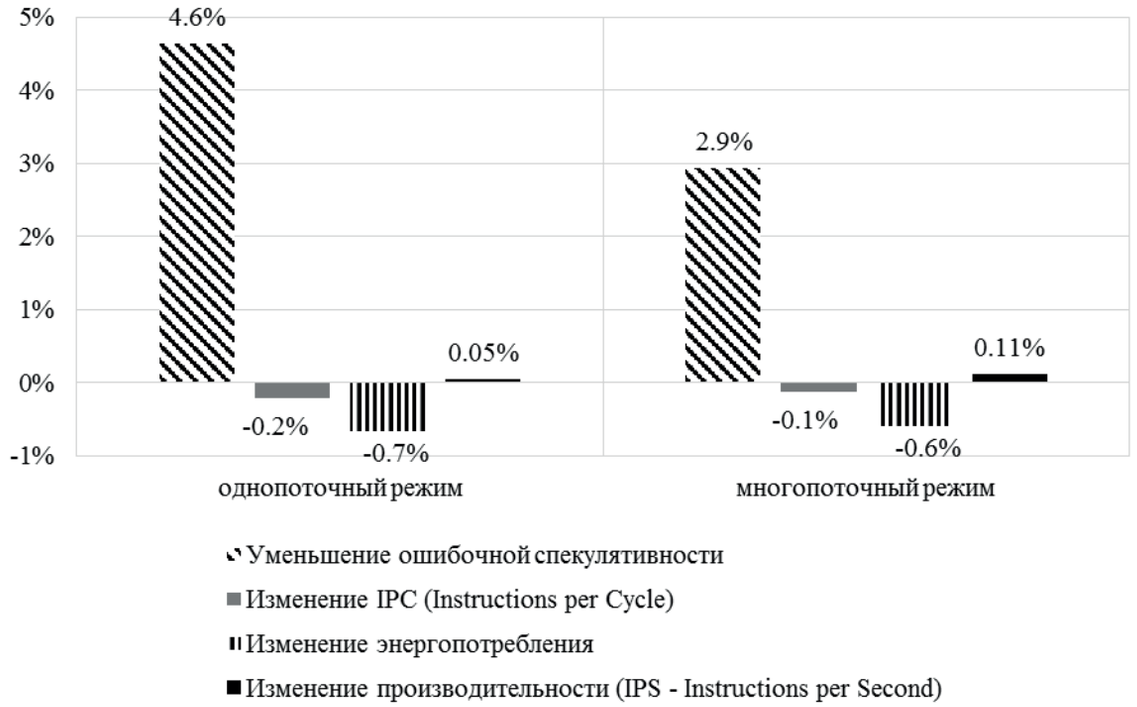


Рис. 2. Результаты моделирования оптимальных конфигураций разработанного метода в однопоточном и многопоточном режимах исполнения инструкций

Литература

1. *Manne S., Klauser A., Grunwald D.* Pipeline Gating: Specualtion Control for Energy Reduction // 25th Annual International Symposium “Computer Architecture”. 1998. P. 132 – 141.
2. *Lee C.J., Kim H., Mutlu O., Patt Y.N.* Performance-Aware Speculation Control using Wrong Path Usefulness Prediction // 14th International Symposium “High Performance Computer Architecture”. 2008. P. 39 – 49.
3. *Baniasadi A., Moshovos A.* Instruction Flow-Based Front-End Throttling for Power-Aware High-Performance Processors // International Symposium “Low Power Electronics and Design”. 2001. P. 16 – 21.

УДК 004.318

Оценка эффективности дистилляции данных в кэше второго уровня на раннем этапе проектирования микропроцессора

Г.А. Чирков, П.И. Крюков, А.И. Титов

Московский физико-технический институт (государственный университет)
ЗАО «Интел А/О»

Размер кэш-памяти микропроцессора является важным фактором, определяющим его производительность: больший размер кэша увеличивает процент попаданий в него, а значит, уменьшает среднее время доступа в память. Однако увеличение кэша сопряжено с дополнительными накладными расходами: увеличением времени чтения, занимаемой площади и др. [1]. Современные исследования предпринимают попытки увеличить вместимость кэш-памяти, не меняя при этом ее размеров. Ярким примером этого является дистилляция кэш-памяти [2] – техника, позволяющая отбрасывать потенциально ненужную часть линии при ее загрузке в кэш и размещать в освободившееся место другие данные. В данной работе предлагается подход для быстрой оценки максимальной возможной эффективности дистилляции кэша второго уровня по сравнению с непосредственным

увеличением кэш-памяти с такими же накладными расходами на площадь, не требующий полноценной реализации дистилляции в потактовой модели процессора.

Дистилляция основана на том факте, что различные данные обладают различными показателями пространственной локальности. В текущих процессорах это никак не используется: данные в кэш загружаются блоками фиксированного размера 64 байта. Однако данный размер не всегда является оптимальным. Так, например, обход столбца матрицы (рис. 1) приводит к тому, что большая часть байтов в линии не используется. В такой ситуации эффективнее было бы отбросить неиспользуемые байты, а на освободившееся место разместить другие линий и тем самым увеличить процент попаданий.

В простейшем случае дистилляции каждая линия виртуально делится на две части одинакового размера (рис. 2). Чтобы предсказывать, какие из частей линии будут использованы, нужно специальное устройство – предсказатель. Перед размещением линии в кэш-память, предсказатель сообщает, будет ли линия использована только наполовину, а также какая именно половина нужна, остальное содержимое линии отбрасывается. Таким образом, в одной ячейке кэша может быть размещено уже до двух половинок разных линий. Такой подход требует определенных издержек. Главной из них является введение двойных тегов, которые нужны для идентификации каждой из двух половинок, размещенных в одном блоке.

В работе была оценена эффективность внедрения дистилляции кэша при использовании идеального предсказателя. Данная оценка легко осуществима, и она позволяет быстро выяснить максимальное возможное преимущество от внедрения дистилляции на этапе раннего проектирования микропроцессора, не реализуя полноценной модели в симуляторе. Оценка прироста IPC для каждой трассы выполняется в два этапа. Сначала по каждой линии собирается статистика доступа к каждой ее половине. Исходя из статистики, выносится решение, можно ли считать ее дистиллируемой или нет. Далее, информация о дистиллируемости каждой линии используется во втором этапе, где на ее основе выносится решение, можно ли конкретную линию загрузить в кэш частично.

Оценка выполнялась на потактовом симуляторе ×86 архитектуры на кэше второго уровня размера 2 МБ, и показала средний прирост IPC +0.8%. Такое значение соответствует кэшу второго уровня размера 2.25 МБ. Расчеты показывают, что двойные тэги увеличивают площадь кэша на 20%, что соответствует его размеру в 2.4 МБ. Таким образом, в рамках данной работы без полноценной реализации дистилляции в симуляторе было выяснено, что даже при использовании идеального предсказателя, внедрение дистилляции в архитектуре ×86 оказывается менее эффективным, чем прямое увеличение кэша.

Для того чтобы увеличить эффективность дистилляции, она может быть скомбинирована с другими подходами к размещению данных в кэше, использующими двойные тэги. Например, в работах [3], [4] для увеличения количества линий в кэше используется компрессия – метод, позволяющий сжимать данные для их более компактного размещения. Комбинация дистилляции и компрессии может оправдать дополнительные затраты, связанные с появлением двойных тегов. Оценка их совместной эффективности является темой для дальнейших исследований.

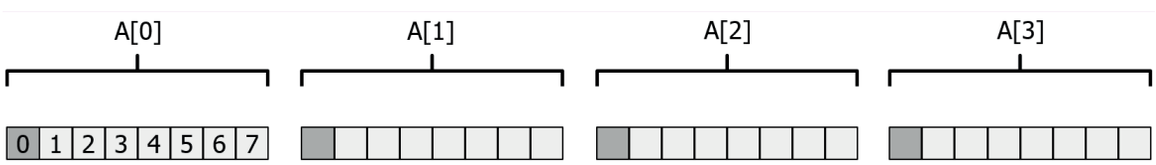


Рис. 1. Расположение матрицы в памяти с точки зрения кэша (темной заливкой выделены те части линий, которые используются при обходе нулевого столбца)

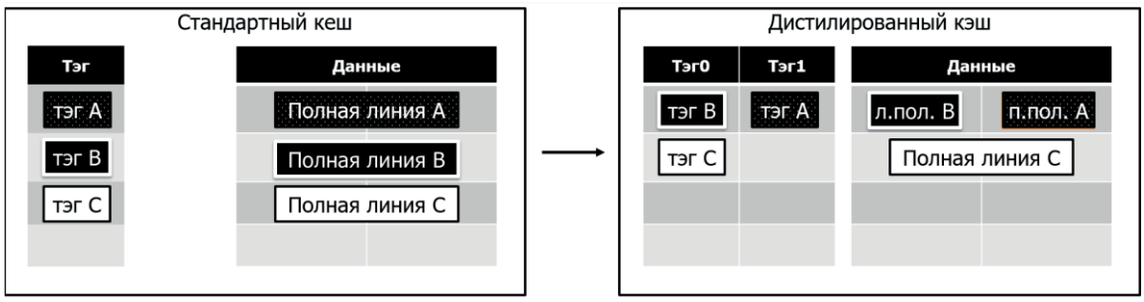


Рис. 2 Кэш с включенной и выключенной дистилляцией

Литература

1. *John Hennessy, David Patterson* Computer Architecture: A Quantitative Approach, 5th edition. Appendix C.
2. *Moinuddin K. Qureshi*, *M. Aater Suleman*, *Yale N. Patt* Line distillation: Increasing Cache Capacity by Filtering Unused Words in Cache Lines // HPCA '07 Proceedings of the 2007 IEEE 13th International Symposium on High Performance Computer Architecture. P. 420 – 429.
3. *Gennady Pekhimenko, Vivek Seshadri, Onur Mutlu, Michael A. Kozuch, Phillip B. Gibbons, Todd C. Mowry* Base-delta-immediate compression: practical data compression for on-chip caches // Proceedings of the 21st international conference on Parallel architectures and compilation techniques. P. 377 – 388.
4. *Somayeh Sardashti, Andre Seznec, David A. Wood* Yet Another Compressed Cache: A Low-Cost Yet Effective Compressed Cache // ACM Transactions on Architecture and Code Optimization (TACO). 2016. V. 13. I. 3.

УДК 004.4'422

Автоматическая векторизация вызовов трансцендентных функций

Д.А. Земляков

ЗАО «МЦСТ»
ПАО «ИНЭУМ им. И.С. Брука»

Как правило, значительная часть времени исполнения программ приходится на циклы, поэтому задача оптимизации циклов важна для обеспечения максимальной производительности [1]. Наличие в теле цикла вызовов трансцендентных функций может значительно ослабить эффект от его векторизации и распараллеливания. В этом случае особенно возникает необходимость в автоматической векторизации операций вызовов. Проблема приобретает наибольшую актуальность применительно к архитектурам со статическим планированием, рассчитанным на достижение высших показателей производительности, к которым относятся серии отечественных микропроцессоров архитектуры «Эльбрус», предназначенных для разработки крупномасштабных информационно-вычислительных систем стратегического назначения [2].

Методы автоматической векторизации исследуются достаточно давно, и как показывает практика, их использование позволяет значительно увеличить производительность процессоров. Большинство алгоритмов ориентировано на использование коротких векторных инструкций, на которые можно заменить группы изоморфных скалярных операций после «раскрутки» цикла. Однако при наличии в цикле вызовов трансцендентных функций наибольший интерес представляет алгоритм, не относящийся к этому классу. В данном алгоритме используются значительно более быстрые векторные трансцендентные функции, использующие архитектурные особенности конкретного микропроцессора. В частности, для микропроцессоров архитектуры «Эльбрус» подобные функции реализованы в библиотеке EML (Elbrus Math Library) [2].

Для векторизации рассматриваются только удовлетворяющие требованиям анализа алгоритма операции самих вложенных циклов с подходящей структурой. В случае известного числа итераций цикла необходимо, чтобы оно превышало некоторое пороговое значение, после которого векторизация становится эффективной. В случае неизвестного

числа итераций строится две версии цикла, к одной из которых применяется оптимизация, а выбор используемой версии происходит при исполнении программы. В рабочем цикле перед операцией вызова трансцендентной функции строятся операции записи ее аргументов во временный входной массив. Вместо чтений результата исходной скалярной операции вызова строятся операции чтения результата векторной функции, взятые из временного выходного массива. В новом пустом эпилоге исходного цикла строится вызов необходимой векторной функции, аргументами которой становятся указанные временные входной и выходной массивы. Оригинальная скалярная операция вызова удаляется, строится копия исходного цикла после вызова векторной функции. В оригинале и копии цикла устраняются избыточные операции.

В случае циклов с большим или неизвестным числом итераций может потребоваться разрезание исходного цикла. Для эффективной работы с данными они должны размещаться в стеке, входной и выходной массивы векторной функции должны помещаться в кэш L1. Исходя из этих требований размером массива была выбрана константа 1000. Также при разрезании исходного цикла внутренний цикл не должен отличаться от исходного с т.з. базовой индуктивности. В результате преобразования строится внешний охватывающий цикл с шагом счетчика равным выбранной константе. Счетчик внешнего цикла одновременно служит начальным значением для счетчика модифицированного внутреннего цикла и его копии, полученной в результате векторизации. Число итераций внутренних циклов на каждом шаге, кроме последнего, равно выбранной константе. На последнем шаге идет работа с оставшимися данными.

Автоматическая векторизация вызовов трансцендентных функций на основе данного алгоритма была реализована и внедрена в оптимизирующий компилятор для архитектуры «Эльбрус». Были сформулированы и протестированы условия применимости оптимизации, легшие в основу анализа контекста. Динамическая проверка количества итераций расширила границы применимости алгоритма. Для избежания выполнения действий, портящих контекст более эффективным методам оптимизации, например вынесению инвариантных операций, алгоритм был дополнен анализом эффективности.

Были проведены замеры времени исполнения задач из пакетов SPEC CPU2006 [3] на машинах с микропроцессорами с архитектурой «Эльбрус», показавшие прирост производительности до 17%.

Литература

1. *Muchnick S.* Advanced Compiler Design Implementation. 5-е изд. San Francisco: Morgan Kaufmann Publishers, 1997. 856 с. ISBN 978-1-5586-0320-2.
2. *Ким А.К., Перекатов В.И., Ермаков С.Г.* Микропроцессоры и вычислительные комплексы семейства Эльбрус. СПб.: Питер, 2013. 272 с. ISBN 978-5-459-01697-0.
3. Standard Performance Evaluation Corporation. [Электронный ресурс] http://www.spec.org/

УДК 004.415.53

Автоматизация поиска ошибок оптимизации в компиляторах языков C/C++ с помощью генератора случайных тестов
Yet Another Random Program Generator

В.Ю. Ливинский[1], Д.Ю. Бабокин[2]

[1]Московский физико-технический институт (государственный университет)
[2]Intel Corporation

Современные компиляторы являются сложными программными системами с большим количество ошибок. Эффективный поиск ошибок и оперативное сообщение о них разработчикам в удобной форме представляется сложной задачей, которую сложно решить без развития новых методов автоматизированного тестирования. Одним из самых хорошо зарекомендовавших себя и эффективным методом является применение генератора случайных тестов. А комбинация его с современными средствами детектирования

неопределённого поведения (undefined behavior sanitizer) и уменьшения размера тестовой программы (C–Reduce [1]), позволяет построить эффективную автоматизированную систему поиска ошибок, способную предоставлять минимальные тестовые примеры разработчикам компилятора.

В качестве случайного генератора тестов использовался и параллельно развивался YARPGen [2]. Несмотря на то, что идея случайной генерации тестов не является новой и существует несколько поколений генераторов, опыт применения даже наиболее развитых решений, таких как Csmith [3], Quest [4] и Orange [5], демонстрирует достаточно существенный потенциал для развития этой области. Именно поэтому нами было принято решение о создании и использовании собственной разработки.

Главными целями при дизайне YARPGen [2] было устранение недостатков предыдущих поколений генераторов, а именно консервативного подхода к устранению неопределённого поведения и отсутствие прямого контроля за параметрами, непосредственно влияющими на частоту срабатывания оптимизаций. В качестве метода устранения неопределённого поведения было выбрано точное моделирование результата вычислений (вместо использования функций-обёрток или отказа от применения знаковых целочисленных типов [6]). Для контроля за частотой срабатывания оптимизаций был проведён анализ различных типов оптимизаций и выделение общих свойств кода, которые необходимо контролировать в генераторе [7]. К таким свойствам кода относятся «содержательный» def-use граф (т.е. необходимо заботиться о достаточном количестве переиспользований переменных и контроля за средней длинной def-use цепочек), наличие участков кода насыщенных однотипными операциями, что многократно повышает вероятность применения оптимизаций основанных на свойствах арифметических операций, а также добавление констант, значения которых наиболее подходят для конкретного контекста (различные константы в арифметических и логических выражения) и так далее.

Применение новых принципов в построении генератора случайных программ позволило экспериментально показать, что возможно находить новые классы ошибок, а значит сохраняется значительный потенциал для улучшения методов генерации тестов. В компиляторе GCC было найдено множество ошибок, присутствующих во многих версиях продукта, и, соответственно, не найденных как другими генераторами тестов, так и другими инструментами и методами поиска ошибок. Наиболее старая найденная ошибка присутствовала в компиляторе GCC более 10 лет.

При этом экспериментальная эксплуатация генератора тестов выявила некоторые интересные особенности, которые стоит учитывать в дальнейшей работе. Так было замечено, что ключевым для поиска максимального количества ошибок является не только возможность генератора создавать код, который вызывает максимально частое срабатывание оптимизаций, но также возможность управлять и экспериментировать со статистическими свойствами генерируемого кода. То есть дизайн генератора должен предоставлять максимальный контроль за такими статистическими свойствами чтобы в дальнейшем позволит автоматизировать подбор таких параметров. Также было замечено, что крайне важно тестировать компилятор с максимальным набором опций. Очевидно, что это способно увеличить количество найденных ошибок, но, как оказалось, мы недооценили этот эффект. Так тестирование GCC в режиме undefined behavior sanitizer позволило вскрыть огромное количество проблем, проявляющихся и при отсутствии этого режима.

Требование максимально эффективного использования автоматизированной системы поиска ошибок налагает дополнительные требования к компилятору и его разработчикам. Во-первых, компилятор должен предоставлять встроенные механизмы для классификации ошибок и автоматического указания на некорректную оптимизацию. Без такого механизма сложно классифицировать различные сообщения об ошибках, а значит избегать дублирования сообщений об ошибках для разработчиков. Отметим, что такие средства присутствуют в ICC и Clang, но отсутствуют в GCC. Во-вторых, без оперативного исправления ошибок в компиляторе, автоматическая система начинает генерировать возрастающее количество дублирующих друг друга ошибок, которые могут оставить незамеченными некоторые новые типы ошибок. Стоит заметить, что все три

команды разработчиков компиляторов, с которыми проводилось экспериментальное внедрение системы, реагировали с различной степенью оперативности, но в сочетании со встроенными механизмами классификации ошибок этого оказывалось достаточно. Стоит отдельно упомянуть, что скорость исправления ошибок в GCC заметно выше, чем в других проектах, и время от сообщения об ошибке до исправления зачастую находилась в пределах одних-двух суток, тем самым отчасти сглаживая проблему отсутствия встроенного механизма классификации ошибок.

За два года удалось обнаружить 55 ошибок в Clang, 80 ошибок в GCC и сравнимое количество ошибок в проприетарных компиляторах (с полным списком найденных ошибок можно ознакомиться на сайте проекта [2]). Многие из ошибок оказались уникальными и вскрывали проблемы, которые присутствовали во многих версиях продукта. Ошибки были обнаружены в самых разнообразных компонентах компиляторов, что позволяет сделать вывод о высокой эффективности разрабатываемого генератора и его применимости для тестирования промышленных компиляторов.

Литература

1. *Regehr J., Chen Y., Cuoq P., Eide E., Ellison C. and Yang C.*: Test-Case Reduction for C Compiler Bugs // Proceedings of 33rd ACM SIGPLAN Conference on Programming Language Design and Implementation. 2012.
2. https://github.com/01org/yarpgen
3. *Yang X., Chen Y., Eide E. and Regehr J.*: Finding and understanding bugs in C compilers // Proc. ACM SIGPLAN Conference on Programming Language Design and Implementation. 2011. P. 283–294.
4. *Lindig C*. Find a compiler bug in 5 minutes // Proc. ACM International Symposium on Automated Analysis-Driven Debugging. 2005. P. 3–12.
5. *Nagai E., Hashimoto A., Ishiura N.*: Reinforcing Random Testing of Arithmetic Optimization of C Compilers by Scaling up Size and Number of Expressions // IPSJ Transactions on System LSI Design Methodology. 2014. V. 7. P. 91–100.
6. *Ливинский В.Ю., Митрохин А.В., Бабокин Д.Ю*. Исследование методов автоматической генерации случайных программ для тестирования компиляторов языков C/C++ // Труды 58-й научной конференции МФТИ, 2015.
7. *Ливинский В.Ю., Митрохин А.В., Бабокин Д.Ю*. Yet Another Random Program Generator - генератор случайных тестов для верификации оптимизаций в компиляторах языков C/C++ // Труды 59-й научной конференции МФТИ, 2016.

Б4УДК 004.428.2

Оптимизация маппинга процессов MPI-программ на кластеры с интерконнектом «Ангара» с помощью алгоритмов разбиения графов

М.Р. Халилов[2], А.В. Тимофеев[1,2,3]

[1]Объединенный институт высоких температур РАН
[2] Национальный исследовательский университет «Высшая школа экономики»
[3]Московский физико-технический институт

Интерконнект «Ангара» [1] является относительно новым отечественным продуктом на рынке высокопроизводительных коммуникационных сетей, но по своим характеристикам данная сеть сравнима со своими зарубежными аналогами, а по ряду параметров даже превосходит их. Для вычислительных кластеров (ВК), использующих интерконнект «Ангара», также имеется специальная реализация MPI [2], представляющая собой адаптированную для данной сети версию MPICH.

На данный момент на ВК с сетью «Ангара» MPI-программы запускаются без учёта особенностей их физической топологии, её иерархии и пропускной способности каналов передачи данных, поскольку текущая реализация MPI на таких кластерах предусматривает линейное отображение MPI-процессов на доступные узлы/ядра процессоров. Данное обстоятельство приводит к увеличению времени выполнения алгоритмов и большим накладным расходам, по сравнению с запуском параллельных программ с использованием

оптимального отображения процессов. Исходя из этого, вопрос, связанный с реализацией программных средств для оптимального отображения MPI-программ на ВК с сетью «Ангара», становится особенно актуальным, а метод оптимизации, описанный в данной работе, позволяет уменьшить время выполнения ряда задач, разработанных с использованием реализаций стандарта MPI.

Идея модернизированного метода оптимизации отображения параллельной программы, основанная на методах из работ [3, 4], заключается в разбиении информационного графа программы на непересекающиеся подмножества интенсивно обменивающихся процессов и привязке этих подмножеств к узлам/процессорам, соединённым наиболее быстрыми каналами связи. Разбиение выполняется для минимизации суммы рёбер, соединяющих разные подмножества разбиения. Разбиение рекурсивно выполняется сначала для уровня, описывающего обмены между вычислительными узлами, а затем для уровня, описывающего обмены внутри каждого из узлов в случае, если внутри узла установлено несколько процессоров. Целью такого разбиения является минимизация времени выполнения программы. Задача разбиения графа является NP-полной. Для её решения целесообразно использовать эвристические алгоритмы дающие решения, близкие к оптимальным.

Организация разбиения информационного графа осуществляется при помощи API-библиотеки разбиения графов METIS [5]. В METIS реализована многоуровневая схема Кариписа – Кумара (Karypis-Kumar, KK) [5] разбиения графов, в основе которой лежит алгоритм рекурсивной бисекции. Вычислительная сложность разбиения графа с использованием схемы KK составляет $T = O(|E|log_2(z))$, где E – количество рёбер в графе, а z – число подмножеств разбиения. Для получения субоптимального отображения необходимо $1 + N$ разных разбиений, где N – число узлов с ненулевым количеством процессоров.

Анализ результатов использования данного метода (рис. 1), реализованного в формате программной библиотеки, на тестах SP и LU из набора тестов производительности NAS Parallel Benchmarks и MPI «Ангара» показал уменьшение времени выполнения на тесте LU от 7% до 25% по сравнению со стандартным распределением процессов при использовании от 24 до 42 MPI-процессов соответственно. На тесте SP удалось достичь до 27% уменьшения времени выполнения при использовании 36 MPI-процессов.

Авторы благодарят коллег из НИЦЭВТа за предоставленный доступ к кластеру «Ангара-К1».

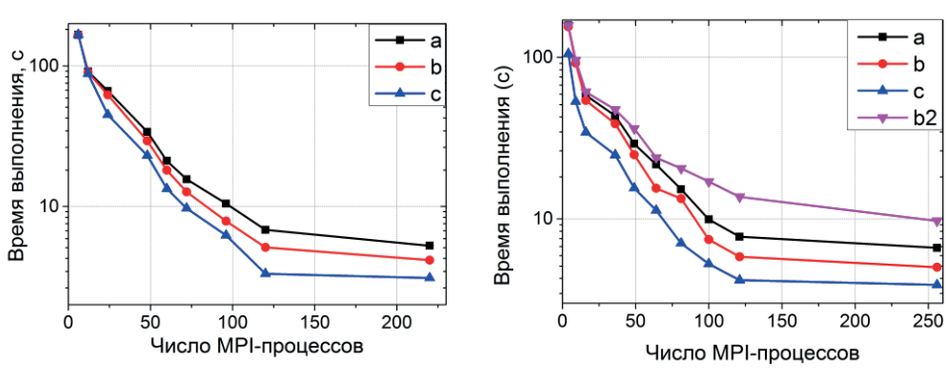


Рис. 1. Зависимость времени выполнения алгоритмов LU (слева) и SP (справа) NAS Parallel Benchmarks от числа MPI-процессов: a) без оптимизации, b) оптимизация с использованием тех же ресурсов, что и во время профилирования, b2) худший вариант случайного отображения, c) оптимизация с использованием всех доступных ресурсов ВК

Литература

1. *Агарков А.А., Исмагилов Т.Ф., Макагон Д.В., Семенов А.С., Симонов А.С.*. Результаты оценочного тестирования отечественной высокоскоростной коммуникационной сети Ангара // Суперкомпьютерные дни в России // Труды международной конференции (26–27 сентября 2016 г., г. Москва). М.: МГУ, 2016. С. 626–639.

2. *MPI Forum*. MPI: A Message-Passing Interface Standard Version 3.1.[Электронный ресурс] URL: mpi-forum.org/docs/mpi-3.1/mpi31-report.pdf
3. *Пазников А. А., Курносов М.Г., Куприянов М.С.* Многоуровневые алгоритмы отображения параллельных MPI-программ на вычислительные кластеры // Проблемы информатики. 2015. Т. 1. С. 4–17.
4. *Hoefler T., Snir M.* Generic topology mapping strategies for large-scale parallel architectures // Proceedings of the international conference on Supercomputing. ACM. 2011. С. 75–84.
5. *Karypis, G. and Kumar, V.* 1998. A Fast and High Quality Multilevel Scheme for Partitioning Irregular Graphs // SIAM Journal on Scientific Computing. 1999. V. 20, N. 1. P. 359–392.

УДК 004.4

Новый подход к созданию сетевых функций

***И.В. Филиппов*[1,2], *А.Ф. Мелик-Адамян*[1]**

[1]Intel

[2]Московский физико-технический институт (государственный университет)

В настоящее время компьютерные сети, помимо пересылки пакетов, выполняют множество задач. К таким задачам можно отнести трансляцию сетевых адресов из локальных в глобальные, систему обнаружения вторжений, систему предотвращения DDOS-атак, глубокая обработка пакета, Firewall и множество других. Такие сетевые задачи называются *сетевыми функциями*.

Исторически сложилось, что такие задачи выполнялись так называемыми middle-box – *специализированным оборудованием*, используемым только для конкретной задачи. У некоторых провайдеров более двадцати таких устройств, соединённых последовательно. Этот подход показал свою неэффективность: дорогое специализированное оборудование, отсутствие гибкости из-за жёстко заданных функций (bump-on-the-wire подход), отсутствие масштабируемости – необходимо всегда иметь максимальное количество оборудования, которое обычно простаивает.

Для решения данных недостатков несколько лет назад появилась концепция виртуализации сетевых функций – NFV [1]. Она предполагает создание сетевых функций не в аппаратуре, а как программ, выполняющихся на аппаратуре широкого назначения. Такое решение дешевле, оркестрируется внутри виртуальных машин или контейнеров и эластично использует предоставляемые ресурсы в зависимости от нагрузки.

Однако создание NFV функций является трудоёмкой задачей: с одной стороны, оно включает в себя низкоуровневые оптимизации, с другой стороны, существуют требования по быстрому прототипированию и внесению изменений, что подразумевает высокуровневые абстракции.

Предлагаемый подход сочетает в себе оба данных требования. Первым шагом предлагаемого подхода является переход от декларативной семантики к семантике исполнения, что означает, что результатом подхода является исполняемый файл. Вторым шагом предлагаемого подхода является построение сетевой функции путём последовательного соединения предопределённых блоков, каждый из которых выполняет конкретную задачу. Вместе данные блоки образуют граф обработки пакетов, строящийся статически перед началом выполнения. Пакеты проходят граф и обрабатываются блоками – функциями. Третий шаг – высокоуровневая настройка (customization) при низкоуровневой оптимизации. Некоторые функции в графе обработки пакетов допускают в качестве параметра пользовательскую функцию, которой будет передан каждый пришедший пакет. Пользователю необходимо только написать функцию, принимающую на вход указатель или вектор указателей на пакеты. Ему не надо задумываться о параллельном доступе к памяти, потоках, кэше, prefetch, драйверах, ядрах и так далее. Все низкоуровневые оптимизации уже реализованы в предопределённых блоках. Такой подход ускоряет создание сетевых функций без потери производительности. Четвёртый шаг нашего подхода – масштабирование в рамках одной машины. Если определённая пользователем функция слишком медленная, она будет склонирована на соседнее ядро

автоматически. При падении потока пакетов клоны будут удалены для достижения эластичности.

Для оценки предложенного подхода был реализован проект YANFF [2] – Yet Another Network Function Framework, использующий язык GO и библиотеку DPDK. Как показали тестовые сценарии, YANFF уменьшает количество кода в пользовательских приложениях в несколько раз, уменьшает затрачиваемое на разработку время и обеспечивает автоматическое масштабирование при незначительных потерях пропускной способности относительно написания такой же сетевой функции на чистом DPDK.

Литература

1. *ETSI.* «Network Function Virtualization» white paper. 2012.
2. Yet Another Network Function Framework. 2017. https://github.com/intel-go/yanff

УДК 004.051

Применимость процессорной архитектуры Epiphany для реализации параллельного алгоритма классической молекулярной динамики

***В. Никольский*[1,2], *В. Стегайлов*[1,2,3]**

[1] Национальный исследовательский университет «Высшая школа экономики»
[2] Объединенный институт высоких температур РАН
[3] Московский физико-технический институт (государственный университет)

Увеличение вычислительной мощности современных суперкомпьютеров связано со значительными трудностями. Причина кроется в том, что производство процессоров близко к достижению физических пределов и дальнейшее увеличение плотности транзисторов на кристалле ограничено. На сегодняшний день наиболее реализуемым решением этой проблемы видится *наращивание параллелизма*. Некоторые исследователи рассматривают архитектуру Parallella как перспективную для создания суперкомпьютера экзафлопсного класса [1].

При создании массово-параллельных систем на базе современной элементной базы энергопотребление становится существенным ограничением масштабируемости и для создания суперкомпьютеров нового поколения оно должно быть многократно уменьшено. В наших предыдущих работах мы оценивали энергоэффективность процессоров архитектуры Arm [2–4], систем-на-чипе с графическими ускорителями [3–4], строили модели их вычислительной эффективности при решении задач молекулярной динамики. Отдельное внимание мы уделили определению пиковой производительности процессоров с набором инструкций ARMv8 [5].

В этой работе мы развиваем поход и исследуем свойства новой массово-параллельной процессорной архитектуры. В работе используется платформа Parallella с чипом Epiphany, которая может масштабироваться до 4096 вычислительных ядер, объединенных высокоскоростной сетью-на-чипе. Каждое отдельное ядро совмещено с небольшим объемом быстрой памяти, управляемой программистом, но лишено кэша. Такая архитектура значительно сокращает энергопотребление и позволяет создавать эффективные параллельные коды. Подобный подход используется в суперкомпьютере Sunway TaihuLight, занимающем первое место в списке Top500 на сегодняшний день.

В нашей работе представлены первые результаты адаптации молекулярно-динамического кода для новой массово-параллельной энергоэффективной архитектуры Epiphany. Сделан обзор используемых технологий, подходов и библиотек (в том числе модель программирования с разделенным глобальным адресным пространством, библиотеки OpenSHMEM, coprthr). Производятся первые оценки энергопотребления системы.

Литература

1. http://wgropp.cs.illinois.edu/bib/talks/tdata/2017/mpix-exascale-ppam.pdf

2. *Nikolskiy V. and Stegailov V.* Floating-point performance of ARM cores and their efficiency in classical molecular dynamics // Journal of Physics: Conference Series. 2016. V. 681, N. 1. P. 012049.
3. *Nikolskiy V.P., Stegailov V.V., Vecher V.S.* Efficiency of the Tegra K1 and X1 Systems-on-Chip for Classical Molecular Dynamics // Proceedings of the 14th International Conference on High Performance Computing & Simulation (HPCS-2016), Innsbruck, 2016. P. 682–689. DOI: 10.1109/HPCSim.2016.7568401
4. *Nikolskii V., Vecher V., Stegailov V.* Performance of MD-algorithms on hybrid systems-on-chip Nvidia Tegra K1 & X1 // Supercomputing. RuSCDays 2016. Communications in Computer and Information Science. Revised Selected Papers. 2016. V. 687. P. 199–211.
5. *Никольский В.П., Стегайлов В.В.* Как приблизиться с пиковому значению Flops/s? Сравнение архитектур x86 и ARMv8 // Труды международной конференции «Суперкомпьютерные дни в России». 2017. С. 595–606.

УДК 004.318

Алгоритмы сжатия данных в кэш-памяти микропроцессоров

А.С. Кожин

Московский физико-технический институт (государственный университет)
АО «МЦСТ»

Современные микропроцессоры имеют многоуровневую иерархию кэш-памяти, которая позволяет повысить пропускную способность и уменьшить среднее время доступа к данным, обладающим пространственной и временной локальностью. Среднее время доступа зависит от коэффициента попаданий в кэш-память и от времени доступа в кэш-память и оперативную память. Увеличение объема кэш-памяти позволяет повысить коэффициент попаданий, хотя может увеличить ее время доступа. В современных микропроцессорах суммарный объем кэш-памяти может достигать десятков и даже сотен мегабайт. При этом основными факторами, ограничивающими максимальный объем кэш-памяти, являются площадь кристалла и рассеиваемая мощность.

Сжатие данных может повысить эффективный объем хранимой информации. В современных вычислительных системах есть примеры использования сжатия в оперативной памяти [1], однако сжатие данных в кэш-памяти до сих пор не применяется в серийных микропроцессорах, хотя исследования на эту тему ведутся достаточно давно [2]. Основные трудности практического применения алгоритмов сжатия в кэш-памяти связаны с необходимостью изменить устоявшуюся структуру кэш-памяти, а также с достаточно большими накладными расходами и увеличением времени доступа при сложной декомпрессии.

Большинство алгоритмов реализуют сжатие отдельных блоков – кэш-строк – и размещают большее количество кэш-строк при увеличении (обычно при удвоении) числа хранимых адресных тэгов. Сложные алгоритмы обеспечивают высокую степень сжатия, до двух раз увеличивая эффективный объем хранимой в кэш-памяти информации на задачах с подходящей структурой данных. В то же время сложные алгоритмы требуют громоздких вычислений при декомпрессии и существенно увеличивают время доступа в кэш-память, поэтому могут замедлить выполнение задач, которые не относятся к категории «Cache Friendly» [3], и задач с низкой степенью сжатия рабочих данных. В качестве примеров выбраны алгоритмы FPC [4] и C-Pack [5]. В основе алгоритма FPC лежат разбиение кэш-строки на фиксированные сегменты и проверка этих сегментов по распространенным шаблонам. Более эффективный алгоритм C-Pack дополняет сжатие по статическим шаблонам динамическим сжатием. В обоих алгоритмах декомпрессия выполняется последовательно, поэтому имеет достаточно большую задержку (5–8 тактов на частоте 2 ГГц и технологии 28 нм).

Более простые для реализации алгоритмы имеют меньшую степень сжатия, но при этом не увеличивают время доступа в кэш-память благодаря быстрой декомпрессии. Эти алгоритмы больше подходят для реализации в серийных микропроцессорах, так как

требуют меньших ресурсов и могут обеспечить работу без ухудшения производительности на любых задачах. Алгоритм ZCA [6] выделяет специальное расширение кэш-памяти для нулевых кэш-строк, в котором хранит только их адресные тэги и состояния. Такой подход не требует никакого дополнительного времени на декомпрессию, но обеспечивает невысокую степень сжатия. Алгоритм BDI [7] разбивает кэш-строку на одинаковые сегменты и проверяет, можно ли их представить как дельты меньшего размера относительно выбранного базового сегмента. Декомпрессия выполняется параллельно во всех сегментах и добавляет всего один такт ко времени доступа в кэш-память.

В работе проведены анализ и сравнение методов сжатия данных в кэш-памяти микропроцессоров. Показано, что метод BDI имеет наибольшую эффективность для практического применения. Представлены результаты исследований с использованием прототипа микропроцессора с архитектурой Эльбрус.

Литература

1. *Abali B., Franke H., Poff D.E., Saccone R.A., Schulz C.O., Herger L.M., Smith T.B.* Memory expansion technology (MXT): software support and performance // IBM Journal of Research and Development. 2001. V. 45, N 2. P. 287–301.
2. *Sardashti S., Arelakis A., Stenström P., Wood D.A.* A primer on compression in the memory hierarchy // Synthesis Lectures on Computer Architecture. 2015. V. 10, N 5. P. 1–86.
3. *Кожин А.С., Нейман-заде М.И., Тихорский В.В.* Влияние подсистемы памяти восьмиядерного микропроцессора «Эльбрус-8С» на его производительность // Вопросы радиоэлектроники. 2017. № 3. С. 13–21.
4. *Alameldeen A.R., Wood D.A.* Adaptive cache compression for high-performance processors // Computer Architecture, 2004. Proceedings. 31st Annual International Symposium on. IEEE, 2004. P. 212–223.
5. *Chen X., Yang L., Dick R.P., Shang L., Lekatsas H.* C-pack: A high-performance microprocessor cache compression algorithm // IEEE transactions on very large scale integration (VLSI) systems. 2010. V. 18, N 8. P. 1196–1208.
6. *Dusser J., Piquet T., Seznec A.* Zero-content augmented caches // Proceedings of the 23rd international conference on Supercomputing. ACM, 2009. P. 46–55.
7. *Pekhimenko G.., Seshadri V., Mutlu O., Gibbons P.B., Kozuch M.A., Mowry T.C.* Base-delta-immediate compression: Practical data compression for on-chip caches // Proceedings of the 21st international conference on Parallel architectures and compilation techniques. ACM, 2012. P. 377–388.

УДК 004.051

Сравнение работы библиотек для быстрого преобразования Фурье FFTW и EML на вычислительном сервере с процессорами «Эльбрус-4С»

***Д.О. Дергунов*[1,2], *А.В. Тимофеев*[1,2,3]**

[1]Объединённый институт высоких температур РАН
[2]Национальный исследовательский университет «Высшая школа экономики»
[3]Московский физико-технический институт (государственный университет)

Работа посвящена исследованию эффективности работы алгоритмов дискретного преобразования Фурье (ДПФ) библиотек fftw и eml на вычислительном сервере с процессорами «Эльбрус-4С». Обе библиотеки содержат реализацию алгоритма Кули–Тьюки быстрого преобразования Фурье (БПФ) для вектора размерности $N = 2^m$, выполняющих ДПФ за $O(N \cdot log(N))$операций [1].

Микропроцессор «Эльбрус-4С» построен в соответствии с архитектурой «Эльбрус», особенность которой заключается в том, что анализ зависимостей и оптимизация порядка операций происходят на уровне компиляции. Поступающие на вход процессору «широкие команды» [2] могут заключать в себе до 23 операций, выполняемых за один такт. Данную особенность можно использовать в задачах с большим количеством подзадач, которые можно выполнять параллельно. Ярким примером задачи с большим

количеством операций, которые можно выполнить параллельно, является алгоритм Кули–Тьюки БПФ.

Библиотеки eml и fftw имеют схожий подход в выполнении БПФ, происходящего в два этапа. Первый заключается в создании «плана», который можно использовать многократно для векторов одинаковой размерности $N = 2^m$. Затем для выполнения алгоритма соответствующей функции нужно передать входной вектор и подготовленный «план».

Библиотека fftw предлагает три флага для инициализации алгоритма: FFTW_ESTIMATE, FFTW_MEASURE, FFTW_PATIENT. Они отличаются временем подготовки (от быстрого к медленному) и временем выполнения подготовленного алгоритма (от медленного к быстрому). eml предлагает только один вариант для инициализации алгоритма.

Измерение времени работы алгоритма заключается в измерении времени подготовки «плана» и измерении однократного применения алгоритма по отдельности. Рассмотрено одномерное ДПФ над входным вектором действительных чисел размерности от 4 до 16777216 и вектором комплексных чисел на выходе. В качестве входных сигналов были приняты белый, розовый и красный шумы. По полученным результатам измерений построена зависимость времени работы алгоритмов от размерности входного вектора.

Анализ результатов показал, что время, затраченное на подготовку «плана» для реализации алгоритма eml значительно меньше, чем fftw в любом из режимов, для представленных размеров входного вектора (рис. 1). Тем не менее, для малых значений входного вектора (от 4 до 4096) алгоритм eml затратил больше времени, чем fftw в любом из режимов, для векторов размером 8192 и 16384 все алгоритмы показывают схожую производительность (рис. 2). С дальнейшим ростом N eml показывает меньший темп роста времени выполнения, чем любой из режимов fftw (рис. 2). Также стоит заметить, что по-разному подготовленные алгоритмы fftw крайне незначительно различаются по времени выполнения (рис. 2), при этом имеют различия по времени подготовки для размера входного массива больше 16 (рис. 1).

Можно заключить, что при работе с векторами размерности более 2^{12} eml эффективнее на обоих этапах; при меньших размерах стоит делать заключения, основываясь на информации, сколько раз в задаче нужно проводить ДПФ для векторов одной размерности. Если один «план» используется < 200 раз, то лучше использовать eml, в противном случае fftw с режимом FFTW_ESTIMATE.

Авторы благодарят В.В. Стегайлова за неоценимую помощь в работе и МЦСТ за предоставленный доступ к вычислительному серверу с процессорами «Эльбрус 4С».

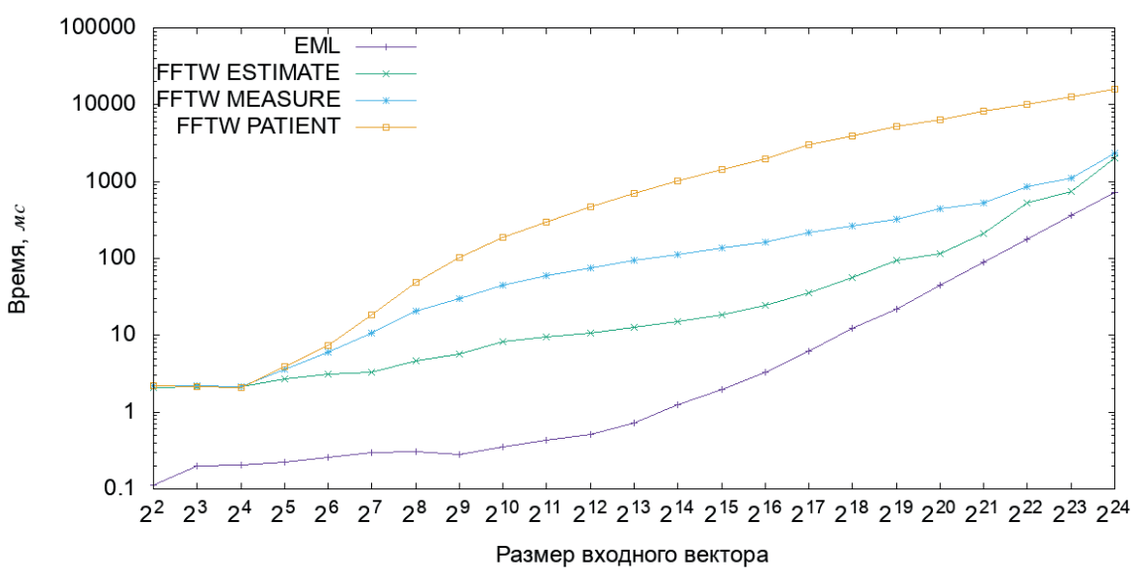


Рис. 1. Время подготовки «плана» для входного вектора размером от 4 до 16777216 библиотекой eml и библиотекой fftw с различными флагами

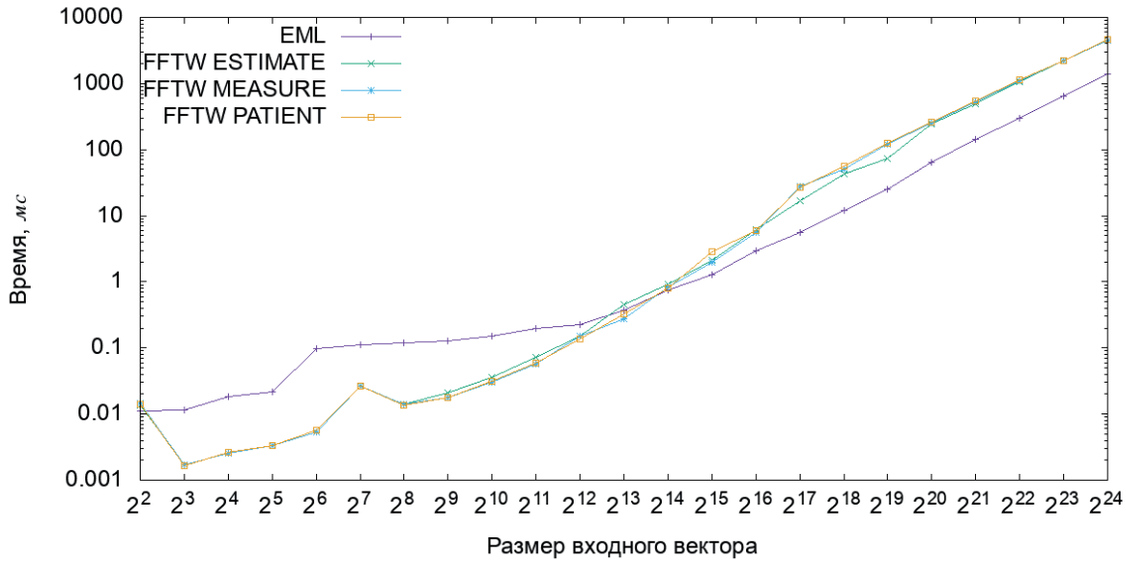


Рис. 2. Время разового выполнения одномерного БПФ над вектором действительных чисел библиотеками eml и fftw (красный шум)

Литература

1. *Cormen T.H., Leiserson C.E., Rivest R.L., Stein C.* Introduction to Algorithms. Third Edition. — The MIT Press, 2009. С. 906–922.
2. *Ким А.К., Перекатов В.И., Ермаков С.Г.* М59 Микропроцессоры и вычислительные комплексы семейства «Эльбрус». СПб.: Питер, 2013. С. 88–93.

Секция интегрированных киберсистем

УДК 519.688

Разработка системы календарного планирования и построения расписаний производственных процессов на НПЗ

М.В. Городнова[1,2], А.И. Коннов[3]

[1]Московский физико-технический институт (государственный университет)
[2]ООО «Центр цифровых технологий»
[3]ЗАО «Хоневелл»

Работа посвящена разработке системы SKARD – имитационной системы календарного планирования и построения расписаний производственных процессов на нефтеперерабатывающем заводе (НПЗ). В отличие от задачи оптимального производственного планирования (текущего планирования), решением которой является составление объемного плана производств на месяц (квартал), разработка такой системы до сих пор остается актуальной. Для решения задач по автоматизации построения календарного плана и расписания привлекаются разнообразные методы прикладной математики (линейного, нелинейного, динамического программирования и др.). Однако применить на практике методы оптимизации календарного плана не всегда является возможным из-за сложности математических моделей и невозможности решения их за приемлемое время. Предлагаемое в работе имитационное моделирование позволяет автоматизировать принятие решений в области составления расписаний задач такой размерности, при которой модели математического программирования не могут быть применены. Объемный план производства, который является решением задачи текущего планирования, включает суммарную оценку количества перерабатываемого сырья, количества производимых продуктов и загрузки установок, которые максимизируют прибыль завода на рассматриваемом промежутке времени (обычно месяц). Календарный план работы завода (план по суткам) и расписание работы завода (почасовой план производства) составляются на основе решения предыдущей задачи с учетом существенных ограничений завода, не учитываемых при решении задачи текущего планирования, таких как скорости потоков, длительность проведения анализов для паспортизации резервуаров, ограничения емкости резервуаров и многие другие. Решением такой задачи должен быть допустимый план производства, который включает в себя объем перекачек между узлами потоковой схемы для каждого периода, равного суткам или часу, и который удовлетворяет всем многочисленным ограничениям модели.

Для решения поставленной задачи выбран имитационный подход [1]. Он заключается в построении имитационной модели выбранного участка производства, включающей в себя отдельные описания узлов потоковой схемы участка в виде настраиваемых, управляющих и зависимых параметров. Настраиваемые параметры – это статические параметры модели, известные данные, которые задаются перед началом поиска решения. Примером таких параметров являются максимальные и минимальные уровни резервуаров, длительность проведения анализов для паспортизации продукта, скорости перекачек насосов и т.д. Управляющие параметры – неизвестные параметры модели, именно их нужно определить для построения плана для каждого периода планирования. Например, объемы налива готовой продукции в резервуары назначения, объемы отгрузки из резервуаров налива. Зависимые параметры описывают вычисляемые параметры модели, полностью определяемые значениями других параметров. Например, текущий уровень резервуара выражается через уровень этого резервуара в предыдущий период и управляющих параметров, отвечающих за исходящие и входящие перекачки. Еще одним примером зависимых параметров являются вспомогательные параметры – параметры, предназначенные для облегчения поиска решения. Например, объем продукта, который еще

можно налить в резервуар, избежав при этом переполнения.

Система SKARD служит для автоматического создания имитационных моделей работы отдельных производственных участков НПЗ исходя из их потокового описания, дальнейшего нахождения с ее помощью плана производства, а также представления решения в виде графиков и отчетов. Для системы разработана библиотека объектов, которые описывают поведение соответствующих технологических объектов, именно на их основе поддерживается автоматическое построение имитационной модели в соответствии с потоковым описанием. Система реализована на языке C#, имеет графический интерфейс пользователя, основанный на представлении имитационных моделей в виде таблиц (рис. 1). Все данные модели при этом расположены в ячейках таблиц. Строки таблиц соответствуют периодам времени, а столбцы соответствуют параметрам модели. При изменении данных в ячейке управляющего параметра происходит автоматический пересчет всех параметров модели, зависящих от него. При этом если изменение управляющего параметра привело к нарушению ограничения модели, например слишком большая перекачка в резервуар привела к его переполнению, система отобразит эту ошибку в протоколе решения, а также в самой таблице окрашиванием данных в красный цвет. Данные модели объединены в соотвествующие таблицы таким образом, чтобы нагляднее представить отдельные узлы потоковой схемы и облегчить процесс ручного редактирования управляющих параметров.

Построение планов в системе SKARD осуществляется при помощи решателей, использующих эвристические алгоритмы, основанные на методе решающих правил [2]. Эвристические алгоритмы используют различные разумные соображения без строгих обоснований и позволяют формировать рациональное (не оптимальное) решение задачи планирования и построения расписаний за короткий промежуток времени. Формирование нужных решающих правил для конкретной задачи происходит при многократном ручном поиске ее решения, а также на основе знаний эксперта в заданной области путем алгоритмического описания подходов, приводящих к допустимому решению задачи. После нахождения плана при помощи одного из таких решателей пользователь имеет возможность вручную изменить необходимые управляющие параметры для модификации автоматически найденного решения.

Разработанная система позволяет автоматизировать процесс посуточного и почасового плана производства на отдельных участках НПЗ и находить решение за приемлемое время. На данный момент система поддерживает построение имитационных моделей товарно-сырьевого парка [3] и первичной обработки нефти. В дальнейшем планируется разработка библиотек объектов для создания моделей смешения, а также поддержка создания плана на основе диаграмм Ганта.

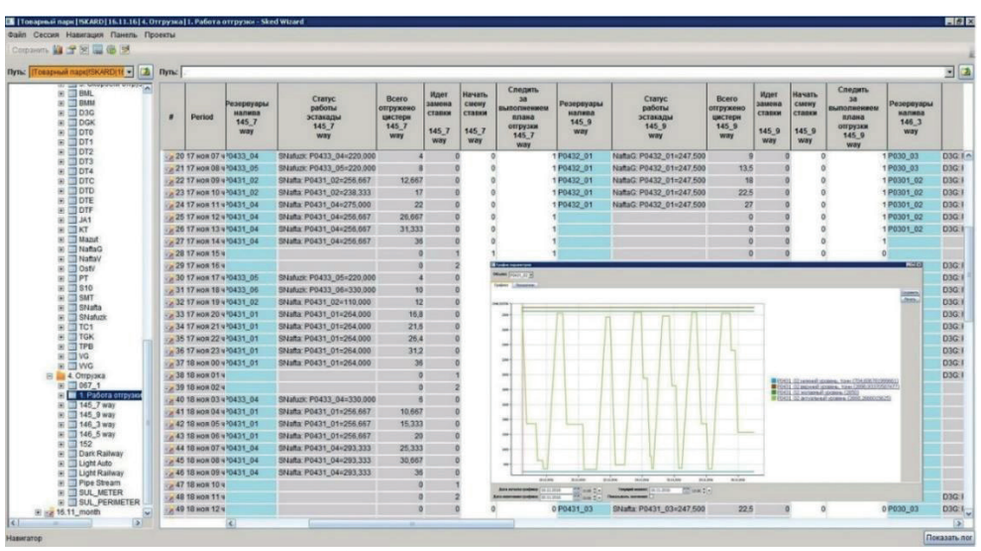


Рис. 1. Интерфейс пользователя системы SKARD

Литература

1. *Проказина М.В., Хохлов А.С., Шайдуллин Р.А.* Имитационные модели в комплексе календарного планирования производства НПЗ // Автоматизация в промышленности. 2012. Н. 10. С. 15–21.
2. *Проказина М.В.* Имитационные модели и методы решающих правил для задачи построения расписаний работ на НПЗ // Труды 58-й научной конференции МФТИ. Аэрофизика и космические исследования. 23–28 ноября 2015. С. 195.
3. *Проказина М.В., Шайдуллин Р.А.* Имитационная модель календарного планирования товарно-сырьевого парка НПЗ // Управление большими системами: материалы X Всероссийской школы-конференции молодых ученых. 2013. Т. 3. С. 257–260.

УДК 517.977.1

Исследование границ применимости алгоритмов управления на основе прогнозирующей модели в условиях неопределенности

А.А. Черешко

Московский физико-технический институт (государственный университет)

Одним из современных формализованных подходов к анализу и синтезу систем управления, базирующихся на математических методах оптимизации, является теория управления динамическими объектами с использованием прогнозирующих моделей Model Predictive Control (MPC). Для MPC на настоящий момент не существует методов, позволяющих аналитически оценить робастную устойчивость МП-контроллера (многопараметрического) по коэффициентам прогнозирующей модели. В литературе, однако, есть многочисленные рекомендации, как путем модификации имеющегося неустойчивого контроллера получить устойчивый [1]. В данной работе такой подход рассматриваться не будет, так как целью исследования является именно оценка устойчивости, имеющегося при рассогласовании параметров модели и реального процесса. Актуальность такого исследования обусловлена тем, что зачастую параметры реального процесса не остаются постоянными во времени: физические устройства технологического процесса подвержены старению, внешним изменениям и модификациям. Таким образом, по мере увеличения времени от внедрения МП-контроллера на производстве накапливается рассогласование между параметрами модели MPC и параметрами процесса, что в конечном счете может привести к дестабилизации контура управления.

В данной работе введён критерий применимости управления, согласно которому исследованы области стабильной работы контроллера (рис. 1).

В качестве передаточной функции объекта выбрано апериодическое звено:

$$F(s) = \frac{K}{Ts+1}.$$

В качестве передаточной функции прогнозирующей модели МП-контроллера выступило следующее уравнение:

$$\hat{F}(s) = \frac{K\prime}{T\prime s+1}.$$

Математически задача MPC-управления ставится следующим образом. Пусть математической моделью объекта управления служит система обыкновенных нелинейных дифференциальных уравнений вида

$$\dot{\mathbf{x}}(t) = f\left(t, \mathbf{x}(t), \mathbf{u}(t)\right),\ \mathbf{x}(0) = \mathbf{x}_0$$

где $\mathbf{x}$ – вектор состояний размерности n, а $\mathbf{u}$ – вектор управления размерности m. На компоненты векторов состояний и управления могут быть наложены ограничивающие условия. Будем считать, что целью управления будет являться обеспечение равенств

$$\lim_{t\to\infty}\left\|\mathbf{x}(t) - \mathbf{r}_x(t)\right\| = 0,\ \lim_{t\to\infty}\left\|\mathbf{u}(t) - \mathbf{r}_u(t)\right\| = 0.$$

Здесь заданные векторные функции определяют некоторую желаемую динамику объекта (r(t) – задающий сигнал). Качество управления при этом будет оцениваться с использованием целевой функции $J\left(\mathbf{x}(t), \mathbf{u}(t)\right)$, заданной на управляемых движениях

объекта. Задача оптимального управления состоит в том, чтобы найти управление, обеспечивающее выполнение целей управления с учетом ограничений, и дополнительно доставляющее минимум функционалу *J*. Для решения задачи управления используется прогнозирующая модель процесса. Она, как правило, не совпадает с исходной, так как невозможно точно проидентифицировать последнюю:

$$\dot{\bar{\mathbf{x}}}(\tau) = f\left(\tau, \bar{\mathbf{x}}(\tau), \bar{\mathbf{u}}(\tau)\right),\ \bar{\mathbf{x}}(\tau)|_{\tau=t} = \mathbf{x}(t).$$

Считается, что на компоненты векторов $\bar{\mathbf{x}}(\tau)$ и $\bar{\mathbf{u}}(\tau)$ действуют те же ограничения, что и на компоненты векторов исходной модели.

Общая схема управления с предсказанием состоит из следующих действий:

1. Оценивание вектора состояния $\mathbf{x}(t)$ реального объекта.
2. Решение оптимизационной задачи $J\left(\mathbf{x}(t), \bar{\mathbf{u}}(t), T_p, T_c\right) \to \min$, где T_p – горизонт предсказания, T_c – горизонт управления.
3. Применение найденного оптимального управления в качестве программного на отрезке $t \in [t; t+\delta]$, где δ – интервал дискретизации системы (в данной задаче $\delta = 1$ мин).
4. Замена времени t на $t+\delta$ и повторение операций 1–3.

Наиболее широко распространенным видом целевой функции *J* является квадратичный функционал вида [2]:

$$J = \int_0^{\infty} \left[\left(\mathbf{x}(t) - \mathbf{r}(t)\right)^T \mathbf{R}\left(\mathbf{x}(t) - \mathbf{r}(t)\right) + \lambda^2 \mathbf{u}^T(t) Q \mathbf{u}(t) \right] dt.$$

Здесь считается $\mathbf{r}_u(t) = 0$. В случае если целевая функция задана в виде квадратичного функционала, а прогнозирующая модель линейная, задача поиска оптимального управления сводится к задаче линейно-квадратичного программирования с ограничениями. R и Q – диагональные матрицы с весовыми коэффициентами.

Также полезно представить здесь дискретную математическую постановку задачи управления на основе прогнозирующего управления, т.к. именно в дискретном виде она решается в промышленных контроллерах:

$$x[k+1] = Ax[k] + Bu[k],\ x[0] = x_0,$$

$$J[k] = \sum_{i=1}^{p} w_i \left(x[k+i \mid k] - r[k+i \mid k]\right)^2 + \sum_{i=1}^{c} r_i \Delta u[k+i-1 \mid k]^2 \to \min_{u[k|k],\ldots u[k+p-1|k]},$$

$$u_{\min} \le u[k+i-1 \mid k] \le u_{\max},\ i = 1,\ldots c,$$

$$-\Delta u_{\max} \le \Delta u[k+i-1 \mid k] \le \Delta u_{\max},\ i = 1,\ldots c,$$

$$x_{\min} \le x[k+i \mid k] \le x_{\max},\ i = 1,\ldots p.$$

Здесь c, p – соответственно горизонты управления и прогнозирования, выраженные в количестве шагов по времени, обозначение $x[i \mid j]$ читается как «значение *x* в момент времени *i*, подсчитанное в момент времени *j*».

Введём критерий применимости МП-регулятора. Будем считать, что МП-регулятор применим к управлению технологическим процессом, если при изменении регулируемой переменной на величину **d**:

-Управление устойчиво, т.е. для любого значения ошибки управления $\bar{e}$ найдется такое время $\acute{t}$, когда текущая ошибка управления e меньше заданной ошибки $\bar{e}$.

$$\forall\, \bar{e} > 0\ \exists \acute{t}: \forall\, t > \acute{t}\ \to e < \bar{e}.$$

-Не позднее времени 10 × **T**, ошибка управления всегда не превышает **d** × 0.05 (5-процентая сходимость).

В результате расчетов была получена область устойчивости в двухмерном пространстве с осями **T'/T**, **K'/K**, изображение которой приведено на рис. 1.

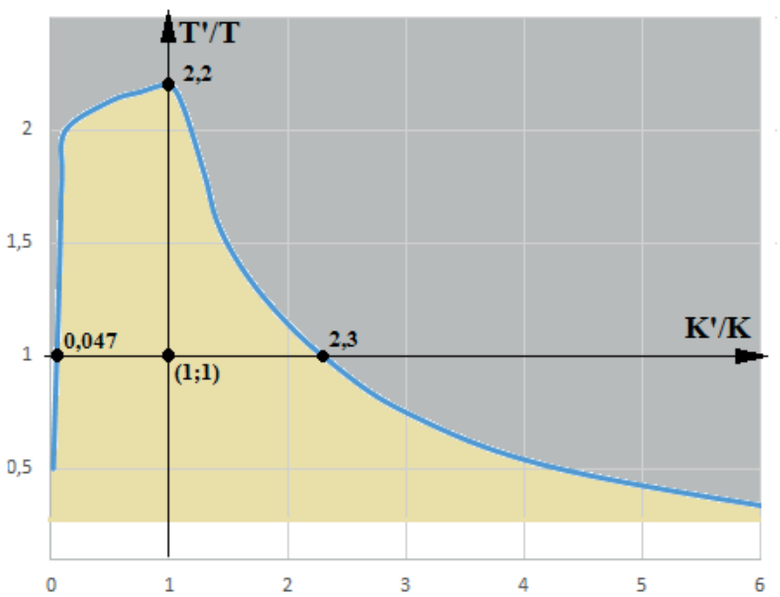


Рис. 1. Области, в которых критерий применимости выполняется (внутри) или не выполняется (снаружи)

На рис. 1 **T'/T** – отношение, показывающее степень ошибки определения коэффициента **T**, а **K'/K** показывает степень ошибки определения коэффициента **K** передаточной функции объекта.

Полезным явлением для МП-контроллера является наличие «безопасных» направлений, что позволяет облегчить выбор в условиях неопределенности при реализации контроллера в промышленной системе. Судя по рис.1, при большой ошибке определения коэффициента **K'** для корректной работы рекомендуется снизить коэффициент **T'** и перейти в устойчивое управление.

Литература

1. *Никифоров В.О.* Адаптивное и робастное управление с компенсацией возмущений. СПб: Наука, 2003. 282 с.
2. *Kothare M V., Balakrishnan V. and Morari M.* Robust constrained model predictive control using linear matrix inequalities // Automatica. 1996. V. 32, N 10, P. 1361–1379.

УДК 65.658.5

Разработка и применение архитектурных моделей системного проектирования

В.В. Кондратьев, Л.А. Хачатуров, Н.А. Кожевников

Московский физико-технический институт (государственный университет)

При создании высокотехнологичных продуктов сегодня применяют стандарты и методологии системного инжиниринга – ISO 15288, Geram, NASA и многие другие. Надо признать, что эти стандарты и методологии во многом не гармонизированы друг с другом. Актуальной является задача построения компактной формализованной «зонтичной» методологии, позволяющей путем локализации единого ядра референтных принципов и моделей единообразно представить и применить архитектурные модели различных методологий системного инжиниринга. В работе предлагается подход к решению этой задачи на основе методологии 2.0 [1–4].

Пусть *A* обозначает некоторую сущность искусственно созданной системы. Будем применять следующие архитектурные модели:

- Модели *ABS*, *A Breakdown Structure*. Это иерархические таксономии сущностей, построенные по принципу «сущность *A* состоит из сущностей $a1, a2, \ldots$».
- Модели матриц соответствия *DSM* (*A, B*), Design Structure Matrix сущностей $A = \{a_i\}$ и $B = \{b_j\}$. Это матрицы, задаваемые всеми соответствиями $a_i \times b_j$.
- Композитные архитектурные модели: задаются композициями (метаархитектурами) наборов сущностей, иерархических таксономий сущностей, матриц соответствия таксономий.

Как пример приведем локализацию описанной в [3] методологии системного проектирования технических систем.

Набор используемых в методологии сущностей: требования к технической системе, функции технической системы, техническая система и ее компоненты, работы по созданию технической системы и ее компонент.

Модели *BS*, иерархические таксономии сущностей: *RBS*, *Requirement BS* – иерархическая модель требований; *FBS*, *Function BS* – иерархическая модель функций; *PBS*, *Product BS* – иерархическая модель компонент; *WBS*, *Work BS* – иерархическая модель работ.

Модели *DSM*, матрицы соответствия сущностей: *DSM* (*RBS*, *FBS*) – соответствия требований и функций; *DSM* (*FBS*, *PBS*) – соответствия функций и компонент; *DSM* (*RBS*, *RBS*) – соответствия (компромиссы) требований; *DSM* (*FBS*, *FBS*) – взаимодействия функций; *DSM* (*FBS*, *PBS*) – функциональная архитектура технической системы; *DSM* (*PBS*, *PBS*) – связи и интерфейсы компонент; *DSM* (*PBS*, *WBS*) – соответствие компонент технической системы (результатов) и проектных работ по ее созданию; *DSM* (*WBS*, *WBS*) – потоковые модели процессов.

Референтная композиция/метамодель методологии системного проектирования [3] представлена на рис. 1.

Выводы

1. Предложен подход к компактному единообразному представлению композитных архитектурных моделей системного проектирования. На основе подхода построены представления метамоделей методологии системного проектирования [3], Geram, NASA. Решения применены при описании системных методологий в профильных дистанционных курсах по системному проектированию на платформах Coursera (USA: www.artofsystems.ru.) и Moodle (MIPT).
2. На основе разработанных решений началась поэтапная разработка облачного сервиса «Архитектурный конфигуратор»: этап 1 – «Рабочие панели для архитектурного моделирования, в дистанционных курсах»; этап 2 – «Сервисы концептуального архитектурного проектирования продуктов и систем деятельности высокотехнологичных предприятий».
3. Выход на модели *WBS* в цепочке моделей, представленных на рис. 1, позволяет на аналогичных принципах переходить к построению архитектурных моделей бизнес-процессов и систем менеджмента. Таким образом, создана возможность применения единообразного сквозного архитектурного моделирования от методологии системного инжиниринга до менеджмента и управления.

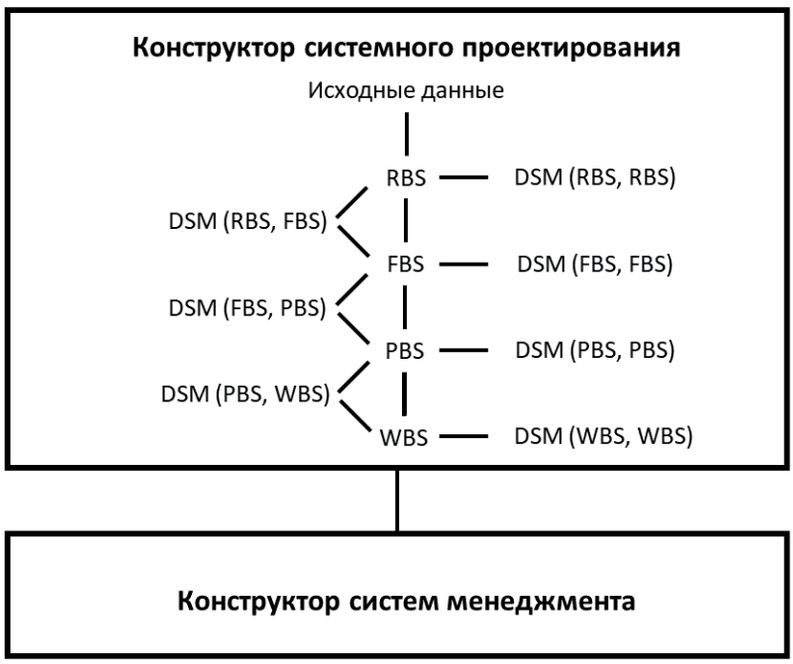


Рис. 1. Композитная архитектурная метамодель системного проектирования

Литература

1. *Новиков А.М.*, *Новиков Д.А.* Методология. М.: СИНТЕГ, 2007. 668 с.
2. *Новиков Д.А*. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. М.: ЛЕНАНД. 2016. 154 с.
3. *Романов А.А.* Прикладной системный инжиниринг. М.: Физматлит. 2015. 555 с.
4. *Кондратьев В.В.* Управление архитектурой предприятия: конструктор регулярного менеджмента. 2-е изд., перераб. и доп. М.: ИНФРА-М. 2015. 358 с.

УДК 681.5

Параметрическая идентификация моделей смешения качественных показателей дизельных топлив

А. Бурда

Московский физико-технический институт (государственный университет)

Одной из центральных проблем моделирования смешения товарных нефтепродуктов является нелинейное смешение ряда их качественных показателей. Вследствие нелинейного характера физико-химических закономерностей и наличия погрешности измерения свойств, построить идеально точную математическую модель принципиально невозможно. Поэтому для прогнозирования свойств нефтепродуктов используются эмпирические подходы. Нелинейные модели смешения свойств нефтепродуктов, которые могут быть найдены в научной и технической литературе, представляют собой зависимости свойств смеси от свойств ее компонентов. При построении таких моделей их параметры подбираются на основе имеющегося набора данных, что приводит к изменению точности метода при изменении набора данных.

В работе рассматриваются различные модели смешения качественных показателей дизельных топлив, сравнивается их точность на наборе актуальных данных российского нефтеперерабатывающего завода (НПЗ), а также ставится задача параметрической идентификации параметров этих моделей для повышения их точности. Линейные свойства дизельных топлив смешиваются следующим образом.

1. Линейный закон смешения:

$$P_B = \sum_{i=1}^{n} X_i P_i , \quad (1)$$

где P_B - значение свойства смеси, P_i – значение свойства i-го компонента в смеси, а X_i – доля i-го компонента в смеси, причем $\sum_{i=1}^{n} X_i = 1$. Плотность дизельных топлив смешивается линейно и для неё может применяться закон (1).

К основным нелинейным показателям качества дизельных топлив можно отнести температуры вспышки, помутнения и фильтруемости; цетановое число, вязкость и точки фракционного состава. При моделировании данных показателей качества дизельных топлив используются следующие модели смешения [1].

2. Индекс смешения:

$$BI_{P_i} = f(P_i), \quad (2)$$

$$BI_{P,B} = \sum_{i=1}^{n} BI_{P_i} X_i, \quad (3)$$

здесь BI_{P_i} – индекс свойства P_i для i-го компонента, а $BI_{P,B}$ – индекс смешения продукта. Тогда искомое свойство смеси можно получить, сделав следующее обратное преобразование:

$$P_{Blend} = f^{-1}(\sum_{i=1}^{n} f(P_i) X_i), \quad (4)$$

где f^{-1} – обратная функция преобразования, а P_{Blend} – значение свойства продукта.

В литературе [2] может быть найден явный вид функции f для каждого из показателей.

Формула индекса температуры вспышки имеет вид

$$FI = 10^{[a_1 - a_2\, lg(1{,}8F+492)]}, \quad (5)$$

где FI – индекс смешения температуры вспышки; F – температура вспышки, °С; a_1, a_2 – коэффициенты.

Формула индекса температуры помутнения и фильтруемости имеет вид

$$TI = [a_1(1{,}8T + 492)]^{a_2}, \quad (6)$$

где TI – индекс смешения температуры помутнения либо фильтруемости; T – температура помутнения либо фильтруемости, ºС; a_1, a_2 – коэффициенты.

Формула индекса вязкости имеет вид

$$BI_{\nu_i} = a_1 - a_2\, lg\, lg(\nu_i + a_3), \quad (7)$$

где BI_{ν_i} – индекс вязкости ν_i для i-го компонента, ν_i – вязкость i-го компонента в сСт при 40 ºС, a_1, a_2, a_3 – коэффициенты.

Формула индекса смешения цетанового числа имеет вид полинома второй степени:

$$CI = a_3 + a_2 * CN + a_1 * CN^2 , \quad (8)$$

где CI – индекс смешения цетанового числа, CN – цетановое число, a_1, a_2, a_3 – коэффициенты.

3. Метод Dupont

Метод интерактивных коэффициентов, или интерактивный метод корпорации Dupont, выражается следующей формулой:

$$P_{Blend} = P_1X_1 + P_2X_2 + \cdots + P_nX_n + a_{12}X_1X_2 + a_{13}X_1X_3 + \cdots + a_{n-1,n}X_{n-1}X_n , \quad (9)$$

где P_i – свойство i-го компонента, P_{Blend} – свойство смеси; X_i – концентрация i-го компонента в смеси ($\sum_{i=1}^{n} X_i = 1$); n – число компонентов; a_{ij} – интерактивный коэффициент.

Эта формула кроме линейного смешения учитывает также попарное взаимодействие всех компонентов. Интерактивные коэффициенты описывают влияние каждой пары компонентов на изменение свойства смеси. Эти коэффициенты имеют ясный физический смысл. Так, например, a_{12} отражает влияние нелинейного эффекта взаимодействия первого и второго компонента.

4. Линейные бонусы

Линейными бонусами называются такие числа, добавив которые к начальным значениям свойств компонентов смешения, значение свойства смеси можно рассчитать по линейному закону следующим образом:

$$P_{Blend} = \sum_{i=1}^{n} X_i(P_i + \Delta_i), \quad (10)$$

где P_{Blend} – значение свойства смеси, P_i – значение свойства i-го компонента смеси, Δ_i – значение бонуса свойства i-го компонента смеси, а X_i – доля i-го компонента в смеси, причем

$$\sum_{i=1}^{n} X_i = 1.$$

На основе обработанных данных мировых НПЗ были получены коэффициенты нелинейных законов смешения (5) – (8). Однако для конкретного НПЗ можно повысить точность прогнозирования приведенных выше методов путем корректировки данных коэффициентов с помощью параметрической идентификации [3]. Для этого необходимо собрать набор фактических данных об операциях смешения на НПЗ, который включает рецептуру смешения, качество компонентов смешения, а также качество получившейся смеси. Для вычисления коэффициентов на основе этих данных решается задача минимизации невязки между рассчитанными по модели и измеренными свойствами смеси:

$$\sum_k (R_k - \hat{R}_k)^2 \to \min, \quad (11)$$

$$R_k = f(a, P_{ik}), k = 1 \dots K, \quad (12)$$

здесь k – номер операции смешения, K – общее число операций смешения, $\hat{R}_k$ –свойство смеси в операции смешения k, полученное в результате лабораторного анализа, R_k – прогнозное свойство смеси в операции смешения k, P_{ik} – значение свойства i-го компонента в смеси в операции смешения k, f – модель смешения, a – искомые переменные модели – коэффициенты метода. Задача (11) – (12) при K операций смешения имеет K уравнений и для законов смешения (5) – (7) является задачей нелинейной минимизации и имеет 2 переменные (a_1, a_2) для (5) – (6), и 3 переменные (a_1, a_2, a_3) для (7), а для законов (8) – (10) – задачей квадратичной минимизации и имеет 3 переменные (a_1, a_2, a_3) для законов (8), $n(n-1)/2$ переменных $(a_{12}, \dots, a_{n-1,n})$ для (9), n переменных $(\Delta_i, \dots, \Delta_n)$ для (10).

Приведенная в работе корректировка коэффициентов методов на актуальных данных о 12 операциях смешениях приводит к уменьшению среднеквадратичного отклонения ошибки прогноза, в среднем на 20 процентов по сравнению со стандартными коэффициентами метода, и приближает ошибку метода к точности измерения свойств в лаборатории. Применение общих методов учета нелинейности, линейных бонусов и метода интерактивных коэффициентов Dupont дает результаты, сравнимые по точности с методами (5) – (8).

Литература

1. *Ефитов Г.Л., Журавлева Т.Ю.* Математическое моделирование операций смешения. Математические методы в химии и в химической технологии: сборник, 1995. С. 110.
2. *Fahim M.A., Al-Sahhaf T.A., Elkilani A.S.* Fundamentals of Petroleum Refining, Elsevier, 2010. ISBN: 978-0-444-52785-1.
3. *Дилигенская А.Н.* Идентификация объектов управления. Самара: Самарский государственный технический университет, 2009. 136 с.

УДК 519.234.2

Исследование экстремального индекса случайного процесса по наблюдениям различной частоты

М.С. Рыжов[1,2], Н.М. Маркович[2]

[1]Московский физико-технический институт (государственный университет)
[2]Институт проблем управления им. В.А. Трапезникова РАН

При изучении случайных процессов интерес представляют кластеры, или блоки, последовательных наблюдений, превышающих достаточно высокий уровень. Для меры зависимости экстремумов случайного стационарного процесса используется экстремальный индекс. Её обратная величина аппроксимирует средний размер кластера превышений уровня. Поэтому актуальной задачей является оценивание величины

экстремального индекса и уровня, при котором оно достигается. В данной работе, основываясь на исследовании Robinson, Town (2000) о зависимости экстремального индекса от частоты наблюдения, предлагается непараметрическое оценивание экстремального индекса и исследование зависимости результата от частоты.

Теория

Пусть $N_{r_n}(u_n)$ размер кластера наблюдений $(X_1, X_2, \dots, X_{r_n})$, превышающих уровень u_n, наблюдаемого процесса $\{X_n\}$, где $r_n = o(n)$, $u_n = a_n x + b_n$, $a_n > 0, b_n \in R$, - нормализованные последовательности, такие что для $\forall x$ существуют $\mu \in R, \sigma > 0, \zeta \in R$ такие, что [1–2]:

$$\lim_{n\to\infty} n\{1 - F(a_n x + b_n)\} = \left\{1 + \frac{\zeta(x-\mu)}{\sigma}\right\}_+^{-\frac{1}{\zeta}}, \quad (1)$$

где $\{\dots\}_+ = max\{\dots, 0\}$.

Распределение размера кластера для выбранного уровня u_n определяется как $\pi_n(j) = P(N_{r_n}(u_n) = j,\ N_{r_n}(u_n) > 0)$, а значит для экстремального индекса (ЭИ) верно [2]:

$$\theta^{-1} = \lim_{n\to\infty} \sum_{j=1}^{\infty} j\pi_n(j). \quad (2)$$

Пусть последовательности $(X_1, \dots, X_i, \dots, X_n)$ соответствует ЭИ θ_1 с соответствующим распределением размера кластера $\pi_1(j)$, а подпоследовательности $\left(X_1, \dots, X_{di}, \dots, X_{d\left\lfloor\frac{n}{d}\right\rfloor}\right)$ с частотой d, $1 \le d < n - \theta_d$. Для стационарного распределения, удовлетворяющего условию перемешивания $D\{u_n\}$ [1] и пределу (1), в работе [2] доказано, что

$$\overline{\theta_d} = d\left\{1 - \sum_{j=1}^{d-1}\left(1 - \frac{j}{d}\right)\pi_1(j)\right\}\theta_1, \quad (3)$$

где $\theta_d \le \overline{\theta_d}, 0 \le \overline{\theta_d} \le 1$, а также

$$\pi_1(1) = \frac{2\overline{\theta_1} - \overline{\theta_2}}{\theta_1}, \pi_1(j) = \frac{2\overline{\theta_j} - \overline{\theta_{j+1}} - \overline{\theta_{j-1}}}{\theta_1}. \quad (4)$$

Для того чтобы сделать оценку значения ЭИ θ^*, предположим выполнение всех условий для формул (3) и (4) для выборки, $\theta_d = \overline{\theta_d}$. Будем считать, что все соотношения верны не только для ЭИ θ, но и для $\theta(u)$ – оценочного значения, полученного с помощью заранее оговоренного метода вычисления, которому по формуле (4) соответствует $\pi_1(j, u)$. Сделав такие предположения, можно построить алгоритм для выбора u_{opt}, и далее - оценки ЭИ $\theta^* = \theta(u_{\text{opt}})$.

Алгоритм

1. Для каждого значения уровня u вычислить значения $\{\theta_1(u), \theta_2(u), \dots, \theta_d(u)\}$.
2. Вычислить
$$\pi_1(1, u) = \frac{2\theta_1 - \theta_2}{\theta_1},\ \pi_1(j, u) = \frac{2\theta_j - \theta_{j+1} - \theta_{j-1}}{\theta_1}. \quad (5)$$
3. Вычислить $\widehat{\theta_d}(u) = d\left\{1 - \sum_{j=1}^{d-1}\left(1 - \frac{j}{d}\right)\pi_1(j, u)\right\}\theta_1(u)$.
4. Для каждой последовательности $\left\{X_k, \dots, X_{k+di}, \dots, X_{k+d\left\lfloor\frac{n-k}{d}\right\rfloor}\right\}$, $1 \le k < d$, и для значения уровня u вычислить оценки $\left\{\theta_d^k(u)\right\}$ и их средние $\theta_{mn}(u) = \frac{1}{d-1}\sum_{k=1}^{d-1}\theta_d^k(u)$.

5. Вычислить

$$MSE(d,u) = \left(\theta_{mn}(u) - \widehat{\theta_d}(u)\right)^2 + \frac{1}{d-2}\sum_{k=1}^{d-1}\left(\theta_{mn}(u) - \theta_d^k(u)\right)^2, \qquad (6)$$

и найти минимум $MSE(d,u)$ при u_{opt}.

6. Используя найденное u_{opt}, вычислить оценочное значение ЭИ $\theta^* = \theta(u_{\text{opt}})$.

Результаты

Проведено сравнение предложенного метода поиска значения ЭИ, где уровень u_{opt} вычисляется методом бутстрепа [3] и методом (5) на разных модельных процессах. Пример их сравнения для процесса ARMAX со значением $\theta = 0.4$ показан на рис. 1, где методом (5) получен для оценки θ^* результат 0.42, методом бутстреп — 0.61. Предложенный метод (5) в отличие от метода бутстреп, который имеет два параметра, имеет один параметр, частоту *d* , исследование которого является темой для будущих исследований.

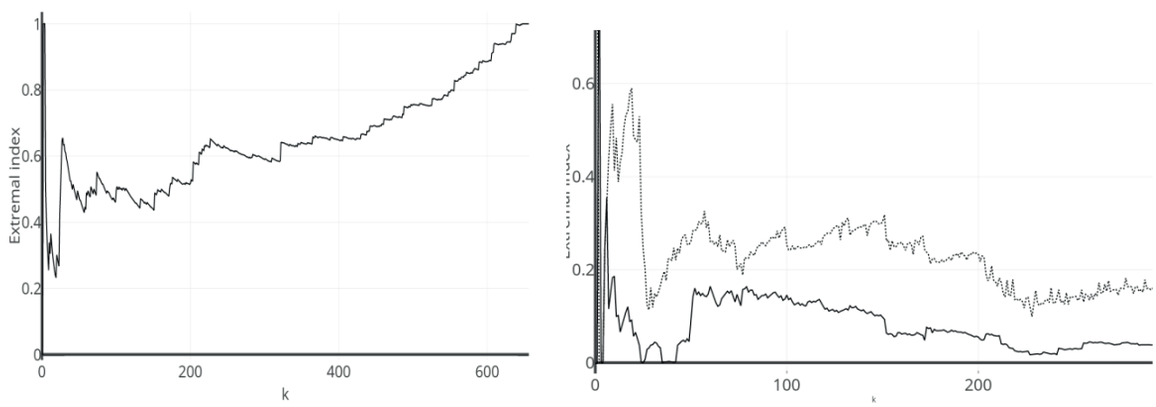


Рис 1. Слева значение оценки ЭИ $\theta(u)$, посчитанного интервальным методом против *k*, числа элементов выборки, превышающих уровень *u*; справа MSE в смысле бутстрепа (точечная линия) и метода (5) против *k*

Литература

1. *Leadbetter M. R.* Extremes and local dependence in stationary sequences, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete. 1983. 291–306.
2. *Michael E. Robinson, Jonathan A. Town* - Extremal analysis of processes sampled at different frequencies, J.R. Statist. Soc. B. 2000. Pt. 1, 117–135.
3. *Markovich N.M., Ryzhov M.S., Krieger U.R.* Nonparametric Analysis of Extremes on Web Graphs: PageRank versus Max-Linear Model, DCCN-2017, Moscow, 25–29 September 2017.

УДК 658.5

Разработка оптимизационных моделей оперативного планирования нефтеперерабатывающих/нефтехимических производств

Н. Байбородов

Московский физико-технический институт (государственный университет)

На всех нефтеперерабатывающих заводах задача оптимального производственного планирования является одной из ключевых, поскольку позволяет определить, как эффективнее переработать поступающее сырьё в готовую продукцию и оценить экономический эффект. Для решения задач оптимального производственного планирования (текущее планирование) во всем мире используются системы моделирования, с помощью которых можно построить математическую модель

предприятия. Математические модели производства включают в себя отдельные подмодели установок, а также взаимосвязи и преобразования потоков с учетом их качества. Математическую постановку задачи оптимального производственного планирования в общем виде можно записать следующим образом [1]:

$$F = \sum_{j=1}^{m} c_j x_j - \sum_{j=m+1}^{n} d_j x_j \to \max \quad (1)$$

$$\underline{b_i} \le \sum_{j=1}^{n} a_{ij} x_j + \sum_{j=n+1}^{p} a_{ij}(x_j) x_j \le \overline{b_i}, i = 1, \dots, k, \quad (2)$$

$$x_j \ge 0, j = 1, \dots, p. \quad (3)$$

Здесь c_j – цена продажи единицы x_j, j = 1, ... , m – переменные продажи потоков модели; d_j – стоимость покупки единицы x_j, j = m+1, ... , n – переменные покупки потоков модели; x_j, j = n+1, ... , p – переменные внутренних потоков модели, нагрузки установок, качество смесей и т.д.; a_{ij} – постоянные коэффициенты матрицы ограничений; $a_{ij}(x_j)$ – переменные коэффициенты матрицы ограничений, зависящие от x_j; $\underline{b_i}$, $\overline{b_i}$ – левые и правые части ограничений, i = 1, ... , k. Критерием решения данной задачи является максимизация прибыли F. Учитывая имеющиеся ограничения, задача оптимального производственного планирования является задачей нелинейного программирования на невыпуклом множестве.

В общей задаче производственного планирования особое внимание уделяется процессу оперативного планирования – задаче детализации производственного плана, полученного путем решения задачи текущего планирования, на ближайший короткий календарный отрезок времени (неделя, декада) с учетом полученной фактической информации о производстве за период времени, который завод отработал внутри текущего горизонта планирования [2].

Основной целью оперативного планирования является получение ответа на очень важный вопрос для персонала предприятия – как действовать в ближайший период времени в условиях сложившейся производственной ситуации, чтобы выполнить поставленный производственный план на расчетный период времени. Также детализация текущего плана необходима для облегчения решения задачи календарного планирования, поскольку на заводе имеются установки разной степени инерционности, то есть присутствуют установки, у которых переключают режимы работы достаточно редко, например, один раз в неделю или месяц (АВТ, риформинг, гидроочистка), и установки, режимы работы которых переключают часто, например, 1…2 раза в день (резервуары, смесители). Установки с большей степенью инерционности определяют производство и, работая в выбранном режиме, производят продукцию с фиксированными коэффициентами отборов и показателями качества. Решение задачи детализации на ближайший календарный отрезок времени позволит, рассчитав режимы работы крупных установок, получить готовые рецептуры смешения продуктов и полупродуктов для дальнейшего составления расписаний. Таким образом, составляя расписания работы завода, необходимо будет только следить за соблюдением полученных рецептур и выполнением логистических правил работы завода, что значительно упрощает данную задачу [3–4].

Целью работы является создание генератора оперативной модели планирования нефтеперерабатывающих/нефтехимических производств, улучшающего результат по сравнению с уже имеющимися и облегчающего дальнейшее составление расписания. В результате проведённой исследовательской работы предлагается решать задачу детализации производственного плана в следующей постановке:

$$F = \sum_{t=1}^{h}\sum_{j=1}^{m} c_j^t x_j^t - \sum_{t=1}^{h}\sum_{j=m+1}^{n} d_j^t x_j^t - \sum_{j=1}^{n} \alpha_j (u_j^+ + u_j^-) - \sum_{j=1}^{n} \alpha_j \sum_{t=1}^{h} (\beta_j^t + \gamma_j^t) - \\ - \sum_{t=1}^{h}\sum_{j\in X_3} \varepsilon_j^t q_j^t \to \max \quad (4)$$

$$\underline{b_i^t} \le \sum_{j=1}^{n} a_{ij}^t x_j^t + \sum_{j=n+1}^{p} a_{ij}^t (x_j^t) x_j^t \le \overline{b_i^t}, i = 1, \dots, z; t = 1, \dots, h; \quad (5)$$

$$y_k^{t+1} = y_k^t + \sum_{j\in X_{k_1}} x_j^t - \sum_{j\in X_{k_2}} x_j^t ; 0 \le y_k^t \le S_k^t; t = 1, \dots, h-1; k = 1, \dots, f; \quad (6)$$

$$\sum_{t=1}^{h} x_j^t + u_j^+ \ge \underline{W_j}, j = 1, \dots, n; \quad (7)$$

$$\sum_{t=1}^{h} x_j^t - u_j^- \ge \overline{W_j}, j = 1, \dots, n; \quad (8)$$

$$x_j^t + \beta_j^t \ge \underline{w_j^t}, j = 1, \dots, n;\ t = 1, \dots, h; \quad (9)$$

$$x_j^t - \gamma_j^t \le \overline{w_j^t}, j = 1, \dots, n;\ t = 1, \dots, h; \quad (10)$$

$$x_j^t - q_j^t = 0, t = 1, \dots, h; j \in X_3(t); \quad (11)$$

$$T = \sum_{t=1}^{h} \tau_t; \quad (12)$$

$$x_j^t \ge 0, u_j^- \ge 0, u_j^+ \ge 0, q_j^t \ge 0, \beta_j^t \ge 0, \gamma_j^t \ge 0, j = 1, \dots, p; t = 1, \dots, h. \quad (13)$$

Здесь T – фиксированная длина горизонта планирования; τ_t, t = 1, … , h – длительность периодов t; X – множество всех переменных модели; c_j^t – цена продажи в периоде t единицы x_j^t, j = 1, … , m – переменные продажи потоков модели в периоде t; d_j^t – стоимость покупки в периоде t единицы $x_j^t, j = m + 1, \dots, n$ – переменные покупки потоков модели в периоде t; $x_j^t, j = n + 1, \dots, p$ – переменные внутренних потоков модели в периоде t, а также нагрузки установок, качество смесей и т.д.; y_k^t, k = 1, … , f – переменные запасов потоков модели к концу периода t; x_j^t, $j \in X_{k_1}$, $X_{k_1} \in X$ – множество переменных модели (покупки, продажи, внутренние потоки), пополняющих запас потока y_k^t; $x_j^t, j \in X_{k_2}, X_{k_2} \in X$ – множество переменных модели (покупки, продажи, внутренние потоки), расходующих запас потока y_k^t; α_j– величина штрафа за покупку единицы u_j^+, $u_{j\,j}^-$, β_j^t, γ_j^t– штрафные переменные модели за невыполнение суммарного плана по переработке сырья или производства продуктов за весь горизонт планирования T, либо в отдельном периоде t; ε_j^t – величина штрафа за покупку единицы, q_j^t – штрафные переменные, которые равны активности переменных модели x_j^t в периоде t, $j \in X_3, X_3(t) \in X$ – переменные модели, соответствующие нагрузкам установок в нежелательных режимах работы в периоде t; a_{ij}^t – постоянные коэффициенты матрицы ограничений в периоде t; $a_{ij}^t(x_j^t)$ – переменные коэффициенты матрицы ограничений, зависящие от x_j^t в периоде t; $\underline{b_i^t}$, $\overline{b_i^t}$, S_k^t, $\underline{W_j}$, $\overline{W_j}$, $\underline{w_j^t}$, $\overline{w_j^t}$ – левые и правые части ограничений. Критерием решения данной задачи является максимизация чистой прибыли F с учётом приоритетов выполнения производственных задач в периодах t.

Литература

1. *Хохлов А.С., Цодиков Ю.М., Баулин Е.С.* Оптимизационные модели НПЗ/НХК и средства их поддержки. М.: РГУ нефти и газа им. И.М. Губкина, 2015. 9 с.
2. *Баулин Е.С.* Автоматизированная актуализация оптимизационных моделей планирования нефтеперерабатывающих/нефтехимических производств. М.: Баулин Евгений Сергеевич: дис. канд. техн. наук: 05.13.06 2014. 15 с.
3. *Баулин Е.С.* Последовательность решения задач производственного планирования и составления расписаний нефтеперерабатывающего производства.
4. *Баулин Е.С., Бронин А.Б., Хохлов А.С.* Скользящая детализация текущего плана деятельности НПЗ/НХК и актуализация оптимизационных моделей планирования // Автоматизация в промышленности. 2012. № 10. С. 8–14.

УДК 519.6

Математическое моделирование установок первичной переработки нефти в оптимизационных моделях планирования работы нефтеперерабатывающих предприятий

А.К. Власов

Московский физико-технический институт (государственный университет)

Введение

На всех нефтеперерабатывающих предприятиях особое значение придают решению задачи оптимального производственного планирования (ОПП), позволяющему определить, как наиболее эффективно переработать сырье в готовую продукцию с экономической точки зрения. Для решения задачи ОПП используются LP-модели, процедура поиска решения в которых основана на эвристическом методе последовательного линейного программирования (ПЛП). Однако сильным недостатком подобных моделей является зависимость решения задачи от начальных прогнозируемых оценок и структуры матрицы задачи (матрицы ограничений). Перед тем как рассчитать производственный план с помощью LP-модели, пользователям необходимо, во-первых, подготовить актуальные исходные данные о производстве и ввести их в модель, во-вторых, выбрать наиболее удобный метод математического моделирования производства, что, по сути, означает определение наиболее корректной матрицы задачи ОПП.

Математические способы моделирования

При установлении границ кипения фракций при первичной переработке нефти обычным явлением считается появление промежуточных фракций или так называемых «хвостов» перегонки. Перед пользователем LP-моделей ставится задача учета данного явления в математических моделях АВТ.

В работе предлагается сравнить два метода моделирования работы установок первичной переработки нефти на примере модели ректификационной колонны, методом «swing-cut» и методом суперпозиции логических вариантов. Далее приводится описание каждого метода.

- Метод моделирования «swing-cut»

Так как на производстве границы кипения дистиллятов можно смещать, предлагается границы кипения промежуточных фракций делить на две области в определенном отношении и дополнять ими участки выкипания граничащих дистиллятов (см. рис. 1, правая часть равенства соответствует методу моделирования «swing-cut», A_i – дистилляты, a_i – промежуточные фракции, α_i, $(1 – \alpha_i)$ – объемные доли промежуточных фракций, попадающих в соседние дистилляты). При моделировании первичной переработки нефти таким способом с установки получаем дистилляты, каждый из которых состоит из основного погонного слоя и частей промежуточных слоев.

- Метод моделирования суперпозицией логических вариантов

Во втором способе предлагается границы кипения каждого промежуточного слоя целиком включать в область выкипания одного из соседних дистиллятов. Количество

вариантов распределения промежуточных слоев по фракциям зависит от самого количества граничных слоев. К примеру, если в модели нефть содержит n «хвостов», то количество способов, которыми можно распределить «хвосты» по дистиллятам равно 2^n (каждый способ есть логический вариант работы установки АВТ). В модели вся поступающая на установку нефть может быть переработана в различных технологических режимах, при этом с установки имеем $n + 1$ дистиллятов, полученных путем линейной комбинации 2^n логических вариантов работы АВТ (см. рис. 1, левая часть равенства соответствует методу моделирования суперпозицией логических вариантов, где за X_i обозначены коэффициенты линейного разложения, удовлетворяющие условию $0 \leq X_i \leq 1$). Изменяя режим работы установки таким образом, можно добиться точно такого же распределения промежуточных слоев по фракциям, что и в методе «swing-cut».

Несложно показать, что эти способы моделирования математически взаимозаменяемы. Связано это с тем, что, благодаря особой структуре матрицы задачи на рис. 1, ранг основной матрицы равен рангу расширенной, то есть задача разрешима всегда [4]. А то, что решение удовлетворяет физическому смыслу, было проверено путем вычисления физически возможных коэффициентов X_i с помощью программы, созданной в MATLAB.

Для анализа эффективности двух методов математического моделирования установок первичной переработки нефти были созданы две демонстрационные модели НПЗ топливного профиля с разными способами моделирования работы установок АВТ. Размерность матрицы ограничений была следующей: количество строк (ограничений) от 300 до 400, количество искомых переменных от 500 до 600.

Необходимость проведения данных исследований связана с тем, что, как уже было связано выше, задача ОПП является задачей нелинейного программирования на невыпуклом множестве ограничений и для её решения не существует универсальных численных методов, кроме как полного перебора значений всех переменных. Результаты решения этих задач в LP-моделях сильно зависят от заданных начальных предположений об области переменных, в которой будут искать решение, и самой структуры матрицы задачи (количество строк, количество столбцов, количество ненулевых элементов матрицы, количество элементов матрицы пересчитываемых в процессе рекурсии). В связи с этим при использовании каждого из этих методов, на первый взгляд математически эквивалентных, потребуется задавать различные наборы производственных параметров одним и тем же объектам модели, и будут сформированы матрицы ограничений различной структуры.

Результаты исследований

В ходе поставленного эксперимента была получена абсолютная идентичность результатов решения задачи ОПП (целевые функции полностью совпали в разных экспериментах), что доказывает взаимозаменяемость методов моделирования. Однако главным преимуществом метода “swing-cut” оказалась простота создания математической модели АВТ и настройки нужного режима работы. А метод моделирования суперпозицией логических вариантов значительно перегружал матрицу задачи ОПП большим числом дополнительных переменных, что привело к усложнению решения задачи ЛП и увеличению времени создания модели. Но при этом упростился анализ корректности решения задачи. В процессе создания моделей и проведения экспериментов были сделаны следующие выводы:

- Выбор метода моделирования зависит от поставленных задач и степени адекватности модели производства.
- Необходимо продолжить вычислительные эксперименты на моделях реальных НПЗ, так как размерность матрицы ограничений среднего по производительности НПЗ (переработка нескольких миллионов тонн нефти в год) порядка десяти тысяч строк и примерно десять тысяч переменных.

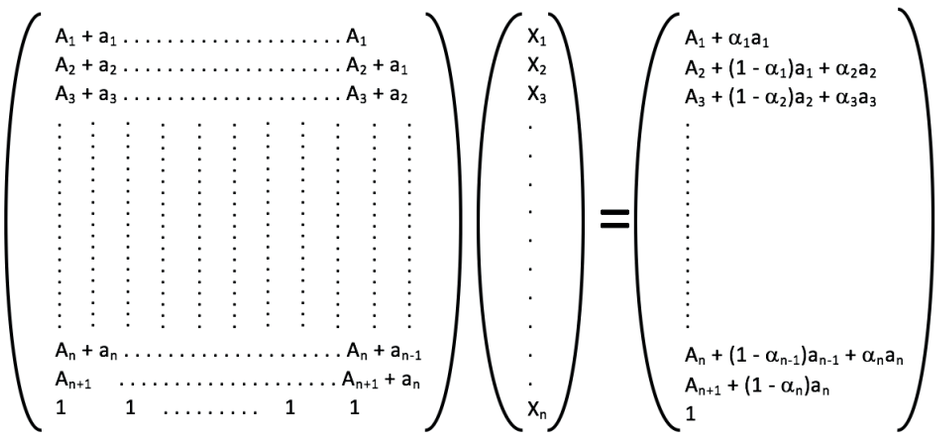


Рис. 1. СЛАУ в матричном виде для нахождения коэффициентов X_i

Литература

1. *Баулин Е.С.* Автоматизированная актуализация оптимизационных моделей планирования нефтеперерабатывающих/нефтехимических производств: диссертация на соискание ученой степени кандидата технических наук. 2014. 149 с.
2. *Хохлов А.С.* Автоматизированная актуализация оптимизационных моделей планирования непрерывных производств / А.С. Хохлов, А.Б. Боронин, А.Н. Гайнетдинова // Автоматизация в промышленности. 2009. N 7. С. 56–59.
3. *Lefler W.L.* Petroleum refining for non-technical person. Oklahoma: PennWellBooks, 1979. 224 с.
4. *Умнов А.Е.* Аналитическая геометрия и линейная алгебра. М: МФТИ, 2011. §6.6. С. 215.

УДК 51-77

Информационное противоборство в управлении толпой

А.Д. Рогаткин

Институт проблем управления им. В.А. Трапезникова РАН

В моделях порогового коллективного поведения [1] состояние равновесия системы определяется функцией распределения порогов агентов. Результаты исследования теоретико-игровых моделей порогового коллективного поведения имеют множество приложений. Среди них – модели управления толпой, в которых одним из объектов управления являются пороги агентов.

В данном докладе рассматривается следующий способ управления распределением порогов агентов. Пороги выбранной доли агентов либо изменяются с некоторой вероятностью на «0» (что соответствует возбуждению), либо изменяются с некоторой вероятностью на «1» (что соответствует иммунизации к социальному давлению). Такое преобразование функции распределения порогов агентов приводит к соответствующему изменению равновесного состояния толпы. Случайный характер управленческого воздействия описывает ситуацию информационного управления – осуществляются мероприятия по изменению порогов агентов (сообщение им некоторой информации), но результат этих мероприятий (изменение порогов агентов) нельзя предсказать достоверно.

Постановка задачи заключается в следующем. Управление толпой осуществляют два центра. Один из центров стремится путем изменения порогов на «0» максимизировать равновесное состояние толпы (количество действующих агентов). Другой центр путем изменения порогов на «1» стремится минимизировать равновесное состояние толпы. Осуществляемое управление требует некоторых заданных затрат. В результате игры двух центров может возникать равновесное состояние толпы как результат реализации управлений, являющихся равновесиями Нэша антагонистической игры центров. Таким образом, если два центра осуществляют мероприятия информационного управления

противоположной направленности, тогда такая ситуация распределенного контроля может рассматриваться как информационное противоборство [2] между ними. Доклад посвящен результатам разработки теоретико-игровых моделей такого противоборства в рамках теории игр в нормальной форме и иерархических и рефлексивных игр, в том числе, когда предпочтения центров зависят от вероятности выхода управляемой системы из области ее устойчивого равновесия.

Литература

1. *Granovetter M.* Threshold Models of Collective Behavior // AJS. 1978. V. 83. N 6. P. 1420.
2. *Gubanov D.A., Kalashnikov A.O., Novikov D.A.* Game-theoretic Models of Informational Confrontation in Social Networks // Automation and Remote Control. 2011. V. 72. N 9. P. 2001.

УДК 517.977.5

Задача быстродействия при упругом и вязко-упругом взаимодействии тела с поверхностью

А.А. Галяев, П.В. Лысенко

Московский физико-технический институт (государственный университет)
Институт проблем управления им. В.А. Трапезникова РАН

При моделировании ударов в механической системе используется представление, в котором система по достижению в фазовом пространстве ограничения в общем случае мгновенно перескакивает в другую точку с теми же пространственными координатами, но с другими значениями проекций скоростей. Эти новые значения проекций скоростей задаются при помощи ньютоновского коэффициента восстановления, в то время как сам процесс удара (взаимодействия между телами) оказывается скрыт в этом коэффициенте, поскольку длительность фазы удара полагается равной нулю. Управление в таких системах входит только в безударную фазу движения. В работе рассматривается конечная (ненулевая) длительность фазы удара (взаимодействия с поверхностью препятствия). Решение уравнений движения системы в фазе взаимодействия позволяет связать послеударные макроскопические характеристики системы (скорость, полную энергию и т.д.) с доударными. Другой отличительной особенностью работы является введение в фазу взаимодействия управляющего воздействия [1].

В работе решается задача быстродействия при одностороннем вязко-упругом взаимодействии материальной точки с управляемой поверхностью. Условия окончания взаимодействия определяются через силу, действующую со стороны поверхности на тело. В литературе такие условия окончания взаимодействия называются физическими [2], [3].

Рассмотрена динамика физической системы, состоящей из поверхности, управляемой по скорости, и элемента, включающего в себя пружину и тело конечной массы. Поверхность и элемент испытывают взаимодействие при наличии упругой силы пружины, которая пропорциональна сжатию изначально недеформированной пружины, и вязкой силы Кельвина–Фойгта, пропорциональной относительной скорости тела. Динамика системы описывается уравнениями [4]

$$\begin{cases} \dot{x}_0(t) = u(t), \\ \ddot{x}_1(t) = -\omega^2\left(x_1 - x_0 - \dfrac{l}{2}\right) - 2\alpha(\dot{x}_1 - \dot{x}_0). \end{cases}$$

Здесь x_0 – координата поверхности; x_1 – координата тела массы m с прикреплённой к нему пружиной длиной $\dfrac{l}{2}$ и жёсткости k; α – коэффициент вязкости при

$\alpha \in [0,1]$; ω – круговая частота, равная $\sqrt{\frac{k}{m}}$. Без потери общности будем считать что $\omega = 1$.

При $\alpha = 0$ вязкая компонента силы отсутствует и взаимодействие становится упругим.

На управление наложено ограничение $u \le |u_0|$.

Краевые условия имеют следующий вид:

$$x_0(0) = 0,\ x_1(0) = \frac{l}{2},\ \dot{x}_1(0) = -v_0,\ \ddot{x}_1(\tau) = 0\ .$$

Условие окончания взаимодействия есть физическое условие одностороннего контакта.

Здесь τ – длительность взаимодействия поверхности с пружиной. Решается задача быстродействия, т.е. ищется оптимальное управление $u^*(t)$, минимизирующее функционал задачи $\tau \to \min$. Для решения применён принцип максимума Понтрягина. Закон оптимального управления имеет вид:

$$\begin{cases} u^*(t) = u_0,\ t \in [0,\ \tau_1], \\ u^*(t) = -u_0,\ t \in (\tau_1,\ \tau_1 + \tau_2]. \end{cases}$$

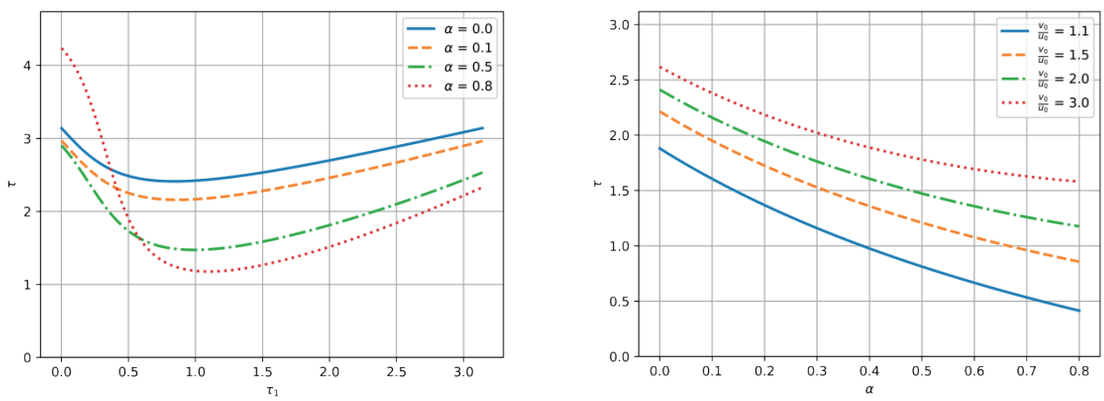
где τ_1, τ_2 – длительности периодов управления. Функция $\tau(\tau_1)$ получена аналитически и имеет вид:

$$\begin{cases} A = -\dfrac{u_0 + v_0}{\omega}, \\ tg\varphi_1 = \dfrac{-Ae^{-\alpha\tau_1}\sin(\omega\tau_1)}{2\dfrac{u_0}{\omega} + Ae^{-\alpha\tau_1}\cos(\omega\tau_1)}, \\ B = \dfrac{2\alpha\omega}{2\alpha^2 - 1}, \\ \tau = \tau_1 + \arctan\left(\dfrac{B + tg\varphi_1}{1 - Btg\varphi_1}\right). \end{cases}$$

В силу сложности функции $\tau(\tau_1)$, исследование её и поиск оптимального τ проводим численно.

Закон оптимального управления, а также коэффициент восстановления (отношение конечной скорости тела к начальной), полученные в работе, являются основой численного моделирования поведения системы и дают начальные условия для описания движения точки после взаимодействия с препятствием. Предложенный подход к нахождению послеударных макроскопических характеристик системы позволит решать и другие задачи оптимального управления механической системой в фазе удара.

В работе исследованы зависимости времени окончания взаимодействия и коэффициента восстановления от вязких свойств. Разработана программа на языке Python и проведено моделирование поведения системы тело-поверхность.



а) б)

Рис. 1. а) зависимость полного времени взаимодействия от длительности первого периода управления;
б) зависимость оптимального решения от коэффициента вязкости

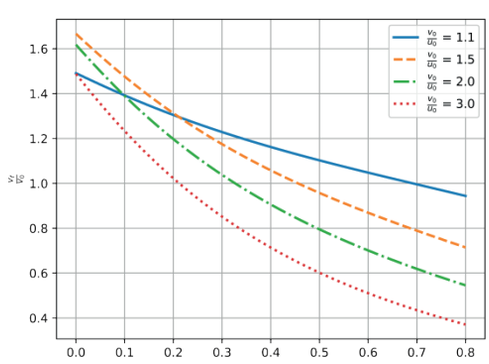


Рис. 2. Зависимость коэффициента восстановления от коэффициента вязкости

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 16-08-01285 а).

Литература

1. *Миллер Б.М., Рубинович Е.Я.* Разрывные решения в задачах оптимального управления и их представление с помощью сингулярных пространственно-временных преобразований. // Автоматика и телемеханика 2013. №12. С. 56–103.
2. *Козлов В.В., Трещев Д.В.* Биллиарды. (Генетическое введение в динамику систем с ударами.). М.: Изд-во МГУ, 1991.
3. *Галяев А.А.* Об одной задаче оптимального управления в фазе удара и унификации моментов окончания взаимодействия // Автоматика и Телемеханика, 2010. №12. С. 10–21.
4. *Галяев А.А.* Об одномерном ударе цепочки тел, обладающей вязко-упругими свойствами // Автоматика и Телемеханика. 2015. №10. С. 40–49.

УДК 004.021

Оценка надежности широкополосной беспроводной сети с линейной топологией и перекрёстным резервированием

Д.А. Радкевич

Московский физико-технический институт (государственный университет)
Институт проблем управления им. В.А. Трапезникова РАН

Рассмотрена резервированная система передачи данных с линейной топологией в виде модели неоднородной системы надежности горячего дублирования с одним ремонтным устройством и показательным временем ремонта отказавших элементов (каналов передачи данных). Для частного случая из четырех базовых станций с наличием кросс-соединений, когда распределение времени безотказной работы экспоненциально, было графически представлено пространство из восьми состояний системы, на основе чего был построен граф перехода процесса, который показывает переходы между какими состояниями системы допустимы (рис. 1а). В результате была выведена система дифференциальных уравнений ($p_i(t)$-вероятность системы находиться в данный момент времени в состоянии i, α_i и β_i – параметры экспоненциального распределения длительности работы и восстановления для каждого канала):

$$\begin{aligned}
p_0'(t) &= -(\alpha_1+\alpha_2+\alpha_3)p_0(t) + p_1(t)\beta_1 + p_2(t)\beta_2 + p_4(t)\beta_3,\\
p_1'(t) &= p_0(t)\alpha_1 - (\beta_1+\alpha_2+\alpha_3)p_1(t) + p_3(t)\beta_2 + p_5(t)\beta_3,\\
p_2'(t) &= p_0(t)\alpha_2 - (\beta_2+\alpha_1+\alpha_3)p_2(t) + p_3(t)\beta_1 + p_6(t)\beta_3,\\
p_3'(t) &= p_1(t)\alpha_2 + p_2(t)\alpha_1 - (\beta_1+\beta_2+\alpha_3)p_3(t) + p_7(t)\beta_3,\\
p_4'(t) &= p_1(t)\alpha_3 - (\beta_3+\alpha_1+\alpha_2)p_4(t) + p_5(t)\beta_1 + p_6(t)\beta_2,\\
p_5'(t) &= p_1(t)\alpha_3 + p_4(t)\alpha_1 - (\beta_1+\beta_3+\alpha_2)p_5(t) + p_7(t)\beta_2,\\
p_6'(t) &= p_2(t)\alpha_3 + p_4(t)\alpha_2 - (\beta_2+\beta_3+\alpha_1)p_6(t) + p_7(t)\beta_1,\\
p_7'(t) &= p_3(t)\alpha_3 + p_5(t)\alpha_2 + p_6(t)\alpha_1 - (\beta_1+\beta_2+\beta_3)p_4(t)\beta_3.
\end{aligned} \qquad (1)$$

Данная система была решена символьно с помощью программной среды Wolfram Mathematica 10. В предположении, что множество отказов представлено состояниями 3, 6 и 7, можно выписать явное выражение для функции надежности $Rt(t) = 1 - p_3(t) - p_6(t) - -p_7(t)$, где p_i – вероятность нахождения системы в состоянии с индексом i, на основе которого был построен график функции надежности в данном процессе (рис.1 б).

Далее были найдены стационарные характеристики системы, которые определяются формулой $\pi_j = \lim_{t\to\infty} p_j,\ j \in \overline{0,7}$. Преобразуя уравнения (1), получим однородную систему с вырожденной матрицей, которую надо дополнить уравнением нормировки $\sum_{j=0}^{7}\pi_j = 1$. Исходными данными для задачи послужили экспертные оценки времени жизни каналов. Среднее время доступности и восстановления каждого из четырех каналов (величины, обратные интенсивностям): $m_{1,0} = 26{,}08(\text{час}),\ m_{1,1} = 23{,}37(\text{мин}), m_{2,0} = 30(\text{час}), m_{2,1} == 15(\text{час}), m_{3,0} = 10000(\text{час}), m_{3,1} = 5(\text{час})$. В результате были получены:

- вектор стационарных вероятностей:

$$\vec{\pi}' = (6.565\cdot10^{-1}, 9.805\cdot10^{-3}, 3.282\cdot10^{-1}, 4.902\cdot10^{-3}, 3.282\cdot10^{-4}, 4.902\cdot10^{-6}, 1.641\cdot10^{-4}, 2.451\cdot10^{-6}),$$

- стационарная надежность:

$$r = 1 - (\pi_3 + \pi_6 + \pi_7) = 0.9949.$$

В случае отсутствия кросс-соединений (последовательная схема из 3 каналов) надежность сети считается, как произведение надежности каждого канала:

$$r = \prod_{i=1}^{3} r_i = \prod_{i=1}^{3} \frac{\alpha_i}{\alpha_i+\beta_i} = 0.6565.$$

Эти результаты показывают, что стационарная надежность системы передачи данных с линейной топологией существенно повышается в случае наличия кросс-соединений.

Во втором случае рассматривается метод исследования характеристик надежности, когда распределение времени безотказной работы не является экспоненциальным, что приводит к необходимости марковизации процесса. Был использован метод введения дополнительной переменной $x(t)$ – время, прошедшее с момента восстановления системы до момента времени t. Учитывая, что вероятность выхода из строя канала за время Δ равна $\frac{a(x)}{1-A(x)}\Delta = \delta(x)\Delta$ (где $A(x)$ – функция распределения случайной величины A – времени безотказной работы канала, $a(x)$ – её плотность распределения), а вероятность прибора восстановиться за время Δ равна $\beta\Delta$ (β – параметр экспоненциального распределения времени восстановления прибора), расписываем вероятность системы находиться в каждом из состояний, что в конечном итоге приведет нас к системе дифференциальных уравнений:

$$\frac{\partial p_0(x)}{\partial x} = -p_0(x)3\delta(x) + \beta[p_1(x) + p_2(x) + p_4(x)],$$
$$\frac{\partial p_1(x)}{\partial x} = -p_1(x)2\delta(x) - p_1(x)\beta + \beta[p_3(x) + p_5(x)] + p_0(x)\delta(x),$$
$$\frac{\partial p_2(x)}{\partial x} = -p_2(x)2\delta(x) - p_2(x)\beta + \beta[p_3(x) + p_6(x)] + p_0(x)\delta(x),$$
$$\frac{\partial p_3(x)}{\partial x} = -p_3(x)\delta(x) - p_2(x)2\beta + \delta(x)[p_1(x) + p_2(x)],$$
$$p_3(0) = \int_0^t p_7(x)\beta\, dx,$$
$$\frac{\partial p_4(x)}{\partial x} = -p_4(x)2\delta(x) - p_4(x)\beta + \beta[p_5(x) + p_6(x)] + p_0(x)\delta(x),$$
$$\frac{\partial p_5(x)}{\partial x} = -p_5(x)\delta(x) - p_5(x)2\beta + \delta(x)[p_1(x) + p_4(x)],$$
$$p_5(0) = \int_0^t p_7(x)\beta\, dx,$$
$$\frac{\partial p_6(x)}{\partial x} = -p_6(x)\delta(x) - p_6(x)2\beta + \delta(x)[p_2(x) + p_4(x)],$$
$$p_6(0) = \int_0^t p_7(x)\beta\, dx\,,$$
$$\frac{\partial p_7(x)}{\partial x} = p_7(x)3\beta + \delta(x)[p_3(x) + p_5(x) + p_6(x)]$$

Полученная система сложна для численного решения стандартными программными методами ввиду наличия большого количества состояний, но в предположении, что время безотказной работы имеет экспоненциальное распределение, мы получим систему, идентичную системе (1), что дает основания полагать корректность составленной системы ДУ и метода в частности.

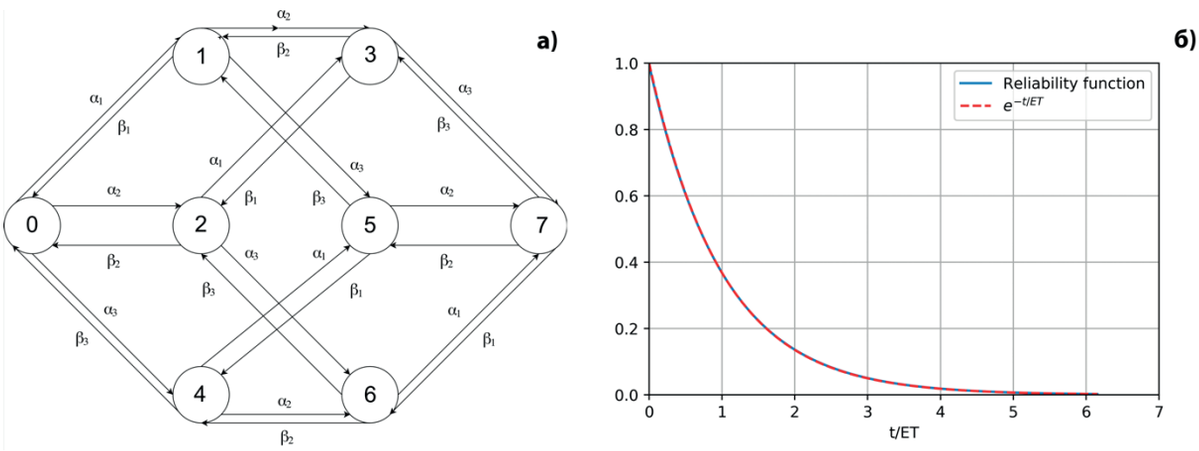


Рис. 1а. Граф переходов процесса. α_i и β_i являются интенсивностями перехода.
Рис. 1б. Функция надежности системы в нормировке на среднее время жизни системы, ***ET*** – время безотказной работы системы.

Литература

1. *Vishnevsky, V., Krishnamoorthy, A., Kozyrev, D., Larionov, A.*: IReview of methodology and design of broadband. Indian Journal of Pure and Applied Mathematics wireless networks with linear topology, 2016. V. 47. P. 329–342.
2. *Rykov V., Itkin V.* Reliability of technical systems and technogenic risk. Gubkin Russian State University of Oil and Gas (National Research University). M., 2015.

УДК 519.8

О методе кластеризации пользователей онлайновых социальных сетей на основе оказываемого на них влияния

Д.А. Губанов, А.Г. Чхартишвили

Институт проблем управления РАН

В настоящее время в связи с развитием интеллектуальных технологий обработки больших объемов данных (data mining) и относительной доступностью данных онлайновых социальных сетей интенсивно разрабатываются методы кластеризации их пользователей (см., например, [1]). Разнообразие существующих методов кластеризации во многом обусловлено спецификой решаемых прикладных задач. Одной из таких прикладных задач, представляющих научный и практический интерес, является задача выявления наиболее влиятельных пользователей (в той или иной предметной области) и оценка того, можно ли каким-то естественным образом разбить пользователей на стабильные подмножества, слабо пересекающиеся по источникам информации, оказывающих на них то или иное влияние. В данном докладе предлагается метод кластеризации, позволяющий получить ответ на этот вопрос.

Предлагаемый метод основывается на выявлении наиболее влиятельных пользователей социальной сети в соответствии с акциональной моделью влияния и влиятельности агентов и мета-агентов [2, 3]. В соответствии с этой моделью пользователи сети (называемые агентами) совершают действия, на множестве которых определено отношение частичного порядка: одно действие может являться следствием другого (например, комментарий к посту в онлайновой социальной сети является следствием этого поста). При этом влияние агента, характеризующееся интенсивностью реакции на его действия, определяется с учетом точки зрения управляющего субъекта (центра), что, в частности, позволяет выделить для анализа те или иные тематические области.

Значимость действий для центра можно рассматривать в несколько различающихся вариантах, имеющих разный содержательный смысл. Например, можно считать, что

значимость каждого действия в онлайновой социальной сети (поста, комментария, лайка и т.д.) не зависит от пользователя, совершившего действие. Однако в данной работе рассматривается нормированная влиятельность: суммарная значимость действий каждого пользователя полагается равной единице (это означает, в частности, что влияние отдельного пользователя на расчет влиятельности не зависит от его активности в сети и определяется лишь тем, как его реакция распределена между различными популярными пользователями).

В онлайновых социальных сетях сравнительно мала доля пользователей с заметной влиятельностью, рассчитываемой на основе акциональной модели (например, в исследовании [4] на 2% пользователей приходится 98% совокупной влиятельности). Поэтому в качестве признаков пользователя при проведении кластеризации можно использовать оказываемые на него влияния со стороны 2% наиболее влиятельных.

Опишем схему предлагаемого алгоритма кластеризации.

1) Расчет нормированной влиятельности пользователей социальной сети в соответствии с акциональной моделью.
2) Формирование стохастических векторов влияний на всех пользователей социальной сети со стороны влиятельных пользователей (в результате данного шага каждый пользователь задается стохастическим вектором, характеризующим влияние на него).
3) Введение меры близости между двумя пользователями, представляющей собой сумму компонент вектора, представляющего собой минимум из влияний на этих пользователей со стороны данного влиятельного пользователя. Вычитая это влияние из единицы, получаем функцию расстояния между пользователями:

$$d(x,y) = 1 - \sum_{k=1}^{l} \min(x_k, y_k),$$

где l – размерность векторов (количество влиятельных пользователей), $x, y \in \boldsymbol{R}^l$ – характеризующие пользователей векторы влияния, $d(x,y) \in [0,\ 1]$. Предложенная функция расстояния удовлетворяет всем трём аксиомам метрики (тождества, симметрии и неравенства треугольника). Целесообразность ввода такой функции (и отказ от использования, например, более традиционной евклидовой метрики) обусловлена содержательными соображениями, а также спецификой структуры влияния в социальной сети.

4) Введение способа расчета центроида кластера как точки, минимизирующей суммарное расстояние до точек кластера.
5) Модификация алгоритма кластеризации k-means в соответствии с пунктами 3 и 4.
6) Кластеризация пользователей социальной сети.

Предлагаемый метод кластеризации пользователей учитывает особенности информационного влияния в социальной сети, что позволяет проверять гипотезу о расслоении пользователей сети на слабо пересекающиеся сообщества в различных тематических областях.

Литература

1. *Aggarwal C.C.* Social Network Data Analytics. New York; Heidelberg: Springer, 2011.
2. *Губанов Д.А., Чхартишвили А.Г.* Влиятельность пользователей и метапользователей социальной сети // Проблемы управления. 2016. N 6. С. 12–17.
3. *Chkhartishvili A.G., Gubanov D.A.* An actional model of user influence levels in a social network // Automation and Remote Control. 2015. V. 76, Issue 7. P. 1282–1290.
4. *Chkhartishvili A.G., Gubanov D.A.* Analysis of User Influence Types in Online Social Networks: An Example of VKontakte // Proceedings of the 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017, Moscow). Moscow, 2017. V. 1. P. 3–5.

УДК 533.922

Перспективные направления использования методов рефлексии к задачам хранения и обработки Big Data

Д.Н. Федянин

Институт проблем управления им. В.А. Трапезникова РАН

Задача, которую поставили перед собой авторы работы, заключается в выделении хотя бы нескольких классов задач, которые, с одной стороны, относились бы к задачам обработки Big Data, с другой – могли бы быть успешно решены методами рефлексии и эпистемической логики, описанными в [1 – 6], например, метод рефлексивных разбиений или метод представления бесконечного дерева информированности к конечному графу, что с математической точки зрения является сведением системы с бесконечным количеством переменных к системе конечного числа переменных. Под успешным решением мы понимаем более производительное достижение результатов, полученных другими методами или более точное приближение к оптимальному результату. В работе мы покажем, как рефлексия может быть использована для обработки Big Data.

Рефлексия – размышления о размышлениях. Размышления о своих размышлениях называется рефлексией первого рода, размышления о размышлении других рефлексией второго рода [1]. Также в литературе встречается понятие эпистемической логики [2, 3] – наука о представлениях, о знаниях, которая включает в себя исследования размышлений агента – человека или искусственного интеллекта – и о природе, и о своих размышлениях, и о размышлении других. Традиционным формальным языком описания таких явлений в эпистемологии является логика [4], в рефлексии – теория графов и теория игр [1]. Рефлексия тесно связана с проблемами искусственного интеллекта [1, 3, 7]. Отделение интеллектуального анализа данных от методов рефлексии является довольно сложной задачей, однако можно выделить следующие отличия рефлексивного анализа:

- широкое использование логических рассуждений,
- меньшее использование традиционных методов машинного обучения – нейронных сетей, байесова обучения, кластеризации, поиска регрессий,
- наличие методов для обработки неопределенности для произвольных вероятностных распределений,
- обилие методик рекурсивных и вложенных алгоритмов и решение обратной задачи: идентификация начальных параметров по известному итоговому результату работы алгоритма,
- широкое применение функциональных языков программирования, в частности Haskell,
- учет когнитивных искажений,
- умение искать транзитивные замыкания логических выражений и по транзитивному замыканию восстанавливать исходные логические выражения,
- предсказание поведения пользователей, нарушителей и т.д.

Широкий интерес к Big Data [8] связан с беспрецедентным ростом мощности информационных систем, позволившим собирать, хранить и обрабатывать огромные массивы информации – данные социальных сетей [9], финансовых рынков [10, 11], номенклатуры и свойств продуктов и т.д. Под Big Data мы будем понимать информационную систему, которую отличает

- большой объем данных,
- невозможность хранения всех данных в одном хранилище данных,
- хранение данных в различных типах структурах и использование различных алгоритмов обработки таких структур,
- существенные ограничения на передачу данных между хранилищами данных – как по объему, так и по скорости,
- постоянное обновление данных.

Рассмотрим проблемы, стоящие перед разработчиками искусственного интеллекта, частью которого являются данные Big Data [12]. Каким образом должно быть устроено мышление проектируемого искусственного интеллекта для принятия решений в приемлемые сроки [5, 13]? Как должна быть устроена группа искусственных интеллектов, имеющих доступ к одному и тоже источнику данных? Как обеспечить безопасность персональных данных [7, 8]? Как масштабировать модели принятия решений пользователями в социальных сетях [14, 15], данные о которых хранятся в Big Data? Для ответов на эти вопросы существует много перспективных направлений, в том числе получение новых знаний из базы данных или данных (KDD), которые включат в себя: последовательное исследование на противоречивость, обобщение информации, генерацию гипотез, проверку гипотез и вывод информации. Одним из подходов к решению этих проблем является поддержка интеллектуального анализа информации и эпистемологического программирования с использованием методов, основанных на рассуждениях [6].

Основным результатом этой обзорной работы является перечень перспективных направлений, которыми являются:

- анализ и моделирование принятий решений в социальных сетях,
- обеспечение безопасности конфиденциальных данных,
- проверка базы на непротиворечивость,
- получение новых знаний автоматическими методами логического вывода,
- согласование и анализ взаимодействия нескольких пользователей,
- оптимизация структуры хранения данных,
- координация автономных групп роботов с сенсорами высокого качества.

Литература

1. *Novikov D., Chkhartishvili, A*. Reflexion & Control: Mathematical models.// Series: Communications in Cybernetics, Systems Science and Engineering (Book 5). CRC Press. March 10, 2014. P. 298.
2. *Fedyanin D.* Threshold and Network generalizations of Muddy Faces Puzzle / Proceedings of the 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017, Moscow). M.: IEEE, 2017. V.1. С. 256–260.
3. *Davis E., Morgenstern L.* Epistemic logic and its applications: Tutorial notes// International Joint Conferences on Artificial Intelligence. 1983. T. 93.
4. *Christoff Z., Hansen J.U.* [*et al.*] Reflecting on Social Influence in Networks // Journal of Logic, Language and Information/ December 2016, Volume 25, Issue 3–4. P. 299–333 https://doi.org/10.1007/s10849-016-9242-y.
5. *Chen M., Mao S., Liu Y.* Big data: A survey //Mobile Networks and Applications. 2014. V. 19. N. 2. P. 171–209.
6. *Smailovic* [*et al.*] Advanced User Profiles for the SmartSocial Platform: Reasoning upon Multi-Source User Data. // Conference: 6th ICT Innovations Conference 2014, At Ohrid, Macedonia, Volume: Web Proceedings of the 6th ICT Innovations Conference 2014. P. 12.
7. *Mehmood A.* [*et al.*], Protection of Big Data Privacy. Access IEEE. 2016. V. 4, P. 1821-1834. ISSN 2169-3536.
8. *Xu* [*et al.*] Information Security in Big Data: Privacy and Data Mining. IEEE Access. 2. 1-28. 10.1109/ACCESS.2014.2362522.
9. *Genesereth M., Dietterich T.* Data Integration: The Relational Logic Approach// Synthesis Lectures on Artificial Intelligence and Machine Learning. Morgan and Claypool Publishers. March 15, 2010. P. 110.
10. *Perner P.,* Mining Sparse and Big Data by Case-based Reasoning// Procedia Computer Science, Proceedings of Knowledge-Based and Intelligent Information & Engineering Systems 18th Annual Conference, KES-2014 Gdynia, Poland. 2014. V. 35. Pages 19-33. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2014.08.081.
11. *Witold P., Shyi-Ming C.*. Information granularity, big data, and computational intelligence// Studies in Big Data, 2197-6503; V. 8, Springer, 2014. P. 444.
12. *Ghosh S., Meijering B., Verbrugge R*. Strategic Reasoning: Building Cognitive Models from Logical Formulas // Journal of Logic, Language and Information. 2014. V. 23. N 1. P. 1–29.
13. *Bellomarini L.* [*et al.*]. Swift logic for big data and knowledge graphs.// International Joint Conference on Artificial Intelligence, 2017.
14. Weichselbraun A., Gindl S., Scharl A., Enriching semantic knowledge bases for opinion mining in big

data applications, In Knowledge-Based Systems, 2014. V. 69. P. 78-85. ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2014.04.039.
15. *Christoff Z.L.* Dynamic logics of networks : information flow and the spread of opinion. // Institute for Logic, Language, and Computation, Universiteit van Amsterdam, PhD preprint. 2016. P. 196.

УДК 544.131

Классификация конформационных структур аморфных полимеров в интересах мембранной технологии

О.А. Милосердов[1,2], М.В. Губко[1,3]

[1]Институт проблем управления им. В.А. Трапезникова РАН
[2]Институт нефтехимического синтеза им. А.В. Топчиева РАН
[3]Московский физико-технический институт (государственный университет)

Мембранное газоразделение является одним из быстро развивающихся направлений мембранной науки и технологии. Полимерные газоразделительные мембраны имеют широкий круг применения в различных отраслях промышленности:

- концентрирование водорода из отходящих газов каталитического риформинга, сбросных газов нефтехимии для последующего применения в процессах гидрирования для получения ценных химических продуктов, очистки нефти и т. д.;
- получение азота для создания инертной среды и обеспечения пожаро- и взрывобезопасности при хранении опасных веществ, нефтепродуктов, сжиженных углеводородов, тушении пожаров в шахтах, обеспечении условий для длительного хранения пищевых продуктов;
- обогащение воздуха кислородом для обеспечения медицинских нужд и технологических процессов в металлургии.

Однако большинство используемых в современных технологических процессах материалов полимерных мембран разработаны в 80-х годах XX века и по своим характеристикам не в полной мере соответствуют новым задачам мембранного газоразделения. Поэтому требуются новые материалы для создания мембран, отличающихся улучшенными транспортными свойствами. Проведение экспериментов и синтез кажущихся перспективными полимеров требует больших средств и времени, поэтому большое значение имеют математические модели, способные предсказывать свойства интересующих полимеров по их структуре. Эти модели позволяют получить структурную формулу полимера с оптимальным набором транспортных свойств. Тем самым экономятся финансовые и временные ресурсы, которые были бы затрачены на поиск, подбор и синтез полимеров с худшими характеристиками.

В данной работе были использованы подходы и результаты, полученные в [1], для подтверждения гипотезы о возможности построения классификации полимеров, используемых в газоразделительных мембранах, по конформациям (пространственной конфигурации) их молекулярных цепей. Подобная классификация уже давно существует для белков, которые являются органическими полимерами (α-спираль, спираль коллагена, складчатые структуры, β-петля) [2]. Создание аналогичной белкам классификации полимерных конформаций будет полезным и для полимеров, используемых в мембранном газоразделении. Однако эта задача гораздо сложнее, чем в случае с белками. Число разнообразных структур и способов их организации для аморфных полимеров во много раз превосходит этот параметр для белков. Также при анализе транспортных свойств полимера важно учитывать взаимодействие с десятками газов-пенетрантов, а не только с водной средой, чем обычно ограничиваются в случае белков, что сильно повышает вычислительную сложность задачи.

Модель, предложенная в [1], основана на компьютерном моделировании конформаций коротких участков макромолекул и методологии предсказания свойств веществ по их структуре. В качестве обучающей (345 наблюдений) и тестовой (146 наблюдений) выборки была использована часть базы данных «Газоразделительные

параметры стеклообразных полимеров», поддерживаемая в Лаборатории мембранного газоразделения ИНХС с 1998 года. В качестве характеристик полимерной цепи использовались кривые зависимости площади полимерной цепи от радиуса обкатки, а также для площадей поляризованной/неполяризованной, положительно и отрицательно заряженной площади. Они позволили предсказывать с хорошей точностью растворимость легких газов в стеклообразных полимерах. Скорректированный коэффициент детерминации составил $R^2 = 0.82$ на обучающей и $R^2 = 0.79$ на тестовой выборке.

После проведения визуального анализа конформаций из набора данных, используемого в [1], было отмечено, что присутствует несколько типовых структур (различного вида спирали, изломы, клубки и прочие), при этом полимеры разной природы могут иметь очень похожие конформации цепи, что позволяет быть уверенными в успешном построении классификации. Для повышения точности вычисления площади поверхности обкатки (accessible surface area, ASA) в химическую СУБД Instant JChem компании ChemAxon нами была встроена возможность ее вычисления по алгоритму Ли-Ричардса [3]. Также написан код для вычисления полярной (ASA_{POLAR}) и неполярной (ASA_{APOLAR}) площади поверхности обкатки.

Для первичной проверки гипотезы о возможности построения классификации полимеров из базы данных [1] были выбраны 16 полимеров, для каждого из них построено по три конформации и вычислены три топологических индекса ASA, ASA_{APOLAR} и ASA_{POLAR}. Проведя визуальный анализ, мы установили, что при исследовании кривых зависимости площади обкатки от радиуса обкатки для нескольких полимеров выделяются несколько видов кривых, а следовательно, их можно будет разделить на классы (см. рис. 1).

В дальнейшем аналогичным образом будут рассчитаны показатели большого числа стеклообразных полимеров из базы [1], полученные кривые будут подходящим образом параметризованы (например, наличие или отсутствие изгиба кривых, убывание или возрастание кривых, угол наклона кривых и т.д.), так что каждому полимеру будет сопоставлена точка в конечномерном пространстве. Также будет вычислено большее количество топологических индексов. С помощью методов машинного обучения с учителем (классификация) и без учителя (кластеризация) будет разработана классификация конформаций полимеров, а также исследована связь конформаций и транспортных свойств (диффузия, проницаемость и растворимость).

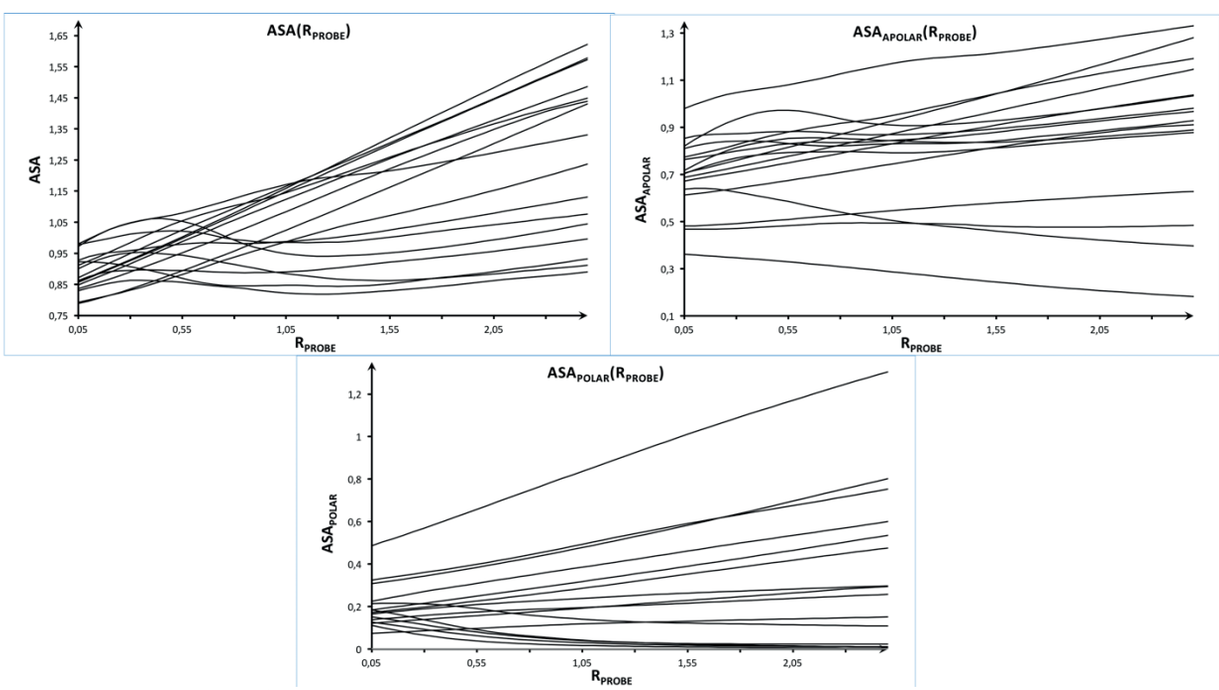


Рис. 1. Графики зависимости площадей поверхности обкатки (полной, незаряженной и заряженной) от радиуса молекулы обкатки

Литература

1. *Goubko M., Miloserdov O., Yampolskii Yu., Alentiev A., Ryzhikh V.* A novel model to predict infinite dilution solubility coefficients in glassy polymers // Journal of Polymer Science Part B: Polymer Physics. 2016. V. 55, N 3. P. 228–244.
2. *Кольман Я., Рем К.-Г.* Наглядная биохимия/ пер. с нем. М.: Мир. 2000. 469 с.
3. *Lee, B; Richards*, FM. "The interpretation of protein structures: estimation of static accessibility"// J Mol Biol. 1971. 55 (3): 379–400.

УДК 330.45, 519.813.7

Константное поведение игроков в экспериментальных играх по распределению ресурса с точки зрения обучения с подкреплением

***В.О. Корепанов*[1]**

[1]Московский физико-технический институт (государственный университет)

В данных серии экспериментальных игр по распределению ограниченного ресурса между игроками ранее было обнаружено большое количество константного поведения (КП) – когда в течение какого-то промежутка времени действия игрока неизменны (с некоторой точностью), см. [1]. При этом в большинстве ситуаций такое поведение не соответствует ни поведению наилучшего ответа, ни даже поведению в сторону наилучшего ответа, что кажется нерациональным. С другой стороны, поведенческая теория игр могла бы объяснять нерациональность через модели ограниченной рациональности.

Вместе с тем дизайн проводимых экспериментальных игр был нетрадиционен – игроки получали реальное вознаграждение за выигрыш на последнем шаге игры, таким образом встаёт вопрос о влиянии дизайна игры на наблюдаемое поведение игроков.

Понять причину КП важно также и потому, что полученные данные по итоговому распределению ресурса (распределение ресурса на последнем шаге игры) оказались интересны с двух точек зрения: неэффективности распределения при том, что механизмы обладали очень хорошими теоретическими свойствами и обнаруженной проблемой манипулируемости данных механизмов [2].

В данной работе базовая идея для попытки объяснения КП состоит в том, что люди проявляют поведение, основанное на обучении с подкреплением: «нащупывают» действия, приносящие больший выигрыш. КП же обусловлено тем, что игрок понимает нестабильность обстановки и стремится оценить выигрыш не по одному наблюдению (выигрыш на данном шаге), а по нескольким (выигрыш от данного действия на нескольких шагах).

Таким образом КП можно разделить на 2 режима: «наблюдение» и «выбор». В режиме наблюдения игрок не меняет свою заявку (с заданной погрешностью), наблюдая как на это отреагируют оппоненты, в режиме выбора игрок выбирает следующее действие для наблюдения. При этом у игрока должно быть два принципа принятия решения: принцип окончания наблюдения и принцип выбора нового действия.

Для принципа окончания наблюдения было выдвинуто несколько гипотез:

(1). Заданное количество шагов.

(2). Падение выигрыша

(3). Выигрыш больше заданного порога

В работе приводится исследование данных для игры распределения ресурса с механизмом Yang-Hajek [3].

Для проверки гипотезы (1) была собрана статистика по длинам всех КП (количество шагов, когда действие игрока не менялось). Оказалось, что распределение длин близко к распределению Парето, при этом на долю КП с длиной 2 пришлось около 57% данных. Если рассматривать отдельно игроков разных типов, то картина примерно похожая. Получается гипотеза не верна, но при этом более половины КП являются двухшаговыми.

Гипотеза (2). Данные показали, что в 75% случаев КП происходит снижение среднего значения выигрыша, если сравнивать выигрыши в начале и в конце КП (первая и вторая половины шагов КП). Таким образом можно считать, что игроки обращают внимание на падение выигрыша и если он присутствует, то они заканчивают режим «наблюдения». При этом сказать точно при каком падении выигрыша это происходит данные не позволяют – в каждом конкретном случае КП величина падения различается, в т.ч. бывают сильные падения в течение КП, после которого «наблюдение» не заканчивается.

Гипотеза (3) для всего набора данных не подтвердилась. Пока остался невыясненным вопрос есть ли порог по выигрышу у каждого игрока в отдельности.

Далее был поставлен вопрос является ли выигрыш информативным признаком, т.е. таким признаком на котором строится принцип окончания наблюдения: КП от не КП и КП длящиеся 2 шага и длящиеся больше 2 шагов? Оказалось, что ответ отрицательный, по крайней мере для линейных неядерных методов классификации, т.к. классы оказываются сильно перемешанными, если рассматривать два признака (выигрыш на прошлом шаге, выигрыш/прирост выигрыша на текущем шаге).

С помощью методов выделения признаков был проведён поиск информативных признаков из набора (полученный ресурс на прошлом шаге, полученный выигрыш на прошлом шаге, полученный штраф на прошлом шаге, прирост полученного ресурса на текущем шаге, прирост полученного выигрыша на текущем шаге, прирост полученного штрафа на текущем шаге). В данном случае также не удалось перейти к значимым признакам, которые бы позволили построить линейный классификатор для двух заданных классов КП.

В работе получены предварительные данные по исследованию константного поведения игроков в играх по распределению ресурса. Результаты пока не позволяют выделить критерии, по которым игроки выбирают изменять своё действие или нет. Попытка связать эти критерии с получаемыми игроками ресурсами, выигрышами и штрафами в игре с помощью методов выделения признаков и классификации пока не удалась. Дальнейшие исследования будут продолжаться в этом направлении и в направлении поиска модели принятия решений игроками при выборе нового действия.

Работа выполнена при поддержке гранта РФФИ № 17-07-01550 А.

Литература

1. *Коргин Н.А., Корепанов В.О.* Решение задачи эффективного распределения ресурсов на основе механизма Гровса-Лейдярда при трансферабельной полезности //Управление большими системами: сборник трудов. – 2013. – №. 46.
2. *Korgin, N.A., Korepanov V.O*. Experimental gaming analysis of ADMM dynamic distributed optimization algorithm // IFAC-PapersOnLine 49.12 (2016): 574-579.
3. *Yang, S., Hajek B*. "Revenue and stability of a mechanism for efficient allocation of a divisible good." preprint (2005).

Секция радиофизики и радиоэлектронных информационных систем

УДК.621.371

Исследование обратного рассеяния металлодиэлектрических объектов

А.В. Тихонова, С.В. Елизаров

ОАО «Радиофизика»
Московский физико-технический институт (государственный университет)

В настоящее время разработчиками летательных аппаратов и двигателей для них всё чаще предлагается вместо металлических элементов и поверхностей использовать в конструкции изделий композитные материалы. При этом, учитывая, что далеко не все элементы металлической конструкции летательного аппарата возможно заменить на композиты, подобная частичная замена может значительно увеличить радиолокационную заметность.

Действительно, из-за наличия множества протяженных участков стыков «металл–диэлектрик» и при необоснованном выборе электрофизических характеристик композитных диэлектрических покрытий в секторах углов, которые не относятся к зеркальным направлениям локации объектов [1], указанные стыки могут значительно увеличивать уровень эффективной площади рассеяния (ЭПР) подобных изделий [2].

Целью работы являлось определение ЭПР модельных тел в секторах углов, которые не относятся к зеркальным направлениям локации. Дополнительно оценивалось влияние электрофизических характеристик материалов, размещенных на стыке «металл–диэлектрик», на увеличение обратного рассеяния исследуемых объектов.

В настоящей работе с учетом бурного роста компьютерных мощностей было решено использовать для расчётов метод конечных разностей во временной области, который основывается на дискретизации уравнений Максвелла, используя аппроксимацию по времени и пространственным координатам.

Для исследования были выбраны 3D–модели тел цилиндроконического типа, позволяющие в заданных секторах углов падения электромагнитной волны на объект, которые не относятся к зеркальным направлениям локации, исследовать вклад протяженного стыка «металл–диэлектрик» в обратное рассеяние. Исследование проводили для модельных тел с фиксированным приведенным диаметром основания конусов λ и различными углами при вершине конусов. Облучение проводилось как со стороны металла, так и со стороны диэлектрика.

В ходе работы был проведён анализ ДОР для объектов конусного типа и было показано, что при этом критерий разбиения поверхности объекта на фацеты в отличие от тел цилиндрического типа должен учитывать дополнительные параметры. Было установлено, что для металлических тел цилиндрического типа оптимальный с точки зрения соотношения «скорость расчета/точность расчета» размер фацета составляет значение $\lambda/4$, для объектов цилиндроконического типа со стыками «металл- диэлектрик» размер фацета должен быть не более $\lambda/7$.

Показано, что при определённых значениях электрофизических характеристик покрытий их скачок на стыках, образованных разнородными материалами, увеличивает обратное рассеяние объекта в исследуемых секторах углов больше, чем геометрический разрыв (щель, канавка) на металлических поверхностях. Поэтому, несмотря на целесообразную с точки зрения снижения массы изделия замену металлических элементов или их поверхностей на композитные материалы, подобные мероприятия при необоснованном выборе диэлектрических характеристик указанных покрытий могут значительно увеличивать уровень радиолокационной заметности летательного аппарата.

Литература

1. *Елизаров С.В., Краснолобов И.И., Лебедев А.М., Семененко В.Н., Федоренко А.И., Фурманова Т.А.* Минимизация вклада в обратное рассеяние от поверхностных волн на тонком металлическом стержне путём нанесения радиопоглощающего покрытия на один из концов стержня // Труды конференции «Излучение и рассеяние электромагнитных волн ИРЭМВ-2013». 2013. С. 329–333.
2. Радиолокационные характеристики объектов: Методы исследования: монография / под ред. С.М. Нестерова. М.: Радиотехника, 2015. С. 309.

УДК 621.396.96

Влияние сглаживания координат на характеристики отождествления целей в пункте боевого управления

И.О. Девятьяров[1], В.А. Доброжанский[2]

[1]Московский физико-технический институт (государственный университет)
[2]ПАО «НПО «Алмаз»

Рассмотрен алгоритм формирования единого массива трасс, алгоритм сглаживания координат и элементов ковариационной матрицы, а также влияние сглаживания на характеристики отождествления.

Отождествление трасс является частью алгоритма формирования единого массива трасс (ЕМТ) пункта боевого управления (ПБУ) перспективного зенитного ракетного комплекса (ЗРК). Отождествление включает в себя три этапа: экстраполяция к единому времени, отождествление по координатам и отождествление по скорости. Отождествление по координатам принимается по результатам вычисления обобщённого расстояния между трассами по формуле

$$\left(\lambda_i - \lambda_j\right)^T K_\lambda^{-1}\left(\lambda_i - \lambda_j\right) < C_1,$$

где $\lambda = (x, y, z)^T$– вектор декартовых координат, K_λ – ковариационная матрица разности координат, C_1 — пороговое значение.

В многофункциональном радиолокаторе (МФР) сглаживание координат целей производится в биконической системе координат (БСК) с помощью рекуррентных α−β фильтров. Для сглаженных координат справедлива следующая формула [1]:

$$\hat{\lambda}_i = \alpha\lambda_i + (1-\alpha)\hat{\lambda}_{эi},$$

где $\hat{\lambda}_i$ – сглаженные значения координаты на текущий момент времени t_i, α – текущий, на момент времени t_i, коэффициент сглаживания по координате, λ_i – текущее измерение координаты (R, $\varphi_н$, $\varphi_в$), $\hat{\lambda}_{эi} = \hat{\lambda}_{i-1} + \hat{\dot{\lambda}}_{i-1}\,\Delta t$ – экстраполированная оценка координаты на текущий момент времени t_i.

Оценки координат, полученные на выходе α−β фильтра, передаются на ПБУ в декартовой местной земной системе координат МФР и сопровождаются информацией об ошибках оценивания, передаваемых в виде ковариационной матрицы оценки координат [2].

Для исследования характеристик отождествления было произведено моделирование приема ПБУ трассовой информации от двух МФР. Воздушная обстановка состояла из двух целей, причём было сделано допущение, что каждая цель сопровождается только одним МФР. Для алгоритма отождествления построена зависимость вероятности наличия в ЕМТ двух трасс от относительного расстояния между целями — вероятность правильного отождествления (ВПО). Координаты цели в БСК для модели обнаружения цели представляли собой нормально распределённую случайную величину с математическим ожиданием, равным истинному положению целей, и заданными СКО.

На рис. 1 приведено сравнение зависимости «эталонной» (полученной для распределения χ^2 со значением ошибки первого рода 0.01) ВПО от расстояния между целями с ВПО «сглаженных» координат целей (оцененных на выходе α−β фильтра). Сравнение производилось для случая, когда отождествление трасс в ПБУ производится

одновременно с оценкой координат целей в МФР. Из рис. 1 видно, что сглаживание координат в МФР в таком случае не влияет на зависимость ВПО от расстояния между целями.

При работе реальных МФР и ПБУ моменты времени оценки координат целей в различных МФР не синхронизируются. Кроме того, существует задержка с момента времени, в который производится оценка координат целей, до начала формирования ЕМТ, обусловленная темпом передачи информации о целях с МФР на ПБУ и темпом работы алгоритма формирования ЕМТ. Таким образом, в ПБУ необходимо производить экстраполяцию координат целей, полученных от МФР, на момент отождествления. На рис. 2 приведено сравнение «эталонной» ВПО с ВПО «сглаженных» координат для случая, когда в ПБУ производится экстраполяция координат целей на момент отождествления. Из рис. 2 видно, что в таком случае характеристика отождествления далека от «эталонной».

Данную проблему предложено решать путем выдачи от МФР на ПБУ совместно с координатами целей ковариационной матрицы оценки координат, экстраполированных на следующий такт сопровождения вместо ковариационной матрицы оценки текущих координат. Результат такого подхода представлен на рис. 3. Таким образом, предложенный подход позволяет решать задачу отождествления координат целей с использованием ковариационной матрицы оценок координат в ПБУ.

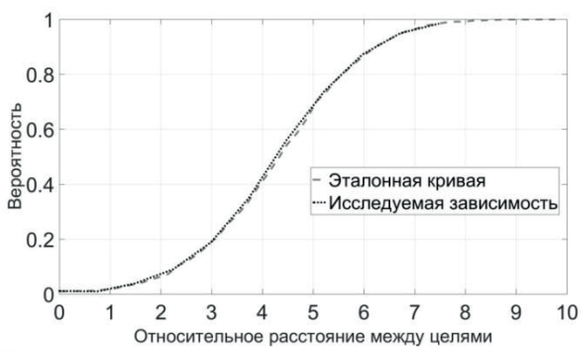


Рис. 1. ВПО для синхронного отождествления и сопровождения целей

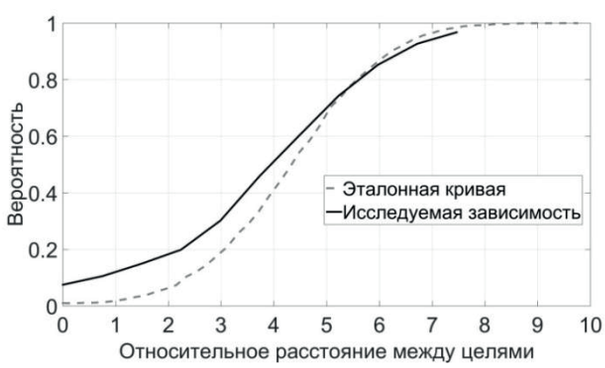


Рис.2. ВПО для асинхронного отождествления и сопровождения целей

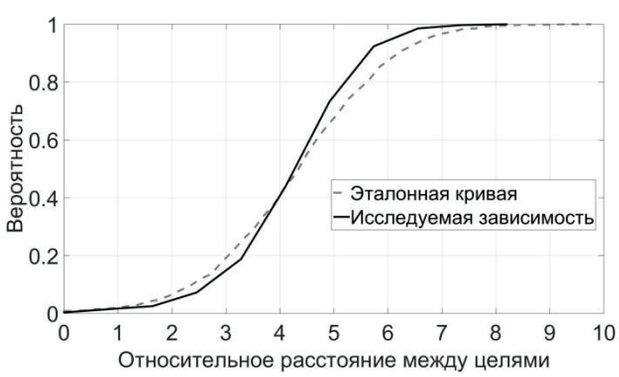


Рис. 3. ВПО для асинхронного отождествления и сопровождения целей с учётом ковариационной матрицы экстраполированных координат

Литература

1. *Биченко И. Г., Волков В. Н., Доброжанский В. А.* Алгоритмы адаптивной фильтрации координат при сопровождении целей в многофункциональном радиолокаторе с секторным и круговым режимами работы. Вторая научно-техническая конференция молодых ученых и специалистов. Сборник докладов. М., Радиотехника, 2012.
2. *Биченко И. Г., Доброжанский В. А.* Отождествление трассовой информации многофункциональных радиолокаторов с учетом ковариационной матрицы ошибок координат. Антенны. М.: Радиоётехника, 2013.

УДК.621.336.96

Оценка влияния фазовых флуктуаций гетеродинных сигналов на результат оптимальной фильтрации ЛЧМ–сигналов в РЛС с когерентным накоплением импульсов

Е.М. Макарычев[1], И.А. Григорьев[2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Радиофизика»

Гетеродины, в качестве которых используются высокостабильные источники частоты, являются важным компонентом большинства радиочастотных и беспроводных систем, характеристики которых непрерывно улучшаются последние десятилетия. Улучшение этих характеристик в свою очередь приводит к повышению технических требований, предъявляемых к источникам частоты, используемым в качестве гетеродинов. Так, существующие задачи в области радиолокации, навигации и связи, требующие длительного накопления принимаемого сигнала, сделали актуальным вопрос о влиянии стабильности всех компонентов системы, в том числе и гетеродинов, на результат оптимальной обработки сигналов.

Необходимость использования высокостабильных источников сигналов в радиолокационных системах обусловлена прежде всего решением задач получения и обработки информации о наблюдаемом объекте с минимальными фазовыми и амплитудными искажениями [1]. В связи с применением в импульсной радиолокации когерентного накопления отраженных от наблюдаемого объекта радиочастотных импульсов, еще более важным вопросом, возникающим в ходе построения станции, является соблюдение когерентности принимаемых импульсов в течение достаточно длительных для детектирования полезного сигнала временных интервалов.

Оценка степени влияния фазовой нестабильности гетеродинных источников на качественные показатели работы станции позволяет сформировать набор требований, в соответствии с которыми должен проводиться выбор принципиальной схемы построения и базовых компонентов гетеродина [2]. Это может быть кварцевый генератор, сопряженный с каскадом умножения для формирования однотонового стабильного колебания или синтезатор частоты на базе кольца ФАП или цифровых схем формирования с целью реализации частотной перестройки.

Данная работа посвящена исследованию влияния фазовых шумов выходного сигнала гетеродина на результат оптимальной обработки ЛЧМ–сигналов в РЛС с накоплением импульсов. Расчёт результата оптимальной обработки ЛЧМ–сигнала производился для модели РЛС с упрощённым приёмно-передающим трактом. В качестве фазовых шумов использовался заранее сгенерированный массив значений шума с заданной спектральной плотностью.

Анализ влияния фазовых шумов производился для работы РЛС в моноимпульсном режиме и режиме когерентного накопления пачки импульсов. Для моноимпульсного режима анализ производился для различных значений длительности импульса, дальности до цели, девиации зондирующего сигнала, а также рассматривались различные спектральные характеристики фазовых шумов гетеродина. При анализе работы РЛС в

режиме когерентного накопления пачки импульсов дополнительно варьировались частота повторения импульсов и время накопления.

Литература

1. *Raven R.S.* Requirements on Master Oscillators for Coherent Radar // Proceedings of the IEEE. Publication. 1966. P. 237–243.
2. *Skolnik M.I.* Radar Handbook // The McGraw-Hill Companies, 2008.

УДК 621.3.095.1

Разработка модели функционирования алгоритмов распознавания осесимметричных объектов наблюдения по поляризационным признакам

А.А. Копылов

Московский физико-технический институт (государственный университет)

Целью работы является разработка модели функционирования алгоритмов распознавания осесимметричных объектов наблюдения (ОН) по поляризационным признакам [1].

Алгоритмы распознавания разработаны для классификации осесимметричных объектов наблюдения по поляризационным признакам.

Модель состоит из функциональных модулей. Каждый модуль отвечает за решение определенной задачи в соответствии с алгоритмами распознавания осесимметричных объектов наблюдения по поляризационным признакам. Блок-схема модели показана на рис. 1.

Модель алгоритма распознавания, основанного на использовании параметров типа параметров Стокса [2], и модель алгоритма распознавания, основанного на использовании параметров двухвибраторной модели [3], для удобства реализации были объединены в одну модель.

Для демонстрации функционирования описываемой модели были рассмотрены практические примеры моделирования алгоритмов для распознавания объектов наблюдения следующих классов:

- сфера (диаметр – 6 λ);
- сфера (диаметр – 10 λ);
- конус (высота – 6 λ, диаметр основания – 6 λ);
- конус (высота – 17.2 λ, диаметр основания – 5.4 λ);
- цилиндр (высота – 6 λ, диаметр основания – 6 λ);
- цилиндр (высота – 21.7 λ, диаметр основания – 9.6 λ).

Для данных классов были построены эталоны, которые содержат средние значения и среднеквадратические отклонения рассматриваемых поляризационных признаков, а также номера тех признаков, которые являются наиболее информативными для каждого класса.

Распознавание ОН проводилось по проверочным реализациям с добавлением шумов для имитированных ОН перечисленных классов.

Таким образом, в работе представлена разработанная модель функционирования алгоритмов распознавания осесимметричных объектов наблюдения по поляризационным признакам.

Кроме того, приведены примеры моделирования функционирования алгоритмов распознавания осесимметричных объектов наблюдения по поляризационным признакам, которые показали корректную работу разработанной модели.

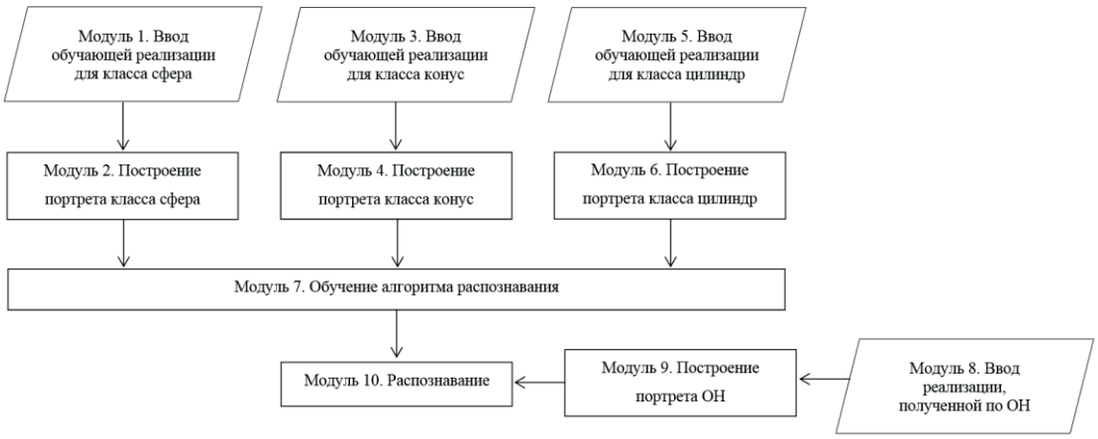


Рис. 1. Блок-схема модели функционирования алгоритмов распознавания осесимметричных объектов наблюдения по поляризационным признакам

Литература

1. *Копылов А.А., Кобельков Г.П., Зимин И.В.* Разработка и исследование алгоритмов распознавания осесимметричных объектов наблюдения по поляризационным признакам // Тезисы докладов III Международной конференции «Инжиниринг & Телекоммуникации – En&T 2016», Москва/Долгопрудный. 2016. С. 91–94.
2. *Козлов А.И., Логвин А.И., Сарычев В.А.* Поляризация радиоволн. Поляризационная структура радиолокационных сигналов. М.: Радиотехника, 2005.
3. *Канарейкин Д.Б., Павлов Н.Ф., Потехин В.А.* Поляризация радиолокационных сигналов. М.: Сов. радио. 1966.

УДК.621.336.96

Разработка и исследование гибридного DDS-PLL синтезатора с алгоритмом подавления побочных дискретных составляющих

А.А. Суханов[1,2], И.А. Григорьев[2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Радиофизика»

Работа посвящена разработке гибридного DDS-PLL-синтезатора частот с подавлением побочных дискретных составляющих. Целью работы является снижение влияния нелинейности ЦАП микросхемы DDS на спектральные характеристики выходных сигналов [1]. В работе представлены результаты исследования спектральных характеристик синтезатора выполненного с применением алгоритма частотной коррекции, который обеспечивает оптимальные сетки частот обеих микросхем DDS в составе синтезатора [2]. В ходе работы существующий алгоритм был оптимизирован с учетом имеющихся зависимостей уровня гармоник от их номера на выходе синтезатора, а также амплитудно-частотной характеристики петли ФАПЧ. Сравнение полученных спектральных характеристик на предварительно выбранной для исследования литерной частоте показало эффективность схемы синтезатора с двумя DDS и существующим алгоритмом частотной коррекции. Доработка существующего алгоритма позволила обеспечить дальнейшее снижение уровня мешающих гармоник и достичь обозначенного в требованиях уровня – 100 дБн. Также были выявлены возможности для дальнейшего улучшения спектральных характеристик гибридного синтезатора в случае предъявления более жестких требований на спектральные характеристики к конечному изделию. Использование одной из микросхем DDS вместо целочисленного делителя в цепи обратной связи ФАПЧ не привело к существенному увеличению уровня фазовых шумов.

Литература

1. *Макарычев Е.М., Григорьев И.А.* Оценка влияния нелинейных искажений цифрового и аналогового трактов DDS на спектры гетеродинных сигналов в области доплеровских отстроек // Радиотехника. 2015. №4. С. 42–48.
2. *Очков Д.С., Формальнов И.С., Григорьев И.А., Макарычев Е.М.* Способ получения радиочастотного сигнала: патент на изобретение №2579570.

УДК 537.874.6

Разработка модели для расчета поляризационной матрицы рассеяния для осесимметричных объектов наблюдения в зависимости от угла между осью симметрии и линией визирования.

Е.Г. Паринов

Московский физико-технический институт (государственный университет)

Целью работы является разработка модели для расчета поляризационной матрицы рассеяния(ПМР) для осесимметричных объектов наблюдения(ОН) в зависимости от угла между осью симметрии и линией визирования.

Полученные массивы замеров ПМР были использованы для моделирования алгоритмов распознавания осесимметричных ОН по поляризационным признакам.

В данной работе была разработана модель для расчета ПМР для идеально проводящих осесимметричных ОН в зависимости от угла между осью симметрии и линией визирования. Для получения ПМР была разработана методика решения задачи дифракции произвольной плоской электромагнитной волны (ЭМВ) на осесимметричном теле. Из граничных условий на поверхности тела после замены поля распределением поверхностных токов получаем интегро-дифференциальное уравнение:

$$\vec{n}\times\vec{E}^{inc}=\vec{n}\times\left(\frac{i\omega}{4\pi}\iint\limits_{S}\vec{J}(\vec{\mathrm{r}}')\,\mathrm{G}(\vec{\mathrm{r}},\vec{\mathrm{r}}')dS'+\frac{i}{4\pi\omega}\nabla\iint\limits_{S}(\nabla_{S'}\cdot\vec{J}(\vec{\mathrm{r}}'))\,\mathrm{G}(\vec{\mathrm{r}},\vec{\mathrm{r}}')dS'\right) \quad (1)$$

здесь $\vec{E}^{inc}$ – падающее электрическое поле, ω – круговая частота, S – поверхность тела, G – функция Грина, $\vec{n}$ – единичный вектор нормали, направленный от поверхности тела.

Решение интегро-дифференциального уравнения (1) позволяет рассчитать поле в дальней зоне, а также ЭПР объекта. Эта методика основана на методе моментов и использует осесимметричность тела [1].

Изначально элементы ПМР рассчитываются в линейном базисе. В случае, если необходимо представить элементы в круговом базисе, применяются соответствующие преобразования.

Для определения углов между линией визирования и осью симметрии тела проводилось моделирование движения объектов наблюдения.

В итоге модель состоит из 4 блоков.

- Моделирование движения ОН.
- Определение углов между линией визирования и осью симметрии ОН.
- Решение задачи дифракции плоской ЭМВ на ОН.
- Преобразование элементов ПМР.

Для верификации модели были проведены сравнения результатов расчетов, получаемых с помощью модели, с результатами экспериментальных измерений [2] и теоретическими решениями [3], имеющимися в литературе. Результаты верификации показали, что модель дает достоверные результаты расчета рассеяния плоской ЭМВ на осесимметричном ОН.

Были рассмотрены некоторые конкретные практические примеры использования модели, в частности, получены реализации замеров ПМР в зависимости от времени наблюдения ОН для следующих тел:

1) сфера (радиус 3 λ),

2) сфера (радиус 4 λ),
3) конус (высота 6 λ, диаметр основания 6 λ),
4) конус (высота 4 λ, диаметр основания 4 λ),
5) цилиндр (высота 6 λ, диаметр основания 6 λ).

На рис. 1 и рис. 2 изображены ЭПР ОН в зависимости от времени наблюдения. На рис. 1 ОН – конус с параметрами: высота 6 λ, диаметр основания 6 λ. На рис. 2 ОН – цилиндр с параметрами: высота 6 λ, диаметр основания 6 λ. В системе координат, связанной с радиолокационной станцией, начальные координаты ОН: $x_0 = 976.5$ км, $y_0 = 913.5$ км, $z_0 = 1100$ км. Начальные скорости: $V_{x0} = -3.1$ км/с, $V_{y0} = -2.9$ км/с, $V_{z0} = -3.5$ км/с. Сплошной линией обозначена вертикальная поляризация, пунктирной – горизонтальная. Время измеряется в секундах, ЭПР в дБм^2.

Таким образом, была разработана модель для расчета ПМР для осесимметричных ОН в зависимости от угла между осью симметрии и линией визирования. Результаты верификации показали приемлемую точность результатов. Также были приведены примеры моделирования замеров ПМР в зависимости от времени наблюдения ОН для различных тел (сфера, конус, цилиндр).

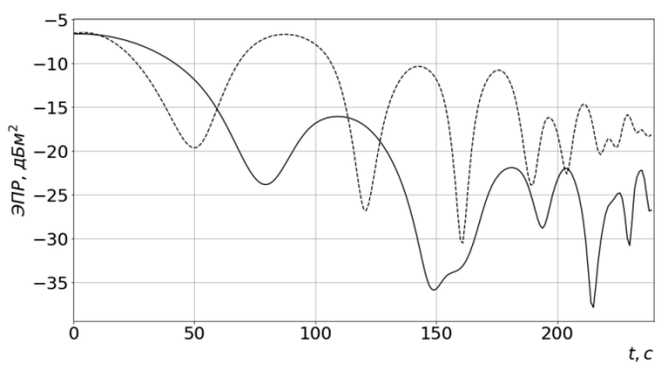


Рис. 1. Зависимость ЭПР конуса высотой 6 λ и диаметром основания 6 λ от времени наблюдения

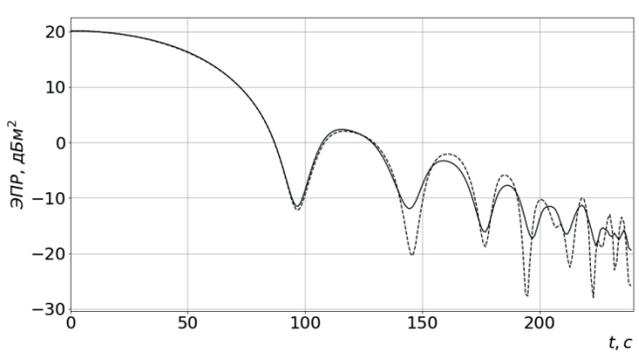


Рис. 2. Зависимость ЭПР цилиндра высотой 6 λ и диаметром основания 6 λ от времени наблюдения

Литература

1. *Glisson A.W., Wilton D.R.* Simple and Efficient Numerical Techniques for Treating Bodies of Revolution // Mississippi Univ University. 1979. P. 137.
2. *Escot-Bocanegra D., Poyatos-Martinez D., Fernandez-Recio R., Jurado-Lucena A., Montiel-Sanchez I.* New bench-mark radar targets for scattering analysis and electromagnetic software validation // Progress in Electromagnetics Research. 2008. V. 88. P. 39 – 52.
3. *Kerker M.* The Scattering of Light and Other Electromagnetic Radiation. – New York: Academic, 1969. P. 666.

УДК 537.8

Излучение релятивистского электрона в фотоннокристаллической структуре

В.А. Астапенко[1], Е.С. Мануйлович[1], С.В. Сахно[1], Ю.А. Кротов[2]

[1] Московский физико-технический институт (государственный университет)
[2] Научно-исследовательский институт «Полюс» им. М.Ф. Стельмаха

Рассмотрена задача взаимодействия релятивистского электрона с фотоннокристаллической структурой. Целью настоящей работы является анализ спектра рассеяния эквивалентных фотонов.

В докладе приведены результаты исследования излучения быстрого электрона в фотонной кристаллической структуре по методу Ферми эквивалентных фотонов [1]. В этой модели рассматривается рассеяние поля эквивалентных фотонов релятивистского электрона при распространении электрона в фотонно-кристаллическом волноводе с боковой полостью и вставками-дефектами [2]. В цитированной работе коэффициент пропускания такой структуры рассчитывается в зависимости от параметров модели. В настоящей работе коэффициент пропускания используется для получения потока фотонов в результате взаимодействия собственного поля падающего электрона. Аналогичный метод был использован для расчета поляризационного тормозного излучения быстрых электронов на металлических наносферах [3].

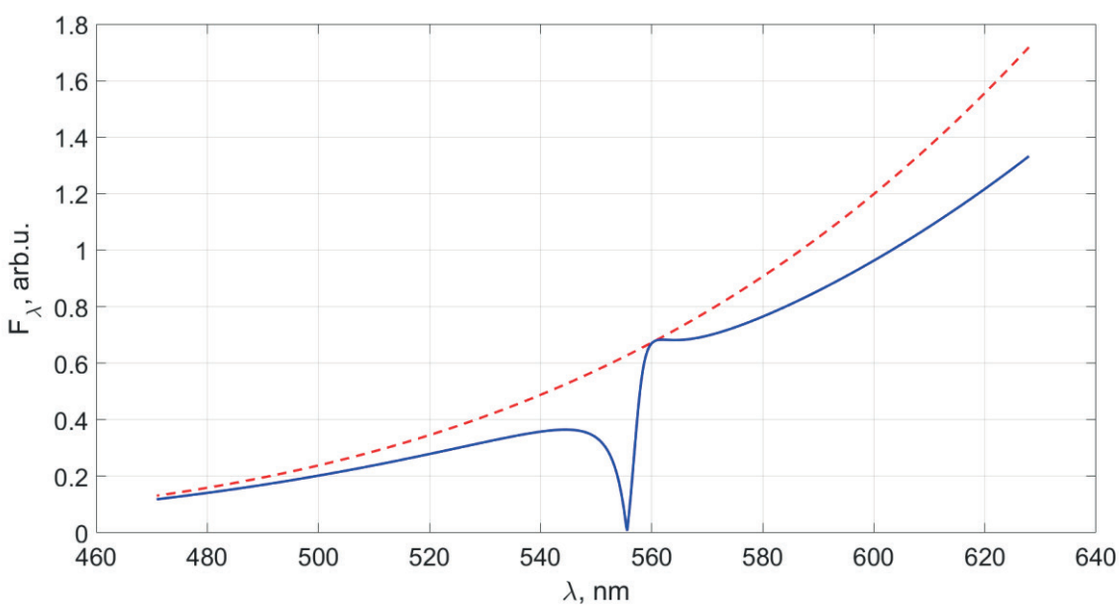


Рис. 1. Спектр эквивалентных фотонов релятивистского (v_e/c = 0.25) электрона (пунктирная линия), спектр прошедшего излучения (сплошная линия)

Результаты расчетов показали, что спектр рассеяния эквивалентных фотонов (см. рис. 1) имеет резонансный характер с ярко выраженным минимумом типа Фано.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 16-37-00108 мол_а.

Литература

1. *Fermi E.* Uber die Theorie des Stossen zwishen Atomen und electrisch geladenen Teilchen // Z. Physik. 1924. V. 29. P. 315.
2. *Shanhui F.* Sharp asymmetric line shapes in side-coupled waveguide-cavity systems // Applied physics letters. 2002. V. 80. I. 6. P. 908.
3. *Astapenko V.A., Sakhno S.V., Krotov Yu. A.* Polarization bremsstrahlung of fast electrons on metal nanospheres in a dielectric matrix in view of plasmon interference effects // Journal of Physics: Conference Series. 2016. V. 732. P. 012025.

УДК 535.3

Рассеяние электромагнитного излучения на полупроводниковых наночастицах ITO

В.А. Астапенко, Е.С. Мануйлович, С.В. Сахно, Е.С. Храмов, Е.В. Сахно

Московский физико-технический институт (государственный университет)

Полупроводниковые наночастицы обладают рядом особенностей, которые делают их привлекательными для практического использования: например, частоты локализованных поверхностных плазмонных резонансов (Localized Surface Plasmon Resonance, LSPR) лежат в видимом и в ИК-диапазонах [1], причем частота LSPR может быть изменена путем введения легирующих примесей и изменением размера самой наночастицы.

В данной работе рассчитывается величина спектрального сечения рассеяния электромагнитного излучения на полупроводниковых наночастицах ITO. Расчет осуществлялся в рамках теории Ми [2], [3]. Предполагалось, что частицы имеют сферическую форму и помещены в диэлектрическую матрицу. Таким образом, интегральное по углу выражение для сечения рассеяния имеет следующий вид:

$$\sigma_{\text{int}}^{scat}(\omega)=\frac{2\pi c^2}{\omega^2\varepsilon_m}\sum_{n=1}^{\infty}(2n+1)\left(|a_n(\omega)|^2+|b_n(\omega)|^2\right), \tag{1}$$

где c – скорость света в вакууме, ω – частота излучения, ε_m – диэлектрическая проницаемость среды, $a_n(\omega)$ и $b_n(\omega)$ – коэффициенты Ми, которые, в том числе, зависят от радиуса мишени r, ε_m и диэлектрической проницаемости наночастицы $\varepsilon(\omega)$, которая, в данном случае, может быть описана с помощью классической модели Друде [4]:

$$\varepsilon(\omega)=\varepsilon_\infty-\frac{\omega_p^2}{\omega^2+i\omega\gamma}, \tag{2}$$

где ε_∞ – высокочастотная диэлектрическая проницаемость вещества, γ – константа релаксации, ω_p – плазменная частота.

В табл. 1 приведены параметры Друде, которые были получены на основании экспериментальных данных в работе [5].

На рис. 1 приведены результаты расчета сечений рассеяния на наночастицах ITO с разным процентом легирования. Расчет был осуществлен при $\varepsilon_m = 1$, $\varepsilon_\infty = 4.1$ [6].

Как следует из рис. 1, повышение уровня легирования приводит к сдвигу длины волны плазмонного резонанса в коротковолновую область, а также приводит к росту амплитуды резонансного пика и его сужению. Также видно, что с ростом радиуса наночастицы наблюдается увеличение амплитуды сечения при одном и том же уровне легирования.

Таблица 1

Параметры Друде наночастиц ITO с различным процентным содержанием олова

Легирование, %	5	8	10
ω_p, эВ	1.57	1.72	1.89
γ, эВ	0.21	0.22	0.15

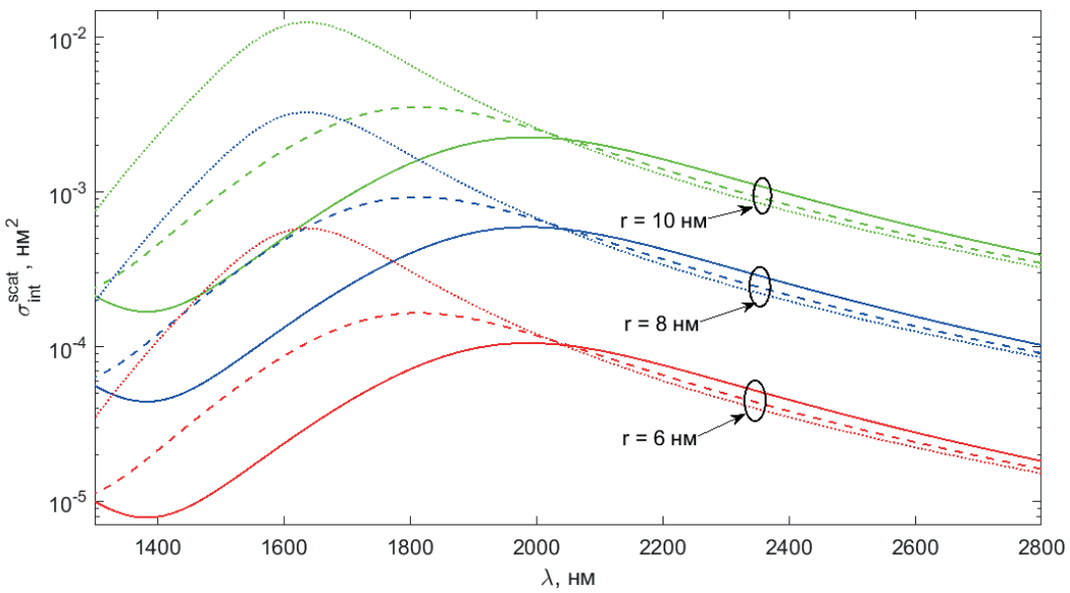


Рис. 1. Зависимости интегрального сечения рассеяния на наночастицах ITO разного радиуса от длины волны излучения при различном процентном содержании олова: сплошная кривая – 5%; штриховая кривая – 8%; штрих-пунктирная кривая – 10%

Работа выполнена при финансовой поддержки Министерства науки и образования РФ, ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (уникальный идентификатор RFMEFI57816X0199).

Литература

1. *Luther J.M., Jain P.K., Ewers T., Alivisatos, A.P.* Localized surface plasmon resonances arising from free carriers in doped quantum dots // Nature Materials. 2011. V. 10. P. 361.
2. *Mie G.* Beiträge zur Optik trüber Medien, speziell kolloidaler Metallösungen // Annalen der Physik. 1908. V. 330. P. 377.
3. *Hulst H. C. van de.* Light scattering by small particles. New York, Dover Publications, 1981. 470 p.
4. *Kuttge M., Kurz H.* [*et al.*]. Analysis of the propagation of terahertz surface plasmon polaritonson semiconductor groove gratings // Journal of Applied Physics. V. 101. I. 2. P. 023707.
5. *Kanehara M., Koike H., Yoshinaga T., Teranishi T.* Indium tin oxide nanoparticles with compositionally tunable surface plasmon resonance frequencies in the near-IR region // Journal of the American Chemical Society. 2009. V. 131. P. 17736.
6. *Solieman A., Aegerter M.A.* Modeling of optical and electrical properties of In_2O_3: Sn coatings made by various techniques // Thin Solid Films. 2006. V. 502. I. 1–2. P. 205.

УДК 621.396.96

К вопросу о сопровождении маневрирующих объектов αβ-фильтром при наличии скоростной ошибки по дальности

М.А. Мурзова

Московский физико-технический институт (государственный университет)
ПАО «Радиофизика»

В радиолокационных станциях обнаружения для зондирования пространства используют линейные частотно-модулированные сигналы (ЛЧМ). При использовании ЛЧМ-сигналов полученные в РЛС измерения дальности содержат скоростную ошибку. Скоростная ошибка возникает из-за доплеровского смещения частоты отраженного сигнала. Следовательно, при разработке алгоритмов сопровождения радиолокационных объектов по данным РЛС с ЛЧМ-сигналом необходимо учитывать в составе входной информации наличие скоростной ошибки по дальности [1].

В [2], [3] рассматривается фильтр Калмана (ФК) в установившемся режиме работы. В модели движения предполагается, что объект движется с постоянной скоростью и ускорением, которое выступает в качестве входного воздействия со случайными характеристиками. В модели измерений предполагается, что измерения содержат скоростную ошибку по дальности. Для данного ФК получены точностные характеристики фильтра, такие как ковариационные матрицы ошибок оценок и ошибок экстраполяции [2]. Также получены сглаживающие коэффициенты α и β фильтра Калмана в установившемся режиме. В [3] получены выражения динамических ошибок по дальности и скорости, возникающих при совершении маневра объектом и учитывающие скоростную ошибку. Выражение, описывающее ковариационную матрицу ошибок сглаживания для αβ-фильтра, получено в работах [3 – 5]. В [3] получены оптимальные сглаживающие коэффициенты αβ-фильтра по критерию минимума среднеквадратического отклонения (СКО) суммарной ошибки (случайной и динамической) по дальности и скорости. Важно отметить, что в [3] при минимизации СКО суммарной ошибки использовалось соотношение между параметрами α и β, полученное в [2]. В [4], [5] получены условия устойчивости αβ-фильтра, зависящие от коэффициента скоростного смещения.

В ряде других работ [6-9] проведено исследование влияния скоростной ошибки на характеристики как фильтров более высокого порядка, так и атмосферных фильтров.

В данной работе получено оптимальное соотношение между сглаживающими коэффициентами α и β, при которых дисперсия суммарной ошибки оценки и ошибки экстраполяции достигает глобального минимума. Используя полученное αβ-соотношение и условие устойчивости αβ-фильтра из [4], [5], получена область допустимых значений параметра фильтра β в зависимости от коэффициента скоростного смещения.

Полученное оптимальное αβ-соотношение минимизирует дисперсию суммарной ошибки, следовательно, улучшает точность сопровождения маневрирующих объектов. В сравнении с [2], [3], при использовании полученного оптимального αβ-соотношения достигается глобальный экстремум.

Литература

1. *Ширман Я.Д.*, *Манжос В.Н.* Теория и техника обработки радиолокационной информации на фоне помех. М.: Радио и связь, 1981.
2. *Wong W., Blair W.D.* Steady-state tracking with LFM waveforms // IEEE Transactions on Aerospace and Electronic Systems. 2000. V. 36, N 2. P. 701−709.
3. *Jain V., Blair W.D.* Filter Design for Steady-State Tracking of Maneuvering Targets with LFM Waveforms // IEEE Transactions on Aerospace and Electronic Systems. 2009. V. 45, N 2. P. 765−773.
4. *Фарбер В.Е.* Анализ характеристик алгоритмов определения параметров движения космических аппаратов по информации радиолокационных средств, использующих зондирующие сигналы с линейной частотной модуляцией // Космические исследования. 1995. Т. 33. № 1. С. 31−35.
5. *Трофименко М.А., Фарбер В.Е.* Оценка влияния наличия скоростной ошибки при измерениях дальности в РЛС с ЛЧМ-сигналом на границы устойчивости алгоритмов оценки дальности и радиальной скорости // Радиотехника. 2015. № 10. С. 7−16.
6. *Трофименко М.А., Фарбер В.Е.* Оценка влияния скоростного смещения в радиолокационных станциях с ЛЧМ-сигналом на границы устойчивости сопровождения входящих в атмосферу космических объектов // Труды МФТИ. 2015. Т. 7. № 2. С. 156−166.
7. *Trofimenko M.A., Farber V.E.* Influence of range-Doppler coupling on the tracking stability of reentering space objects. // 2015 International Conference on Engineering and Telecommunication. IEEE. 2015. P. 40 – 44.
8. *Мурзова М.А., Фарбер В.Е.* Анализ атмосферного фильтра, адаптированного к наличию скоростной ошибки по дальности // Радиотехника. 2017. № 4. С. 5−14.
9. *Трофименко М.А., Фарбер В.Е*. Оценка влияния скоростной ошибки на устойчивость фильтров второго порядка // Радиотехника. 2016. № 4. С. 5−17.

УДК 621.396.67

Анализ подходов построения электрически малой СШП печатной антенны диапазона 1-10 ГГц

А.В. Уваров[1,2], А.В. Уваров[1]

[1]Институт радиотехники и электроники им. В.А. Котельникова РАН
[2]Московский физико-технический институт (государственный университет)

Работа раскрывает результаты поиска и анализа подходов построения электрически малой СШП печатной антенны для измерителя мощности диапазона 1-10 ГГц. Разработка СШП антенны была реализована в рамках создания носимого компактного измерителя мощности электромагнитного излучения сантиметрового диапазона индивидуального использования, назначение которого сбор и предоставление пользователю информации об интегральном значении мощности электромагнитного излучения, фиксируемого устройством. Такой измеритель мощности должен охватывать все основные коммерческие технологии беспроводной передачи данных, в частности сотовой связи GSM, UMTS, LTE, а также стандарты Wi-Fi и Bluetooth, что определило требования к антенне: (1) по рабочему диапазону частот – от 1 ГГц до 10 ГГц, (2) по уровню отражения сигнала по входу антенны, S_{11} менее -10 дБ, (3) по всенаправленным излучающим свойствам (КНД не более 3 дБ). Дополнительное требование к устройству по эргономике, небольшому размеру, не более размеров кредитной карты, и плоскому форм-фактору задается способом его применения, а именно использованием устройства в повседневной жизни любого современного человека.

Отметим, что требования, накладываемые на антенну, противоречат друг другу. С одной стороны, антенна должны иметь малый размер, а с другой – обеспечивать сверхширокий диапазон рабочих частот. При этом известно из теории фундаментальных ограничений антенн [1 – 3], что ширина полосы ограничена сверху и предел пропорционален третьей степени электрического размера антенны. Таким образом, требование сверхширокополосности антенны и электрически малого размера являются противоречащими друг другу, и при проектировании антенны должен быть выбран разумный компромисс между ними.

Для определения ограничения на минимальный достижимый размер печатной антенны был использован фундаментальный предел на характеристики печатных СШП антенны, полученный авторами ранее. Из сравнительного анализа различных типов печатных СШП антенн (монопольных, лог-периодических, Вивальди и дипольной антенны «бабочки») была выбрана печатная монопольная антенна, как обладающая характеристиками, наиболее приближенными к значению фундаментального предела и ненаправленными излучающими свойствами. В ходе численной оптимизации конфигурации печатного монополя были достигнуты следующие компромиссные характеристики: коэффициент отражения по входу менее -10 дБ в диапазоне частот 1,3 – 10,0 ГГц и -2,7 дБ на частоте отсечки 1 ГГц, а также коэффициент направленного действия не более 3 дБ, при габаритах печатной платы □□ × □□ мм. Стоит отметить, что для обеспечения требований по технологичности и стоимости была выбрана широко распространенная конфигурация печатного стека – двухслойная печатная плата с ламинатом FR-4 в качестве подложки в двух вариантах: толщиной 0,6 мм и 1,0 мм.

Для дальнейшего уменьшения размера устройства измерителя мощности был применен хорошо зарекомендовавший себя подход совместного использования площади земляного электрода монопольной антенны интегральными цепями приемника [4]. Проведенная оптимизация цепей приемника с помощью методов численного электродинамического анализа позволила обеспечить электромагнитную совместимость антенны и цепей приемника во всем сверхширокоом диапазоне частот.

Литература

1. *Chu L.J.* Physical limitations of omnidirectional antennas // Journal of Applied Physics. 1948. V. 19. P.1163–1175.

2. *McLean J.S.* A Re-Examination of the Fundamental Limits on the Radiation Q of Electrically Small Antennas // IEEE Transactions on Antennas and Propagation. 1996. AP-44. P. 672 – 676.
3. *Gustafsson M.* Physical limitations on antennas of arbitrary shape // Proc. R. Soc. A. 2007. V. 463. P. 2589–2607
4. *Uvarov A.V. Gerasimov M.Y., Uvarov A.V.* Designing a Printed Miniature Antenna for 3-5 GHz Range Integrated on PCB with UWB Direct Chaotic Transceiver Module // Proceedings of PIERS 2017. 2017.

УДК 539.1

Взаимодействие осциллятора Морзе с ультракоротким импульсом гауссовой формы

В.А. Астапенко, Е.В. Сахно

Московский физико-технический институт (государственный университет)

Гармонический осциллятор является хорошей моделью для описания колебательного движения атомов в молекуле при малых энергиях возбуждения [1]. Однако для описания колебаний атомов при более высоких энергиях используют модель ангармонического осциллятора, например осциллятора Морзе. Данный осциллятор представляет особый интерес, так как данная модель достаточно хорошо описывает колебания атомов в двухатомных молекулах.

Уравнение движения осциллятора Морзе при воздействии на него электрического импульса имеет вид

$$\ddot{x} = \frac{\omega_0^2}{k} \cdot \left(\exp\left(-2 \cdot k \cdot x\right) - \exp\left(-k \cdot x\right)\right) - \delta \cdot \dot{x} + \gamma \cdot f\left(t\right), \quad (1)$$

где ω_0 – частотный параметр (в пределе малых смещений соответствует собственной частоте гармонического осциллятора), x – координата отклонения осциллятора от положения равновесия (точка обозначает производную по времени), k – параметр потенциала, δ – коэффициент затухания, γ – коэффициент связи электрического поля $E(t)$ с осциллятором [2].

В данной работе рассматривается возбуждение осциллятора Морзе ультракоротким электромагнитным импульсом гауссовой формы:

$$f\left(t\right) = \exp\left(\frac{-t^2}{2\tau^2}\right)\cos\left(\omega t + \varphi\right), \quad (2)$$

где τ – длительность импульса, ω – несущая частота импульса, φ – начальная фаза [3].

Проведен анализ спектральной и временной зависимостей поглощенной энергии осциллятором Морзе, а также приведено сравнение со случаем гармонического осциллятора.

Анализ производился при различных значениях безразмерного параметра частотной отстройки ξ:

$$\xi = \frac{\omega - \omega_0}{\omega_0} \cdot 100\%. \quad (3)$$

Расчет поглощенной энергии гармоническим и ангармоническим осцилляторами под воздействием электрического поля $E(t)$ осуществлялся по формуле

$$\varepsilon = 2\gamma \int_{-\infty}^{\infty} \dot{x}\left(t\right) E\left(t\right) dt, \quad (4)$$

где $E\left(t\right) = E_0 \cdot f\left(t\right)$, E_0 – амплитуда электрического поля $E(t)$.

На рис. 1 приведена зависимость поглощенной энергии осциллятором Морзе как функции длительности импульса при различных коэффициентах γ.

Из рис. 1 видно, что при малых параметрах γ (γ = 0.1 и γ = 0.5) количество поглощенной энергии осциллятором Морзе монотонно возрастает с ростом коэффициента γ. Однако при значениях γ > 1 на графике появляются осцилляции.

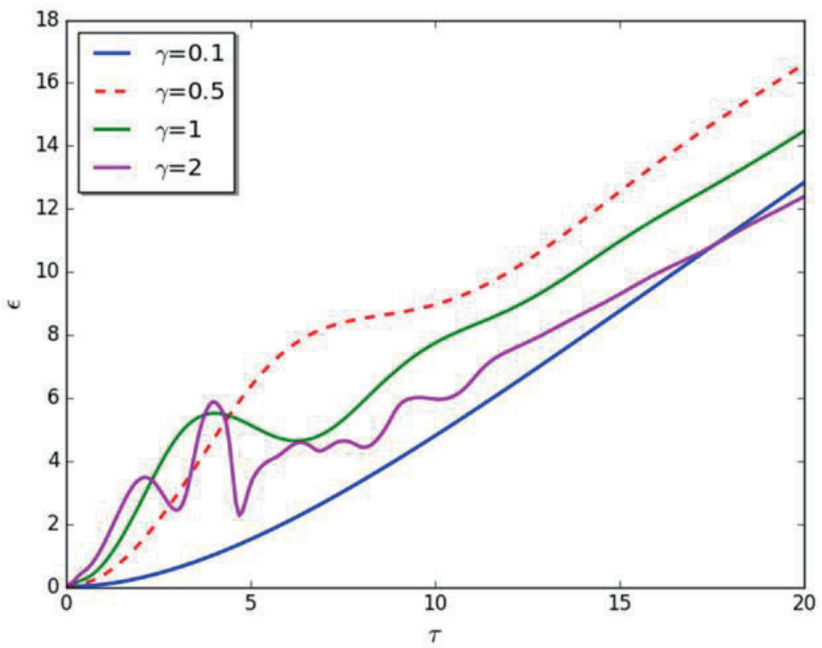


Рис. 1. Зависимость поглощаемой осциллятором Морзе энергии ε как функции длительности τ при различных параметрах γ; δ = 0.1, ω_0 = 2, ξ = 0 %

Работа выполнена в рамках Государственного задания Министерства образования и науки РФ (задание № 3.9890.2017/8.9).

Литература

1. *Гребенник А.В., Крюков А.Ю.* Лабораторный практикум по физической химии. Спектрохимия. М.: РХТУ, 2015.
2. *Астапенко В.А.* Взаимодействие излучения с атомами и наночастицами. – Долгопрудный: Издательский Дом «Интеллект», 2010. 496 с.
3. *Астапенко В.А.* Взаимодействие электромагнитных импульсов с классическими и квантовыми системами. М.: МФТИ, 2013.

УДК 537.874

Классическая модель возбуждения резонанса Фано–Фешбаха лазерным импульсом

***П.А. Головинский*[1,2], *А.В. Яковец*[1], *В.А. Астапенко*[1]**

[1]Московский физико-технический институт (государственный университет)
[2]Воронежский государственный технический университет

Интерференция Фано является универсальным явлением, поскольку проявление деструктивной интерференции мод не зависит от характера среды. Важность резонансов Фано с практической точки зрения заключается в той информации, которую они содержат о конфигурации взаимодействующих мод и внутренних потенциальных полях в низкоразмерных структурах. Она может быть извлечена из интерференции волн в разных каналах. Классическая модель резонансов Фано состоит из слабо связанных между собой

осцилляторов, возбуждаемых внешней силой [1–3]. Резонанс Фано можно также моделировать, используя эквивалентные электрические колебательные системы [4].

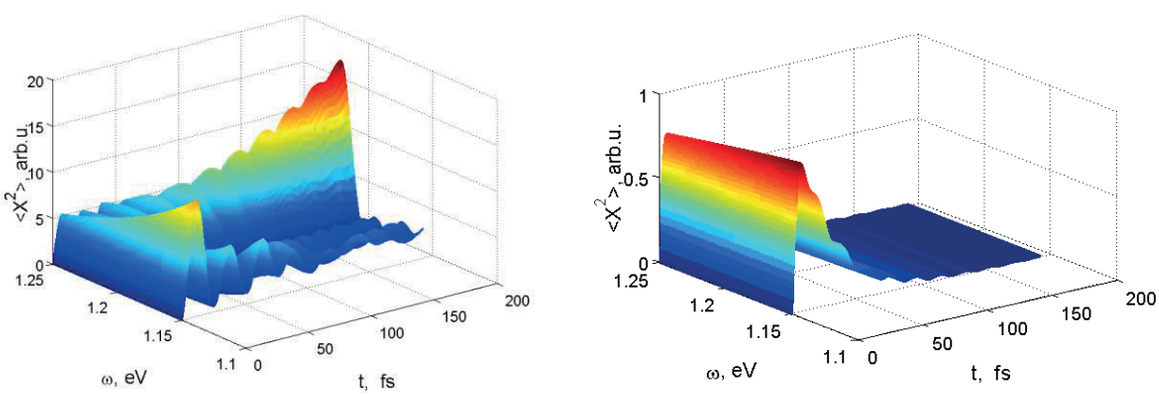
В работе исследуются дисперсионно-временные зависимости резонанса Фано для следующих систем.

1. Двух связанных осцилляторов при возбуждении импульсной силой вида $f(t) = f_0 \sin \omega t$ и $f(t) = e^{-\lambda t} f_0 \sin \omega t$.

2. Оптически связанная квантовая точка (нанокристалл) и металлическая наночастица при возбуждении полем $f(t) = f_0 \sin \omega t$ и $f(t) = e^{-\lambda t} f_0 \sin \omega t$.

Из представленной на рис. 1 а зависимости наглядно видно развитие во времени формирования резонанса Фано. Для спектрально узких резонансов и широкополосного импульса детали строения импульса становятся несущественными, и удобной формой представления импульса становится постоянный по величине спектр, эквивалентный действию δ-импульса. На рис. 1 б представлены результаты расчета динамики возбуждения системы широкополосным импульсом. Наглядно видно отсутствие зависимости динамики возбуждения от несущей частоты, означающее универсальность линейного отклика системы на предельно короткий импульс.

Полученные на основе модели связанных классических осцилляторов результаты в действительности имеют более широкую область применимости, поскольку линейный отклик системы полностью описывается ее дисперсионными свойствами. Это следует из возможности представления импульсов произвольной формы в виде интеграла Фурье. Поэтому конкретная реализация линейного оператора, обладающего необходимым спектром, не сказывается на описываемых свойствах.



а) б)

Рис. 1. Дисперсионно-временная зависимость резонанса Фано для системы двух связанных осцилляторов модельной системы при возбуждении импульсной силой вида: а) $f(t) = f_0 \sin \omega t$, б) $f(t) = e^{-\lambda t} f_0 \sin \omega t$, $\lambda = 0.3$

Работа выполнена в рамках Государственного задания Министерства науки и образования РФ (задание № 3.9890.2017/8.9).

Литература

1. *Andryushin A.I., Kazakov A.E., Fedorov M.V.* Effect of resonant electromagnetic field on the autoionizing states of atoms.//Sov. Phys. JETP 55, 53–58 (1982).
2. *Kiröla E. and Eberly J.H.* Quasicontinuum effects in molecular excitation.//J. Chem. Phys. 82, 1841–1854 (1985).
3. *Knight P.L., Lauder M.A., and Dalton B.J.* Laser-induced continuum structure.//Phys. Rep. 190, 1–61. 1990.
4. *Bixon M.*, *Jortner J.* Intermolecular radiationless transitions.// J. Chem. Phys. 42, 715–726. 1968.

УДК 537.874.7

Влияние атмосферных газов на энергетические потери при распространении радиоволны *S*-диапазона

***П.А. Гусенков*[1,2]**

[1]Московский физико-технический институт (государственный университет)
[2]ПАО «Радиофизика»

В работе рассматривается влияние тропосферных факторов на распространение радиоволны *S*-диапазона в атмосфере.

Одним из наиболее важных источников потерь являются атмосферные газы [1]. Из них наиболее крупными являются потери, вызываемые поглощением энергии сигнала на молекулах кислорода и, в меньшей степени, водяного пара [1], происходящим вследствие возникновения явлений поляризации молекул в электромагнитном поле и резонанса собственных колебаний поляризованных молекул с электромагнитной волной [2].

На основе моделей распределения атмосферных температуры и давления в зависимости от высоты над поверхностью Земли были рассчитаны величины потерь, вызываемых поглощением молекулами кислорода O_2 на трассе распространения радиосигнала в зависимости от угла места радиолокатора [3], [4].

$$\gamma_{\text{п}} = \gamma_0 \left(\frac{P}{P_0}\right)^2 \left(\frac{T_0}{T}\right)^{5/3}, \tag{1}$$

$$T = T_0 - 0{,}0065 \cdot h, \tag{2}$$

$$P = P_0 e^{\frac{-Mgh}{RT}}, \tag{3}$$

$$L = \sqrt{(R_{\text{з}} + h)^2 - {R_{\text{з}}}^2 \cdot \cos^2\theta} - R_{\text{з}} \sin\theta, \tag{4}$$

$$K = 2L\gamma_0 {T_0}^{5/3} \cdot \int_0^{10000} \frac{e^{-\frac{2Mg}{R}\frac{h}{T_0 - 0{,}0065 \cdot h}}}{(T_0 - 0{,}0065 \cdot h)^{5/3}} dh. \tag{5}$$

Здесь P, P_0 – атмосферное давление на высоте h и на поверхности соответственно, T, T_0 – температура воздуха на высоте и на поверхности соответственно, M – молярная масса кислорода, g – ускорение свободного падения, R – универсальная газовая постоянная, $R_{\text{з}}$ – радиус Земли, θ – угол места, L – длина трассы радиосигнала, $\gamma_{\text{п}}$ и γ_0 – коэффициенты поглощения при заданных значениях P и T и при нормальных условиях соответственно.

На рис. 1 изображены результаты моделирования величины потерь.

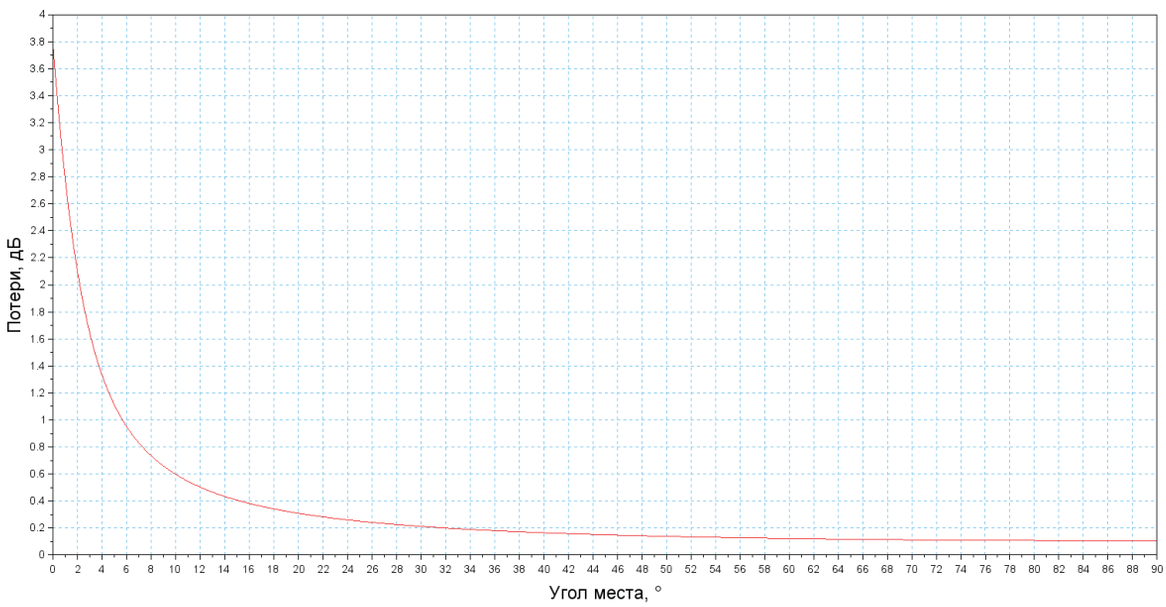


Рис. 1. Величина потерь в дБ для зондирующего сигнала с длиной волны 10 см как функция от угла места радиолокатора в градусах

Результаты численных расчётов потерь для радиосигнала с длиной волны $\lambda = 10$ см показывают, что величина потерь не превосходит 4,436 дБ при условии распространения радиоволн вдоль линии горизонта; при увеличении угла места потери уменьшаются.

Таким образом, разработанная модель позволяет определить и исследовать величину энергетических потерь в зависимости от характеристик атмосферы и параметров РЛС в точке базирования комплекса.

Литература

1. *Мельник Ю.А.* Радиолокационные методы исследования Земли. М.: Советское радио. 1980. 264 с., с ил.
2. *Калинин А.И.* Распространение радиоволн на трассах наземных и космических радиолиний. М.: Связь, 1979. 296 с.
4. *Бартенев В.А., Болотов Г.В., Быков В.Л. и др.; Под ред. Кантора Л.Я.* Спутниковая связь и вещание: Справочник. 3-е изд., перераб. и доп. М.: Радио и связь, 1997. 528 с.
5. *Черный Ф.Б.* Распространение радиоволн. М.: Советское радио, 1962.

УДК 621.396.67

Режимы работы квадрифилярной спиральной антенны

И.А. Барашкина, Д.А. Дёмин, И.В. Филатов

Московский физико-технический институт (государственный университет)

Квадрифилярная спиральная антенна (КСА) – один из наиболее распространенных типов резонансных антенн с круговой поляризацией. Образована 4 спиральными излучателями, сдвинутыми относительно друг друга по фазе на 90°. В зависимости от геометрии и типа антенны возможна реализация множества режимов работы антенны, имеющих различные характеристики излучения, например, диаграммы направленности. Так, варьируя геометрию КСА, можно достичь режимы как с высоконаправленной ДН, так и ненаправленной. При этом поляризация КСА не зависит от геометрических параметров – поляризация излучения вдоль оси антенны остается круговой. Благодаря этим свойствам, КСА нашли широкое применение в системах телеметрии и космических аппаратах, где часто отсутствует система ориентирования и используются антенны с круговой

поляризацией. Именно поэтому важно рассмотреть работу различных типов и режимов КСА.

В [1] описано, как геометрия антенны влияет на ее диаграмму направленности. В [2] приведен пример оптимизации КСА, реализующей максимально широкую диаграмму направленности при минимальных геометрических параметрах, работающую на 2 резонансе.

В докладе рассматриваются характеристики антенны на частотах 1–3 последовательных резонансов со следующими геометрическими параметрами:

- $L = 0{,}75\lambda$ – длина плеч;
- $\alpha = 53{,}3°$ - угол намотки;
- $R = 0{,}5\lambda$ – радиус антенны,

где λ – длина волны, соответствующая первому последовательному резонансу.

На рис. 1 представлены диаграммы направленности трех рассматриваемых режимов. Из графика видно, что на втором резонансе (F_2 = 2.82 GHz) можно достичь наиболее широкой диаграммы направленности. Варьируя геометрические параметры антенны, можно контролировать величину минимума в центре ДН (например, уменьшая радиус антенны) и прийти к режиму максимально плоской ДН. Первый же резонанс (F_1 = 0.94 GHz) дает более узкую диаграмму направленности.

Другая важная характеристика излучения – коэффициент эллиптичности (рис. 2). Уже на первом резонансе он имеет достаточно широкую полосу (88°) по уровню 0.5. На втором резонансе эта ширина больше (97°), т.е. охватывается вся верхняя полусфера.

Таким образом, наиболее приемлемый с практической точки зрения режим работы КСА соответствует второму резонансу (рис. 3). Связано это с оптимальными входными характеристиками антенны.

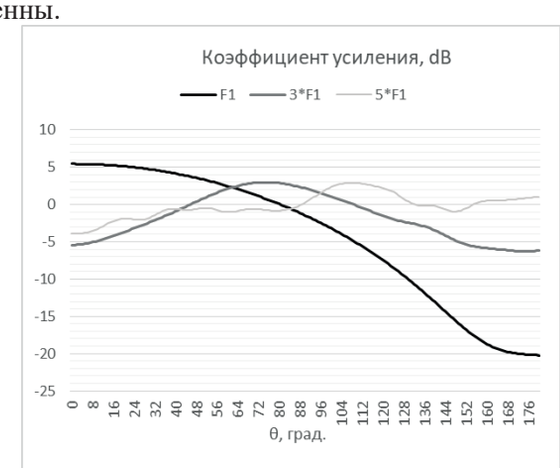


Рис. 1

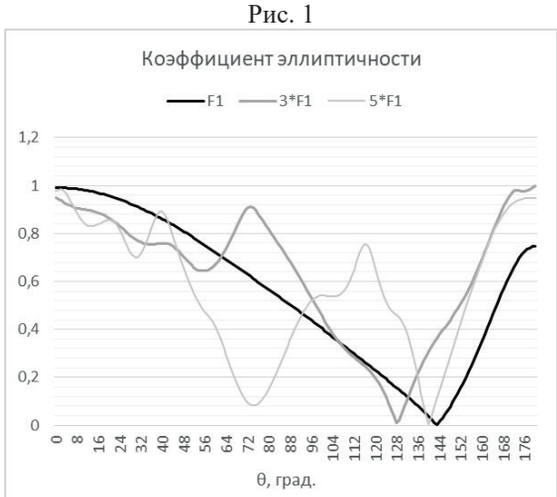


Рис. 2

Рис. 3

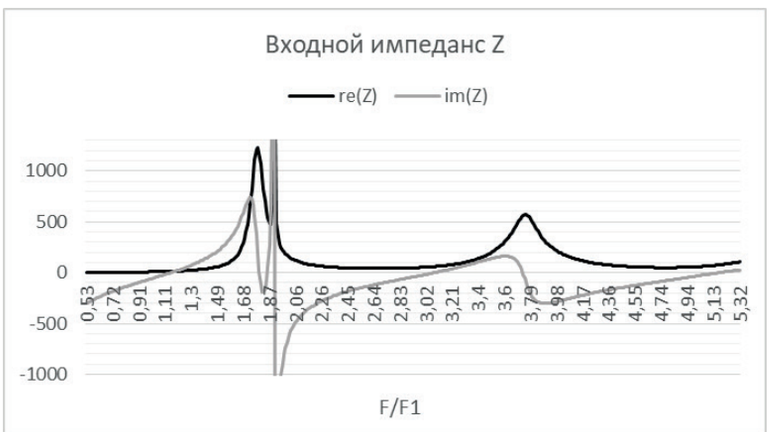


Рис. 4

Так, на втором резонансе входное сопротивление близко к 50 Ом (рис. 4), что обеспечивает хорошую согласованность антенны. Входное сопротивление, соответствующее первому резонансу, в свою очередь составляет единицы Ом, что приводит к плохой согласованности антенны и высоким потерям на отражение при питании антенны от 50-омной линии передач.

Литература

1. *Balanis C.A*. Modern antenna handbook // John Wiley & Sons. 2008.
2. *Дёмин Д.А, Стукалова Е.С, Филатов И.В, Чубинский Н.П.* Компактная квадрифилярная антенна S-диапазона // Журнал радиоэлектроники. 2017. №2.

УДК 621.3.09

Оценка возможности построения имитатора радиолокационного сигнала для РЛС с синтезированной антенной

***Д.В. Орлов*[1,2], *В.Л. Коданев*[1,2]**

[1]Московский физико-технический институт (государственный университет)
[2]АО «Концерн «Вега»

Радиолокационные системы с синтезированием апертуры антенны (РСА) представляют собой сложные радиотехнические системы [1–3], поэтому возникает задача проверки работоспособности РСА до проведения полетов с использованием ЛА. Наибольшей достоверностью обладают результаты натурных испытаний, но возможности их проведения для РСА ЛА и получение требуемого объема информации ограничены. При

этом натурные испытания РСА ЛА представляют собой длительный и дорогостоящий процесс.

Наибольшее распространение получило математическое моделирование РСА. Однако для построения математического описания процессов РСА необходимо четкое представление не только о структуре, поведении отдельных элементов, но и о взаимодействии между ними с учетом действия различных факторов. Поэтому используют различные имитаторы, которые позволяют имитировать (моделировать) процессы, происходящие на борту ЛА [4].

Наиболее широко используют модели, представляющие собой сочетание физической и математической модели с использованием измерительной аппаратуры. Так как количество летных испытаний РСА ограничено крупными финансовыми и временными затратами на техническую проверку всех основных узлов самолета, возможности тестирования и калибровки радиолокационной станции упираются в недостаток полученных данных. Напротив, испытания с использованием программных математических моделей внешней тактической обстановки позволяют набрать достаточное количество статистических данных, но никак не отражают работу выходных узлов станции.

Этих недостатков лишены наземные испытательные комплексы, которые основаны на приеме и ретрансляции сигнала, полученного от РСА. Подобные устройства активно разрабатываются и модернизируются в ряде российских и иностранных предприятий. Большинство наземных испытательных стендов позволяют без особых проблем сымитировать сигнал, отраженный от стационарной или движущейся цели, при работе радиолокатора в импульсном режиме.

Особый интерес представляют наземные испытания радиолокационной станции с синтезированием апертуры. Данный режим основан на когерентном приеме отраженного сигнала в процессе движения самолета, что позволяет добиться гораздо большего разрешения по азимуту.

Так как необходимость ортогонального перемещения самолета относительно наблюдаемых целей существенно усложняет процесс наземных испытаний, данная область является малоизученной и наверняка будет развиваться в будущем.

Необходимым условием получения синтезированной апертуры антенны, является ее перемещение относительно наблюдаемых целей с течением временем. При проведении испытаний в наземных условиях самолет остается неподвижным. Но так как любое движение является относительным, для достижения поставленной задачи достаточно осуществлять перемещение наблюдаемых им объектов.

Движение целей задается в расположенном в близи антенны ретрансляторе сигнала. Данное устройство позволит создавать сигнал, отраженный сразу от нескольких перемещающихся объектов.

Во время испытаний бортовая навигационная система (БНС) работает в режиме имитации навигационных данных, задающем равномерное движение самолета. Вектор скорости самолета, выдаваемый БНС, должен в точности соответствовать параметрам, записанным в ретранслятор сигнала. В случае корректной настройки навигационных данных в ретрансляторе и БНС, радиолокационная станция самолета оказывается в состоянии, приближенном к полетным условиям, что позволяет осуществлять тестирование режима синтезирования антенны.

В качестве платформы для определения формы отраженных сигналов и их параметров выбрана библиотека Matlab Simulink. Каждый блок модели выполняет преобразование сигнала, соответствующее его изменению при распространении через свободное пространство и физические элементы радиолокационной станции.

Электромагнитное поле на апертуре антенны радиолокационной станции формируется как сумма импульсных сигналов, отраженных от нескольких точечных целей. Так как каждый из выше указанных сигналов имеет различную частоту за счет доплеровского смещения при отражении, их суперпозиция будет иметь сложную структуру, которую можно сымитировать только при одновременной частотной и амплитудной модуляции излученного сигнала.

Кроме того, задержка принимаемого сигнала будет зависеть от расстояния до области наблюдения. Подобного эффекта можно добиться, используя управляемую линию задержки.

Так как положение основного лепестка ДНА при движении самолета остается неподвижным, а направление на цель меняется с течением времени, амплитуда принятого сигнала от каждой цели будет варьироваться в соответствии с диаграммой направленности.

Учитывая все вышеперечисленные эффекты, программа, составленная в Matlab Simulink, формирует имитационный сигнал. При физическом моделировании получение сложного сигнала производится с использованием квадратурного модулятора, управляемого аттенюатора и линии задержки.

Программируемая логическая интегральная схема осуществляет управление элементами, формирующими отраженный сигнал. С этой целью в плату заранее записываются имитационные данные, полученные в программной среде.

Исходя из структуры отраженного и излученного сигналов, Matlab Simulink формирует квадратурный сигнал необходимый для работы устройства физического моделирования внешней тактической обстановки.

Для имитации внешней тактической обстановки предлагается использовать ретранслятор сигнала, расположенный вблизи антенны РСА.

Так как антенны бокового обзора комплексов радиолокационной разведки и радиолокационного дозора и наведения располагаются на нижней стороне фюзеляжа с направленным вниз под углом к земной поверхности основным лепестком ДНА, имитатор сигнала должен устанавливаться в непосредственной близости от самолета, чтобы попадать в область излучения диаграммы направленности антенны.

Коэффициент усиления антенны в ближней зоне будет значительно отличаться в зависимости от положения ретранслятора сигнала, в следствии чего он должен определяться устройством при приеме излученного сигнала и использоваться при формировании отраженного сигнала. Для поддержания принятого сигнала в заданном динамическом диапазоне используются устройства защиты и управляемые аттенюаторы.

Для предотвращения влияния сигнала, излученного радиолокационной станцией, на принимаемые данные в область излучения антенны бокового обзора РСА подстилается отражающая поверхность в виде листа стали или алюминия.

Литература

1. *Бакулев П.А. Радиолокационные системы.* М.: Радиотехника, 2015. 440 с.
2. *Верба В.С., Татарский Б.Г.* Радиолокационные системы авиационно-космического мониторинга земной поверхности и воздушного пространства. М.: Радиотехника, 2014. 576 с.
3. *Дудник П.И.* Авиационные радиолокационные комплексы и системы. М.: Издательство ВВИА им. проф. Н.Е. Жуковского, 2006. 1112 с.
4. *Важенин В.Г.* [*и др*.]. Полунатурное моделирование бортовых радиолокационных систем, работающих по земной поверхности: учебное пособие/под общ. ред. *В.Г. Важенина*. Екатеринбург: Изд-во Урал. ун-та, 2015. 208 с.

УДК 537.8, 621.396

Достижимые значения эффективной магнитной проницаемости больших систем нерезонансных магнитных диполей

К.С. Лисовская, Н.П. Чубинский

Московский физико-технический институт (государственный университет)

В последние несколько десятилетий активно ведутся исследования метаматериалов, сред, представляющих собой большие упорядоченные системы электрически малых магнитных и/или электрических диполей [1]. Такие среды в переменном электромагнитном поле поляризуется и изменяют локальные электрические параметры. Благодаря этому

свойству они представляют интерес для создания материалов с различными значениями эффективной диэлектрической и магнитной проницаемостей [2], [3].

В многочисленных теоретических исследованиях после пионерской работы Веселаго В.Г. [2] анализировались изотропные среды с отрицательными диэлектрической и магнитной проницаемостями, приводились их уникальные свойства. В начале 2000-х годов начали появляться прикладные исследования, в какой-то степени подтверждающие теоретические прогнозы. Наши исследования для искусственных магнетиков показали, что нерезонансные системы МД действительно позволяют получить эффективную проницаемость такой среды менее единицы. Однако оставался открытым вопрос, какие минимальные значения эффективной магнитной проницаемости физически реализуемы, достижимы ли отрицательные ее величины.

Была рассмотрена среда, заполненная магнитными диполями (МД) в виде круглых колец радиуса *a* и диаметром провода 2*r*. Кольца располагаются в прямоугольных ячейках с центрами x_i, y_j, z_k и не имеют электрического контакта между собой. В выбранном частотном диапазоне размеры колец должны удовлетворять условиям квазистатического приближения $2\pi a \ll \lambda$. Если оси колец ориентировать вдоль оси z, то минимальные размеры ячеек $l_x = l_y > 2a$ и $l_z > 2r$ и только составляющая $\vec{B}_{0z}$ внешнего магнитного поля $\vec{B}_0$ наводит в них токи. Алгоритм определения эффективной магнитной проницаемости такой среды: $\vec{\mu}_{ef}(\omega) = \mu' - j\mu''$ [4] основан на определении вектора магнитной поляризации $\vec{M}(x_i, y_j, z_k)$, то есть *средней* индукции магнитного поля $\left\langle \vec{B}_{in}(x_i, y_j, z_k) \right\rangle$, наведенной внешним полем в пределах элементарной ячейки, включающей кольцо:

$$\vec{\mu}_{ef}(x_i, y_j, z_k) = 1 + \left\langle \vec{B}_{in}(x_i, y_j, z_k) \right\rangle \Big/ \vec{B}_{0z} = 1 + \vec{\chi}_m, \qquad (1)$$

где $\vec{\chi}_m$ – магнитная восприимчивость поляризованной среды. Искомые наведенные поля каждого кольца $\vec{B}_н(x, y, z; x_i, y_j, z_k)$ пропорциональны наведенным в них токам $\vec{I}_{ijk}(x_i, y_j, z_k)$. Найдем их, используя алгоритмы для расчета распределения наведенных токов [5 – 7], корректно работающие при любой степени взаимодействия между МД, а также при произвольных размерах системы. Затем следует весьма затратная операция вычисления локальных средних наведенных полей $\left\langle \vec{B}_{in}(x_i, y_j, z_k) \right\rangle$ даже для систем умеренных размеров: $N = N_x N_y N_z \geq 10^6$ колец. Подавляющее число расчетов были проведены для колец с умеренной толщиной проводника колец: $p = a/r = 10$. Они показали, что при вариациях плотности упаковки по осям координат невозможно получить: $\vec{\chi}_m \approx \left\langle \vec{B}_{in}(x_i, y_j, z_k) \right\rangle \Big/ \vec{B}_{0z} \geq -(0,5...0,7)$.

Целью настоящих исследований стало строгое определение минимальных значений $\vec{\mu}_{ef} = 1 + \vec{\chi}_m$ в больших системах МД. Необходимость такого уточнения связана с тем, что в высокочастотном приближении (сильный скин-эффект, активное сопротивление кольца R пренебрежимо мало по сравнению с его индуктивным сопротивлением ωL) с увеличением диаметра проводника $2r$ распределение плотности тока по его сечению становится все более неравномерным. Это приводит к изменению индуктивности, определенной согласно [8] для равномерного распределения тока по поверхности проводника. В результате точных расчетов показано, что в уединенном кольце при увеличении a/r от 0,05 до 0,25 магнитная восприимчивость $\vec{\chi}_m$ возрастает от -0,47 до-0,23. В предыдущих расчетах предполагалось обратное.

В больших 3D-системах в зависимости от плотностей упаковки МД (то есть степени их взаимного влияния) по осям координат эти величины могут изменяться не более чем в два раза в ту или другую сторону. Таким образом, в больших системах

нерезонансных МД эффективная магнитная проницаемость может быть меньше единицы, но не может достигать нулевых или отрицательных значений. В резонансных системах МД легко получить как большие отрицательные, так и положительные значения: $\bar{\mu}_{ef}(\omega) = \mu' - j\mu''$, но только при больших потерях, когда $\mu' \square \mu''$, и в очень узкой полосе частот.

Литература

1. *Щелкунов С.А., Фриис Г.Т.* Антенны. Теория и практика под ред. Л.Д. Бахраха пер с англ; М.: Сов. Радио, 1955.
2. *Веселаго В.Г.* Электродинамика веществ с одновременно отрицательными ε и μ // УФН. Т. 92. Вып. 3. 1967.
3. *Pendry J.B., Holden A.J., Robins D.J., Stewart W.J.* // J. Phys.: Condens. Matter. 1998. V. 10. N 22. P. 4785.
4. *Семенов Н.А.* Техническая электродинамика: учеб. пособие для вузов. М.: Связь, 1973. 480 с.
5. *Борзунова К.С., Чубинский Н.П.* Поле электрически малого магнитного диполя в квазистатическом и волновом приближениях // Сб. докладов II Всерос. Армандовских чтений. – Муром. 26. 2012.
6. *Борзунова К.С., Чубинский Н.П.* Алгоритмы определения эффективной магнитной проницаемости системы магнитных диполей. Радиофизика метаматериалов // Сб. докладов IV Всерос. Армандовских чтений. Муром, 27-29.05.2014. ISSN 2304-0297(CD-ROM)
7. *Борзунова К.С., Чубинский Н.П.* Физика взаимодействия электромагнитных волн с большими системами электрически малых диполей // Сб. докладов VI Всерос. Армандовских чтений. Муром, 29.05-02.06.2016. С. 426-438. ISSN 2304-0297 (CD-ROM)
8. *Калантаров П.Л., Цейтлин Л.А.* Расчет индуктивностей. Справочная книга. Ленинград: Энергоатомиздат, 1986.

Секция радио и информационных технологий

УДК 621.396.7

Поиск и настройка на станцию цифрового радиовещания

Д.М. Мингазов

Московский физико-технический институт (государственный университет)

Частотный ресурс ограничен и его эффективное использование является одной из важнейших задач в радиовещании.

Использование стандартов цифрового радиовещания дает выигрыш по сравнению со стандартами аналогового радиовещания в энергопотреблении и в удельном количестве переданной информации. На сегодняшний день по всему миру страны внедряют цифровое радио.

Системы цифрового радиовещания имеют свои особенности, которые необходимо учитывать. В случае мобильного приема возникает проблема многолучевого распространения с динамическими частотно-селективными замираниями. В таких системах используется OFDM-модуляция сигнала для работы в условиях помех, многолучевого распространения и прочих особенностей радиоканала.

Для эффективной работы системы необходимо автоматическое сканирование эфира с дальнейшим выводом списка станций с соответствующими частотами вещания. Так как мгновенный переход с аналогового радиовещания на цифровое невозможен, необходим универсальный метод, который бы отличал станции соответствующего вещания друг от друга при их одновременной работе.

Алгоритмы поиска и настройки на станцию цифрового вещания были предложены в работах [1–4], но они не обладают необходимой универсальностью, которая бы позволяла детектировать станции аналогового вещания и отличать их от станций цифрового вещания.

В предлагаемом алгоритме учтены постоянно меняющиеся факторы, воздействующие на канал. Также алгоритм осуществляет поиск станций не только цифрового вещания, но и аналогового, а возможность настройки на центральную частоту позволяет дальнейшую обработку сигнала.

Литература

1. *Urkowitz H*. Energy Detection of Unknown Deterministic Signals // Proceedings of the IEEE. 1967. V. 55. N 4. P. 523.
2. *Axell .E*., *Larrson E.G*. Optimal and Sub-Optimal Spectrum Sensing of OFDM Signals in Known and Unknown Noise Variance // IEEE journal on selected areas in communications. 2011. V. 29. N 2. P. 290.
3. *Chaudhari S., Koivunen V., Poor H.V.* Autocorrelation-based decentralized sequential detection of OFDM signals in cognitive radios // IEEE Transactions on Signal Processing. 2009. V. 57. N 7. P. 2690.
4. *Danev D.* On signal detection techniques for the DVB-T standard // Proceedings of the 4th International Symposium on Communications, Control and Signal Processing. 2010.

УДК 517.977

Гарантированное оценивание вектора состояния орбиты космического объекта по угловым измерениям с использованием симплекс-метода

И.С. Соколов

Московский физико-технический институт (государственный университет)
ОАО «МАК "Вымпел"»

Рассматриваются два следующих подхода к решению задачи оценивания вектора состояния орбиты космического объекта (КО) по оптическим измерениям [1–4].

1. Традиционный байесовский подход [4], в рамках которого неизвестные величины интерпретируются как случайные и характеризуются некоторыми распределениями вероятности. При этом под оцениванием понимается построение апостериорной плотности вероятности оцениваемого вектора и апостериорной доверительной области, содержащей КО с требуемой вероятностью.
2. Гарантированный подход [5], [6], под которым понимается построение апостериорной области, содержащей с гарантией оцениваемый вектор, который вместе с ошибками измерения интерпретируются как неизвестные величины. Предполагается, что оцениваемый вектор априори принадлежит гипершару с центром в начале координат и известным (достаточно большим) радиусом, а компоненты вектора ошибок ограничены по модулю известными константами.

Рассматривается случай, когда функция, связывающая измеряемые угловые координаты с оцениваемым вектором параметров движения КО, может быть с достаточной точностью линеаризована относительно некоторой опорной орбиты.

В этом случае в предположении гауссовских распределений оцениваемого параметра и ошибок измерения применение байесовского подхода приводит к фильтру Калмана–Бьюси, позволяющего вычислить оптимальную в среднеквадратическом смысле оценку (апостериорное среднее) и ковариационную матрицу ошибок оценивания, которые полностью определяют искомую гауссовскую апостериорную плотность вероятности и апостериорную доверительную область.

Рассматриваемый гарантированный подход в этих условиях сводится к задаче определения выпуклого гипермногогранника, который апостериори содержит с гарантией оцениваемый вектор параметров. В работе [7] вместо указанного гипермногогранника с помощью симплекс-метода предлагалось определять гиперпараллелепипед с ребрами, параллельными инструментальной системе координат, в которой рассматривается движение КО.

В докладе показывается, что предложенный в [7] алгоритм в ряде случаев приводит к гарантированной области, которая существенно больше гипермногогранника минимального объема, с гарантией, содержащей оцениваемый вектор. Предлагается основанный на симплекс методе алгоритм, позволяющий определять в этих случаях гарантированную область существенно меньшего размера. Приводятся сравнительные результаты моделирования.

Литература

1. *Gauss K.F*. Theory of the Motion of the Heavenly Bodies Moving about the Sun in Conic Sections // 1809 Dover Publications, Inc. New-York. 1963. Reprint (6, T).
2. *Chang C.B.* Ballistic Trajectory Estimation with Angle-Only Measurements // IEEE Trans on AC. 1980. V. AC-25. N 3. P. 474–480.
3. *Колесса А.Е., Пругло А.В., Равдин С.С.* Восстановление орбит по угловым измерениям // Радиотехника. 2005. № 10.
4. *Jazwinski A.H.* Stochastic Processes and Filtering Theory. Academic Press. NewYork. 1970.
5. *Кузнецов Ю.Н., Кузубов В.И., Волощенко А.Б.* Математическое программирование: учеб. пособие – 2-е изд., переработанное и дополненное. М.: Высшая Школа, 1980. 300 с.
6. *Куржанский А. Б.* Задача идентификации – теория гарантированных оценок // Автоматика и телемеханика. 1991. № 4. С. 3–26.

7. *Samotokhin A.S., Khutorovsky Z.N.* Determination of Predicted Position of Satellite at Limited Errors of Measurements // Cosmic Research. 2011. V. 49. N 6. P. 510–520.

УДК 519.254

Определение по угловым измерениям и прогнозирование доверительной области параметров орбиты околоземного космического объекта

В.А. Радченко

Московский физико-технический институт (государственный университет)
ОАО «МАК "Вымпел"»

Задача оценивания параметров орбиты по угловым измерениям, полученным с помощью телескопа, является одной из классических задач околоземной астрономии, но она всё ещё остаётся актуальной. В большинстве случаев данная задача рассматривается с некоторыми допущениями: во-первых, орбита известна *a priori* с точностью, достаточной для того, чтобы можно было воспользоваться линеаризацией уравнения наблюдения относительно априорной оценки, и, во-вторых, сеанс наблюдения достаточно продолжителен для того, чтобы построенная оценка вектора состояния обеспечивала корректную линеаризацию уравнения наблюдения. При решении задачи без этих допущений возникает ряд проблем, связанных с нелинейностью уравнений наблюдения и прогноза и, соответственно, отличием плотностей вероятности от гауссовых.

В данной работе предлагаются аналитические методы [1–3] построения оценки вектора состояния орбиты и области его неопределённости в случае неизвестного ранее околоземного космического объекта по короткому треку угловых измерений, а также прогнозирования этого вектора и его неопределённости к любому данному моменту времени, основанные на кусочно-гауссовой [4] и полигауссовой аппроксимациях плотностей вероятности. Использование данных аппроксимаций позволяет решить упомянутые выше проблемы.

Литература

1. *Kolessa A.E., Ivanov V.N., Radchenko V.A.* Searching of Unknown Earth-Orbiting Object in the Next Observation Session // Engineering and Telecommunication (EnT). 2014. P. 33–37.
2. *Колесса А.Е., Тупица Н.К.* Построение орбиты неизвестного околоземного космического объекта по двум полученным на разных витках коротким оптическим трекам // En&T. 2014. С. 90–91.
3. *Колесса А.Е., Радченко В.А.,* Иванов В.Н. Планирование повторного сеанса наблюдений неизвестных космических объектов // Near-Earth Astronomy. 2015. С. 99.
4. *Kolessa, A.E.* Exact formulas for optimal filtering in a nonstationary piecewise-linear problem of parameter estimation // Automation and Remote Control. 1989. V. 50, N 12. Pt. 1. P. 1667–1677.

УДК 519.226.3

Алгоритм обнаружения маневра искусственного спутника Земли по угловым измерениям телескопа

А.П. Иванов

ПАО «МАК «Вымпел»
Московский физико-технический институт (государственный университет)

В данной работе рассматривается задача оперативного определения факта изменения орбиты космического объекта (КО) на основании обработки последовательности угловых измерений сети оптических телескопов по двум сессиям наблюдений. Для решения поставленной задачи предлагается метод построения оптимальной в среднеквадратическом смысле оценки параметров орбиты КО только по последовательности угловых измерений одного трека с перебором всех возможных дальностей на первом пеленге измерений [1–3], а также уточнение данной оценки по двум

и более последовательным трекам с применением полигауссовской аппроксимации исходной апостериорной плотности вероятности [4].

В работе представлен алгоритм обнаружения факта изменения орбиты КО, который основывается на байесовском синтезе алгоритмов принятия решений и представляет собой идентификацию двух последовательностей угловых измерений, полученных с помощью сети оптических телескопов. Демонстрируется преимущество идентификации двух последовательных треков перед классическими методами обнаружения маневра.

В работе предлагается аналитический метод определения порога обнаружения маневра. Представлены численные расчеты идентификации двух треков при различных условиях наблюдения, которые демонстрируют прямую связь порога обнаружения маневра с распределением χ^2 и его зависимость от общего числа угловых измерений в двух треках. Проводится моделирование импульсных продольных маневров космических аппаратов для исследования возможностей обнаружения факта изменения орбиты КО сетью оптических телескопов.

Литература

1. *Колесса А.Е., Пругло А.В., Равдин С.С.* Восстановление орбит по угловым измерениям // Радиотехника. 2005. № 10. С. 5–9.
2. *Kolessa A.E.* Detection of Faint Space Debris Elements with Unknown Orbits // Sixth European Conference on Space Debris. 2013.
3. *Колесса А.Е.* Оценивание параметров движения объектов, наблюдаемых оптическими средствами с малых космических аппаратов // Успехи современной радиоэлектроники. 2010. Т.3.
4. *Kolessa A.E., Radchenko V.A, Ivanov V.N.* Searching of Unknown Earth-Orbiting Object in the Next Observation Session // Engineering and Telecommunication (EnT). 2014. P. 33–37.

УДК 520.82.053

Разработка алгоритма оценки прозрачности атмосферы с помощью All-Sky камеры

Н.В. Богатырев

Московский физико-технический институт (государственный университет)
ПАО «МАК «Вымпел»

Одним из наиболее значимых параметров, из которых складывается астроклимат определенной точки наблюдения, является прозрачность атмосферы [1]. Наиболее большая пропускная способность достигается в двух диапазонах излучения: оптическом и радиодиапазоне. Непрозрачность обусловлена явлением рассеяния света на аэрозолях (атомах и молекулах, содержащихся в атмосфере) и отражением радиоволн от электронов ионосферы. Качественная оценка прозрачности атмосферы в оптическом диапазоне необходима для исследования астроклимата звёздного неба на наличие допустимых условий наблюдения за объектами на околоземных орбитах.

В данной работе прозрачность атмосферы оценивалась с помощью АПК “AllSky” под авторством С.С. Равдина и А.В. Пругло (сопоставление с звездным каталогом, построение карты облаков), где был доработан анализ связи звездных величин из каталога с амплитудой яркости соответствующих звезд, фотометрированных на изображении с камеры. С помощью данной зависимости и пикового показателя оптической прозрачности в данной точке наблюдения (с помощью системы автоматизированного отслеживания аэрозольной прозрачности aeronet), а также, учитывая отклонение светил от зенита, была реализована калибровка фотоматрицы, таким образом, стал известен световой поток, а также прозрачность атмосферы, соответствующие произвольной звезде в определенном участке звездного неба [2]:

$$P_{\Phi} = T\int_0^{\infty} H_{\Phi}(\lambda) I P_T(\lambda) d\lambda,$$

$$I = \frac{e^{\frac{\ln 10}{2.5}(-14.18-m)}}{680\int_0^{\infty} H_{\Gamma}(\lambda) P_T(\lambda) d\lambda},$$

где m – звездная величина, $H_{\Gamma}(\lambda)$ и $H_{\Phi}(\lambda)$ – спектральные характеристики глаза и фотоматрицы. $P_{\text{Т}}(\lambda)$ – спектральная плотность излучения звезды, I – величина, пропорциональная яркости звезды. P_{ϕ} и T – расчетный световой поток и прозрачность атмосферы соответственно.

Целью работы является реализация карты прозрачности для звездного неба в данной точке наблюдения, что будет применительно для составления астроклиматической статистики и дальнейшего решения о целесообразности использования данной точки для задач наблюдения и анализа орбитальных объектов.

Литература

1. *Плакса С.* Астрономические наблюдения в городе. Астроклимат // Интернет-издание. 2008.
2. *Кучеров Н.И.* Астроклимат // М.: Знание, сер. Физика и химия. 1962. N 17. 39 с.

УДК 621.397

Программно-алгоритмическое обеспечение для анализа ошибок оптических наблюдений космических объектов

Е.И. Гундрова, А.П. Лукьянов

ПАО «МАК «Вымпел»
Московский физико-технический институт (государственный университет)

Мониторинг околоземного космического пространства состоит в определении характеристик находящихся в нем искусственных космических объектов как координатных (орбит), так и некоординатных (всех остальных). Все эти характеристики записываются в базу данных, называемую каталогом околоземных космических объектов. Каталог постоянно поддерживается, то есть обновляется и уточняется по мере поступления новых измерений. Для этого привлекаются оптические средства (телескопы), которые, в отличие от радиолокационных, позволяют проводить измерения параметров космических объектов, находящихся на больших дальностях, а также получать дополнительную информацию об их блеске в оптическом диапазоне длин волн [1], [2].

Измерительная информация, полученная в ходе наблюдений, необходима, во-первых, для поддержания существующего каталога космических объектов и, во-вторых, для уточнения параметров их движения (орбит).

Основная трудность – найти такое правило управления телескопом, которое бы обеспечило наибольшую эффективность получаемых результатов – измерений угловых координат космических объектов.

Эффективность одного измерения определяется в соответствии с критерием [3]. В основе критерия лежит отклонение измеренного положения космического объекта от его прогнозного значения. Под показателем эффективности совокупности измерений файла понимается сумма рассчитываемых показателей эффективности по отдельным измерениям этого файла.

Таким образом, оптимальное планирование наблюдений должно выбирать космические объекты, которые, с одной стороны, имели большую ошибку априорных орбитальных параметров из каталога, а, с другой стороны, эта ошибка была не слишком большой, чтобы поиск объекта не занимал много времени, и вероятность его наблюдения

была не очень низкой. Для этого реализуются алгоритмы, повышающие эффективность работы средств наблюдения.

Однако на практике возникает множество ситуаций, выходящих за рамки простых представлений о работе оптических средств, приводящие к тому, что не все теоретически возможные наблюдения оказываются успешными. На неудачу обнаружения космического объекта могут повлиять ряд причин: неточность целеуказания (орбиты в каталоге с недостаточной точностью соответствуют наблюдаемым); неточность прогнозных координат КО как функции времени (для разных моделей движения – разные); неточность наведения (недостаточная точность нацеливания телескопа); недостаточная прозрачность среды в момент наблюдения; недостаточный блеск КО. Для уменьшения доли неудачных наблюдений требуется проведение анализа их деятельности с целью выявления возможностей по улучшению работы.

В данной работе были проанализированы все вышеперечисленные причины, влияющие на успешность наблюдений космических объектов, с помощью разработанного авторами программно-алгоритмического обеспечения, позволившего выявить эти ошибки и повысить эффективность измерений привлекаемых оптических средств.

Литература

1. *Колесса А.Е., Пругло А.В., Равдин С.С., Ким А.К., Лукьянов А.П.* Комплекс алгоритмов автоматического обнаружения космических объектов по оптическим изображениям, оценки угловых координат и параметров орбит. Москва, 2013. 12 с.
2. *Лагуткин В.Н.* Частотные алгоритмы адаптивной нелинейной фильтрации последовательности изображений // Электромагнитные волны и электронные системы. 2013. Т. 18. №5. С. 27–36.
3. *Хуторовский З.Н., Шпитальник М.Ц., Колесса А.Е., Лукьянов А.П.* Критерий и анализ эффективности оптических наблюдений космических объектов телескопами ПАО «МАК «Вымпел» // Сборник трудов международной конференции "Околоземная астрономия–2015", под ред. Шустов Б.М., Рыхлова Л.В., Баканас Е.С, Карташова А.П. 2015. ISBN 978-5-8037-0666-3.

УДК 621.391.8

Масштабирование входных метрик norm-min-sum декодера для вычислений с фиксированной точкой

А.А. Хлынов

Московский физико-технический институт (государственный университет)

При использовании в модеме декодера на ПЛИС, использующего вычисления с фиксированной точкой, требуется подавать значения входных метрик – *llr* (log-likelihood ratio) с фиксированной разрядностью, которая чаще всего составляет 6–8 бит (как пример, в модемах фирмы Comtech для ldpc-кодека). Далее в работе будут рассмотрены низкоплотностные коды (ldpc) и результаты моделирования на примере кодов стандарта CCSDS [1]. Так как декодеры min-sum и norm-min-sum [2], [3] не чувствительны к масштабированию входа, к ним применима процедура нормализации входных метрик или их масштабирование с произвольным коэффициентом.

Нормализация позволяет максимально эффективно передать широкий динамический диапазон входных метрик на вход декодера. Так можно минимизировать эффект насыщения входа, когда декодер начинает работать почти как в режиме с двоичными данными на входе, присутствует лишь эффект квантования.

В приёмной аппаратуре, в состав которой входит разработанный автором декодер на ПЛИС, реализован режим с 6-битными данными на выходе демодулятора, поэтому далее будет рассматриваться реализация декодера с 6-битным входом [4].

$$y'_i = \frac{y_i}{Y_{\max}}, \quad (1)$$

$$y''_i = y'_i * cf_{inp}. \quad (2)$$

Стандартная процедура нормировки (1) предполагает, что масштабирование происходит таким образом, чтобы максимальное (по абсолютной величине) значение

входных данных соответствовало 1, а в случае чисел с фиксированной разрядностью – максимальному числу в двоичном представлении с заданной разрядностью. $Y_{\max}$ – максимальное значение амплитуды входных метрик в принятом кодовом слове. При использовании нормировки (1) на вход декодера передаётся весь динамический диапазон метрик. Однако опытным путём автором установлено, что из-за эффекта квантования масштабированные метрики используются неэффективно и допустимо насыщение части значений метрик. Для изучения влияния такого насыщения далее будет рассмотрено масштабирование (2) нормированных входных метрик с коэффициентом отличным от 1.

Для выбора оптимального значения коэффициента масштабирования входных метрик проведено моделирование декодера с вычислениями с фиксированной точкой на двумерной сетке с различным значением отношения сигнал/шум (для канала с белым гауссовым шумом и сигнальной конструкцией QPSK) и различным значением коэффициента масштабирования нормализованных входных метрик. Вход декодера реализован в 6-битном виде, один двоичный разряд – знак, один разряд – целая часть и четыре разряда – дробная часть числа. Значение битовой ошибки (ber) на графиках приведено в логарифмическом масштабе. Для декодера min-sum для значений $\frac{E_b}{N_0}$ от 1.5 до 2.875 дБ и cf_{inp} от 1 до 32.5 (от 1 до 6 для декодера norm-min-sum) результаты моделирования представлены на рис. 1. Введём поправку на минимальное значение ber (сдвиг по оси z на величину min(log10(ber)) для каждого отдельного значения отношения сигнал/шум для большей наглядности). Легко заметить, что оптимальное значение коэффициента масштабирования (минимизирующее вероятность ошибки) для рассматриваемого диапазона шумов лежит в интервале (1;6) в области «ямы» битовой ошибки. Аппроксимируем значения ber для каждого отдельного значения отношения сигнал/шум на этом интервале полиномом второго порядка. Вычислив координаты вершин полученных парабол, получим значения cf_{inp}, которые будем считать оптимальными. На рис. 2 приведена зависимость оптимального значения cf_{inp} от величины шума (линия «poly»), а также просто значение cf_{inp} на начальной сетке расчёта, при котором достигнута минимальная вероятность ошибки (линия «min»). Те же действия повторим для norm-min-sum декодера с фиксированным значением коэффициента масштабирования промежуточных метрик, соответствующему точке 2.75 дБ [5]. В случае, если динамическое вычисление значения cf_{inp} сложно реализуемо, возможно использовать масштабирование входных значений по табличным коэффициентам, по текущему уровню шума в канале. Также можно заметить, что зависимость коэффициента масштабирования схожа с зависимостью величины обратной к среднему значению амплитуды *llr* для фиксированного значения величины шума.

На основании анализа результатов моделирования кодека можно сделать вывод, что использование дополнительного масштабирования входных метрик перед квантованием может дать выигрыш ber ~ $10^{0.05}$ или по абсолютной величине ~ 10% для значений сигнал/шум 1–3 дБ.

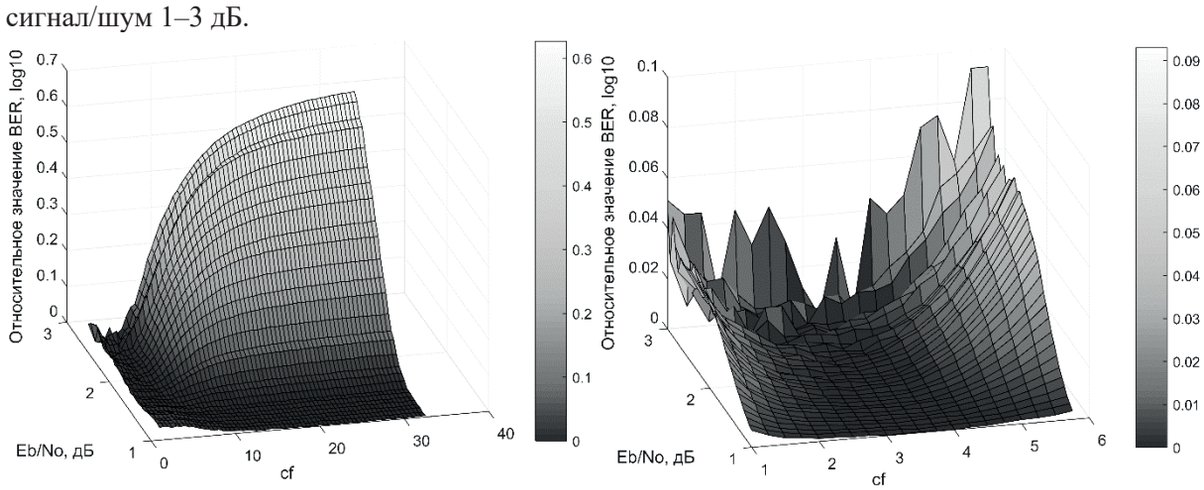


Рис. 1. Влияние коэффициента cf_{inp} на изменение битовой ошибки при различных

значениях отношения сигнал/шум (с поправкой на минимальное значение ber) для min-sum и norm-min-sum декодеров

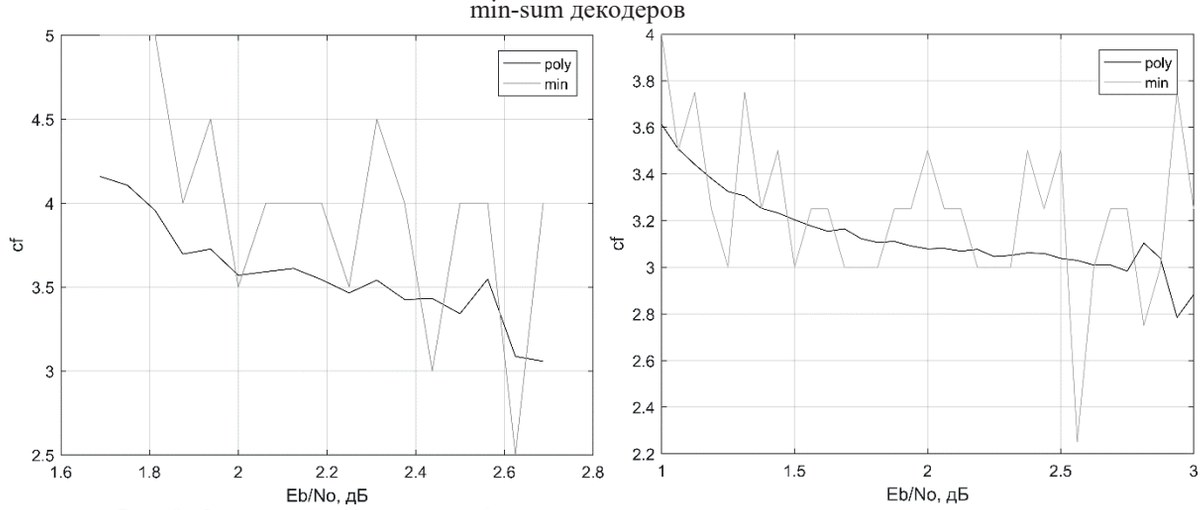


Рис. 2. Оптимальное значение cf_{inp} при различных значениях отношения сигнал/шум для min-sum и norm-min-sum декодеров

Литература

1. *The Consultative Committee for Space Data Systems* TM synchronization and channel coding — summary of concept and rationale. CCSDS 130.1-G-2. 2012.
2. *Хлынов А.А.* Оптимизация min-sum алгоритма декодирования LDPC-кодов // Труды Московского физико-технического института. – М., 2016. Т.8. № 4(32). С.13–17.
3. *Chen J., Fossorier M.* Near optimum universal belief propagation based decoding of low density parity check codes // IEEE transactions on communications. 2002. V. 50, N 3. P. 406–414.
4. *Хлынов А.А.* Влияние квантования входных значений ldpc декодера на распределение ошибок на его выходе // II International Conference «Engineering & Telecommunication En&T 2015». 2015.392 с.
5. *Хлынов А.А.* Методика вычисления масштабирующих коэффициентов normalized min-sum декодера низкоплотностного кода // Труды 59-й научной конференции МФТИ. 2016.

Секция интеллектуальных информационных радиофизических систем

УДК 004.415.25

Распределение виртуальных сенсоров по серверам в горизонтально масштабируемой отказоустойчивой системе на основе архитектуры Sensor-Cloud

А.А. Ширко, А.О. Армяков, А.А. Байтин, К.С. Серебренников

Московский физико-технический институт (государственный университет)

Сенсорные сети применяются для решения широкого спектра задач, таких как мониторинг транспортных средств, мониторинг экологической обстановки, организация логистических сетей с RFID и др. [1, 2]. Сенсорная сеть представляет собой множество пространственно разделенных сенсорных узлов, объединенных в совместную сеть. Большие сенсорные сети теоретически могут ежегодно производить объем данных порядка нескольких петабайт. Одной из особенностей больших сенсорных сетей является непрерывный поток данных, поступающий с варьирующейся скоростью, что делает реализацию сбора, хранения и обработки данных сложной задачей [3]. Традиционный способ управления петабайтными данными с применением реляционных баз данных, хранимых на серверах, не масштабируется должным образом, и, чтобы преодолеть проблему взрывообразного роста объема и потоков данных, требуются новые решения. Это обуславливает необходимость создания программного обеспечения, способного выполнять задачи сбора, обработки и хранения информации от больших сенсорных сетей (в дальнейшем, система для обработки данных от больших сенсорных сетей).

Требования, предъявляемые к системе по обработке данных от больших сенсорных сетей [4]:

- горизонтальная масштабируемость;
- отказоустойчивость;
- обработка потоковых данных без предварительного сохранения с минимальной задержкой.

Одним из перспективных направлений для обработки данных от сенсорных сетей является архитектура Sensor-Cloud. Отличительной особенностью архитектуры Sensor-Cloud являются виртуальные сенсоры. Виртуальные сенсоры могут быть реализованы на основе модели акторов, роль которых исполняют легковесные процессы. Вместе с тем, при разработке системы для обработки данных от больших сенсорных сетей на основе архитектуры Sensor-Cloud возникают следующие проблемы.

1. Как реализовать горизонтальное масштабирование системы и при этом минимизировать количество виртуальных сенсоров, которое необходимо перераспределить при добавлении новых серверов в систему.
2. Как организовать распределение виртуальных сенсоров между серверами.
3. Как организовать маршрутизацию данных, поступающих от физических устройств, к виртуальным сенсорам, обеспечив при этом минимальную задержку обработки данных.
4. Как организовать работу системы, чтобы исключить потерю данных в случае отказа части серверов.

В статье рассматриваются различные методы распределения виртуальных сенсоров между серверами в системе для обработки данных от больших сенсорных сетей на основе архитектуры Sensor-Cloud. Устанавливается, что использование консистентного хеширования с выделением равного количества партиций для каждого сервера позволяет добиться практически равномерного распределения виртуальных сенсоров между серверами. Отказоустойчивость может быть достигнута за счет репликации данных, что

ведет к увеличению сложности поиска местонахождения виртуальных сенсоров.

Литература

1. *Lee S.H.* [*et al.*]. Wireless sensor network design for tactical military applications: remote large-scale environments // Military Communications Conference. 2009. P. 1–7.
2. *Alemdar H., Ersoy C.* Wireless sensor networks for healthcare: A survey // Computer Networks. 2010. T. 54. P. 2688–2710.
3. *Jit B., Maniyeri J., Gopalakrishnan K.* [*et al.*]. Processing of wearable sensor data on the cloud—a step towards scaling of continuous monitoring of health and well-being // Proceedings of the 32nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC '10). 2010. P. 3860–3863.
4. *Армяков А.О., Байтин А.А., Ширко А.А* [*и др.*]. Реализация экспериментально-моделирующего стенда для обработки и сохранения потоков данных от больших беспроводных сенсорных сетей // Сборник трудов конференции Минцевские чтения. 2015. С. 143–151.

УДК 621.396.96

Сравнение ЛЧМ и импульсного сверхширокополосных сигналов в задаче радиолокационного наблюдения на фоне подстилающей поверхности

А.К. Строев

Московский физико-технический институт (государственный университет)

Одной из важных задач современной радиолокации является наблюдение за объектами на фоне мешающего отражения от подстилающей поверхности. Целью работы является выбор оптимального вида сигнала для решения данной задачи. Для примера приведено сравнение ЛЧМ-сигнала и короткого импульса с такой же шириной полосы.

Выберем модель, в которой отражение от поверхности описывается формулой [1], [2]:

$$u(t)=\int F(x,y)\frac{\tilde{\sigma}(x,y)}{4\pi R}A(\Omega)\exp\left(-i(\omega_0+\Omega)\frac{2R(x,y)}{c}\right)dx\,dyd\Omega, \qquad (1)$$

где $F(x,y)$ описывает диаграмму направленности антенны, $\tilde{\sigma}(x,y)\,dx\,dy$ – ЭПР малого участка поверхности (случайная функция), $A(\Omega)$ – спектр огибающей излученного сигнала, ω_0 – несущая частота сигнала.

Выход согласованного фильтра:

$$v(t)=\int F(x,y)\frac{\tilde{\sigma}(x,y)}{4\pi R}\left|A(\Omega)\right|^2\exp\left(-i(\omega_0+\Omega)\frac{2R(x,y)}{c}\right)dx\,dyd\Omega. \qquad (2)$$

Выбрав направление оси y на наблюдаемый объект и считая, что расстояние до отражающей поверхности много больше размера освещаемой лучом области, получим приближенное значение $R(x,y)$:

$$R(x,y)\approx R_0+y\cos\theta, \qquad (3)$$

где θ – угол места источника излучения.

Будем считать, что диаграмма направленности антенны описывается следующей формулой:

$$F(x,y)=\left(\frac{\cos\left(\pi\alpha(x,y)/\alpha_0\right)}{\pi\alpha(x,y)/\alpha_0}\right)^2, \qquad (4)$$

где α_0 – ширина луча, $\alpha(x, y)$ – угол между направлением на точку поверхности с координатами (x, y) и направлением на наблюдаемый объект (максимум диаграммы направленности). Его можно найти по формуле

$$\alpha(x, y) = \arctan\left(\frac{r\sin\theta}{R_0 - r\cos\theta}\right), \quad (5)$$

где $r = \sqrt{x^2 + y^2}$, R_0 – расстояние от радиолокатора до центра наблюдаемой области отражающей поверхности. От этой же точки должны отсчитываться (x, y).

Таким образом, среднее значение отражения от подстилающей поверхности, мешающее наблюдению за объектом, можно рассчитать по формуле (2), подставив в нее выражения (3) – (5) и заменив t на $\frac{2R_T}{c}$, где R_T – расстояние до наблюдаемого объекта, и проведя затем усреднение по большому числу реализаций.

Был проведен расчет для следующих параметров:

- расстояние до центра наблюдаемого участка поверхности 1400 м;
- угол места локатора 45 градусов;
- диаметр луча 0.05 радиан (меньше 3 градусов);
- удельная ЭПР поверхности задается комплексным числом (для учета случайной фазы отраженного сигнала) с нормальным распределением с нулевым средним, стандартным отклонением 0.3 и дельта-корреляцией. В таком случае абсолютное значение ЭПР имеет распределение Релея со стандартным отклонением 0.197. Усреднение проводилось по 50 реализациям;
- Использовалось два сигнала – ЛЧМ-сигнал длительностью 5 мкс с полосой частот 200 МГц и короткий импульс длительностью 5 нс, так что ширина спектра сигналов одинакова. Частота несущей – 1500 МГц.

Результаты моделирования (отношение отклика от поверхности к отклику от точечного объекта с единичной ЭПР, удаленного от поверхности на указанное расстояние) приведены на рис. 1. Сплошной линией обозначен ЛЧМ-сигнал, пунктирной – импульсный.

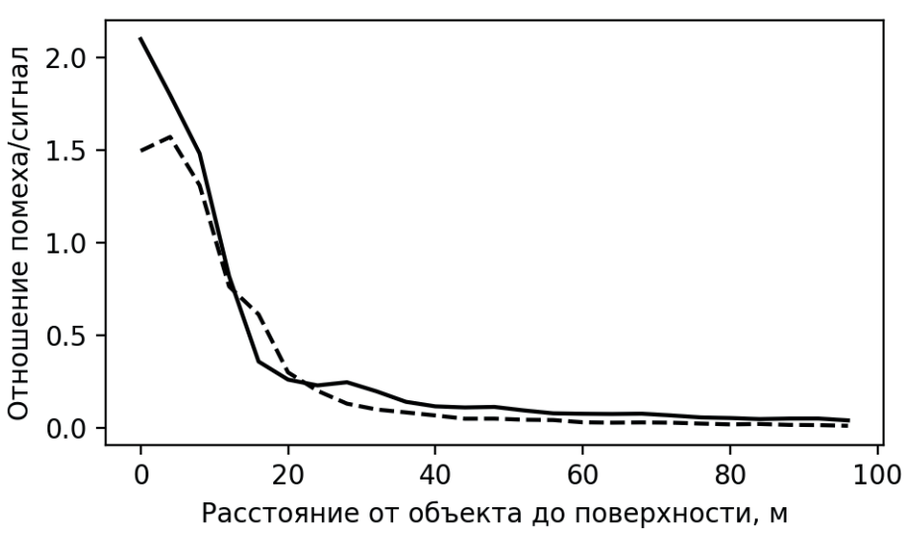


Рис. 1. Среднее значение отражения от подстилающей поверхности для ЛЧМ- (сплошная) и импульсного (пунктирная) сигналов

Из рисунка видно, что мешающее отражение от поверхности заметно ниже при использовании короткого импульса, чем при использовании ЛЧМ-сигнала с такой же шириной спектра, особенно если высота объекта над поверхностью невелика.

Литература

1. *Сколник, М.* Справочник по радиолокации./ пер. с англ.;/под ред. К.Н. Трофимова. 1978.
2. *Жиганов, С.Н.* Модель отраженного от подстилающей поверхности сигнала. // Проектирование и технология электронных средств. 2011. № 1. С. 52–54.

УДК 681.3

Программный комплекс для автоматизации процессов учета в сельском хозяйстве

Р.Т. Агишев[1,4], А.А. Кочкаров[1,2,3]

[1]Московский физико-технический институт (государственный университет)
[2]НТЦ-3 ОАО «РТИ»
[3]Финансовый университет при Правительстве РФ
[4]Сколковский институт науки и технологий

Сельское хозяйство является одной из важнейших отраслей промышленности, основной задачей которой является производство продуктов питания. Однако, в силу высоких темпов роста численности населения планеты, задачи сельского хозяйства значительно усложняются. Поэтому одной из основных тенденций развития отрасли является техническая модернизация. Такие сферы, как робототехника и компьютерное зрение, позволяют автоматизировать процессы сельского хозяйства, способствуя увеличению эффективности отрасли.

Основной задачей данной работы является ускорение процесса подсчета единиц сельскохозяйственных животных. Данная проблема актуальна для крупных фермерских хозяйств. Для ее решения создан программный комплекс на основе библиотеки OpenCV, использующий алгоритмы компьютерного зрения. Приложение позволяет автоматически детектировать и вести учет поголовья крупного рогатого скота, используя медиа-данные.

Для получения изображений и построения карт местности широко используются беспилотные летательные аппараты. Ввиду значимости аэрофотосъемки в настоящее время беспилотники активно применяются и в сельском хозяйстве. К основным достоинствам БЛА, как средства получения медиа данных, можно отнести детализированность изображений (по сравнению с полученными со спутника), возможность съемки в условиях облачности, высокую производительность (до 30 кв км за час при площадной съемке).

Используя программный комплекс на основе компьютерного зрения, БЛА может получать данные и эффективно решать такие задачи, как учет сельскохозяйственных животных. Применение передовых технологий является тем резервом, который позволит повысить урожайность и производительность сельского хозяйства.

Работа выполнена при поддержке РФФИ (грант № 16-01-00342, грант № 16-29-04268) и гранта Президента РФ (НШ-6831.2016.8).

Литература

1. *Simona M.C. Porto, Claudia Arcidiacono, Umberto Anguzza,* A computer vision-based system for the automatic detection of lying behavior of dairy cows in free-stall barns // Biosystems Engineering, 2013. V. 115. N 2. P. 184–194.
2. *Opelt A., Pinz1 A., Zisserman A.* A Boundary-Fragment-Model for Object Detection // European Conference on Computer Vision, 2006.
3. *Szeliski R.* Computer Vision: Algorithms and Applications // Springer. 2010.

УДК 62-529

Разработка моделей и методов оценки летно-технических характеристик БпЛА мультироторного типа

Р.Т. Агишев[1,4], А.А. Кочкаров[1,2,3]

[1]Московский физико-технический институт (государственный университет)
[2]НТЦ-3 ОАО «РТИ»
[3]Финансовый университет при Правительстве РФ
[4]Сколковский институт науки и технологий

Основными результатами проведенной работы являются создание двумерной модели системы БПЛА мультироторного типа и трехмерной модели одного летательного аппарата.

2D–модель системы четырех квадрокоптеров, жестко сцепленных с грузом, позволяет оценивать грузоподъемность летательных аппаратов в условиях меняющейся среды.

С помощью 3D–модели проведены оценки маневренности квадрокоптера, были выявлены основные преимущества и недостатки траекторий БПЛА различной степени гладкости. Полученные результаты сравнительного анализа пространственных кривых позволили описать и реализовать метод автоматического метода выбора траектории подходящей степени гладкости, исходя из взаимного расположения контрольных точек.

Беспилотные летательные аппараты (БПЛА) мультироторного типа широко используются в городских условиях с плотной застройкой. Поэтому движение квадрокоптера вдоль желаемой траектории является важным вопросом. Существует множество алгоритмов реализации этой задачи. Результатом данной работы является реализация алгоритма с минимальной ошибкой следования БПЛА вдоль траектории [9], сравнение её с кривыми, заданными сплайнами меньших степеней. Полученные результаты сравнения позволяют выбрать оптимальную траекторию с точки зрения точности следования ЛА пространственной кривой без существенного снижения скорости. С помощью предложенной модели приведены оценки маневренности БПЛА мультироторного типа.

В данной работе рассмотрены также летно-технические характеристики (ЛТХ) группы БПЛА. Одними из результатов являются описание и создание модели из четырех квадрокоптеров для переноса грузов. Транспортировка грузов является одной из важнейших задач квадрокоптеров. Реализованная компьютерная модель позволяет, варьируя параметры БПЛА, оценивать ЛТХ исследуемой системы.

Кроме того, с помощью созданной модели существует возможность оценивать точность следования группой квадрокоптеров, жестко сцепленных с грузом, желаемой траектории в условиях изменяющейся среды (учтено наличие ветра).

Работа выполнена при поддержке РФФИ (грант № 16-01-00342, грант № 16-29-04268) и гранта Президента РФ (НШ-6831.2016.8).

Литература

1. *Кочкаров А.А., Яцкин Д.В., Рахманов О.А.* Особенности решения задачи геометрического мониторинга // Известия ЮФУ. Технические науки. 2016. № 2(175). С. 158–168.
2. *Кочкаров А.А., Калинов И.А.* Создание программно-аппаратного комплекса пространственной навигации и мониторинга мультироторного БПЛА на основе модифицированного алгоритма визуальной одометрии // Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 09. С. 74–91.
3. *Кочкаров А.А., Яцкин Д.В., Калинов И.А.* Новый подход в применении малых БПЛА для мониторинга сложных пространств // Интеллект и технологии. 2016. № 2(14). С. 68–71.
4. *Кочкаров А.А.* Некоторые особенности применения малых и сверхмалых беспилотных летательных аппаратов // Труды Второй Всероссийской научно-технической конференции молодых конструкторов и инженеров «Минцевские чтения», посвященной 120-летию со дня

рождения академика А.Л. Минца и 60-летию аспирантуры Радиотехнического института. М.: Издательство МГТУ им. Н.Э. Баумана, 2015. С. 301–30.
5. *Mellinger D., Michael N., Kumar V.* Trajectory Generation and Control for Precise Aggressive Maneuvers with Quadrotors // Int. Symposium on Experimental Robotics, 2010.
6. *J. Escareño·S. Salazar·H. Romero·R. Lozano* Trajectory Control of a Quadrotor Subject to 2D Wind Disturbances. // Journal of Intelligent & Robotic Systems. 2013. V. 70. I. 1-4. Pp. 51–63.
7. *Cayero J., Cugueró J., Morcego B.* Impedance control of a planar quadrotor with an extended Kalman filter external forces estimator.
8. *Fink J., Michael N., Kim S., and Kumar V*. Planning and control for cooperative manipulation and transportation with aerial robots // Int. J. Robot. Res. Berlin, 2011.V.70. P. 643–659
9. *N. Michael, D. Mellinger, Q. Lindsey, and V. Kumar*, “The GRASP Multiple Micro-UAV Testbed” // IEEE Robotics and Automation Magazine, 2010.

УДК 004.032.2

Распознавание объектов по нескольким измерениям их поляризационных характеристик с использованием нейронных сетей

Ю.А. Мазко

ОАО «Радиотехнический институт им. академика А.Л. Минца»

В ряде задач распознавания весьма актуальной является задача распознавания объектов, которые находятся под разными ракурсами относительно наблюдателя. В зависимости от угла наблюдения за объектом распознавания и его ориентации в пространстве наблюдатель фиксирует различные значения измеряемой физической величины одного и того же объекта, что усложняет задачу распознавания.

Под ракурсом в данном случае понимается поворот объекта (α, β, γ) в пространстве относительно некоторого исходного состояния a_0 в процессе наблюдения.

В данной работе рассматривается задача распознавания двух объектов (конуса и цилиндра) по измерениям поляризационной матрицы рассеивания (ПМР) при вращении объекта относительно наблюдателя за некоторое фиксированное время наблюдений. Для описания объекта используется не одно, а несколько измерений ПМР, выполненных последовательно.

Исходными данными для распознавания являются измерения элементов ПМР в процессе вращения объектов (конуса и цилиндра). ПМР объектов представляют собой вектор вида (HH_i, HV_i и VV_i), где i = 1,..n.

Задача состоит в распознавании типа объекта по одному или нескольким последовательным измерениям элементов ПМР. Для решения поставленной задачи предлагается использовать методы распознавания с помощью нейронных сетей: персептрона и нейронной сети Кохонена. Данные нейросетевые классификаторы, как утверждается в [1], позволяют повысить эффективность обработки радиолокационной информации.

Проектирование схемы нейронной сети связано со следующими параметрами:

1) размер вектора обучающей выборки, подаваемый на вход сети. Данный параметр влияет на размер входного слоя нейронной сети;
2) желаемый отклик сети. Эти данные необходимы при обучении сети с учителем, содержатся в обучающей выборке, и влияют на выходной слой сети.
3) количество векторов обучения, содержащихся в обучающей выборке. Данный параметр устанавливает ограничение на минимальноее количество синаптических весов в нейронной сети (максимальный размер нейронной сети). В соответствии с [2], размер сети прямо пропорционален количеству векторов обучения.

При решении задачи на вход нейронной сети подаётся одно, три и пять измерений ПМР. Выход сети состоит из двух вещественных чисел в пределе от 0 до 1, соответствующие количественному признаку соответствия входного вектора (векторов) к классу распознаваемого объекта (конусу или цилиндру)

Для оценки параметров нейронной сети используется три вида контрольных выборок:

1) для одного измерения ПМР. Состоит из 182 значений векторов ПМР;
2) для трех измерений ПМР. Состоит из 176 значений векторов ПМР;
3) для пяти измерений ПМР. Состоит из 172 значений векторов ПМР.

Каждый вектор контрольной выборки соответствует определенному значению ПМР для определенного ракурса объекта.

Для обучения нейронной сети используется обучающая выборка, формируемая из контрольной выборки для одного измерения ПМР путём наложения на неё гауссовского шума (математическое ожидание – 0, СКО – 0.5). Размер каждой обучающей соответствует 500 значениям векторов моделируемых объектов.

Исходя из вышеописанных параметров обучающей выборки определим параметры, содержащие в себе 30 (6 × 5) входов, 6 нейронов в первом слое, 6 нейронов во втором слое и 2 нейрона в третьем слое. Нейронная сеть Кохонена представляет собой сеть с 30 входами, двумя выходами с двумя нейронами.

Распознавание при помощи нейронных сетей по нескольким измерениям позволяет повысить вероятность правильной классификации с 0,76 до 0,89 для персептрона с 0,83 до 0,93 для нейронной сети Кохонена (в сравнении с распознаванием по одному значению ПМР).

Расчет исходных данных проводился с помощью программы моделирования обратного рассеяния от объекта сложной формы, основанной на фасеточной модели [3], [4].

Литература

1. *Татузов А.Л.* Нейронные сети в задачах радиолокации. М.: Радиотехника, 2009. 432 с.: ил. (Научная серия «Нейрокомпьютеры и их применение», книга 28)
2. *Widrow B., Stearns S.D.* Adaptive Signal Processing.- Englewood Cliffs, NJ: Prentice-Hall, 1985.
3. *Волкова К.В.* Классификация радиолокационных объектов на основе выявления кластерной структуры данных поляризационной матрицы рассеяния. Вторая Всероссийская научно-техническая конференция молодых конструкторов и инженеров «МИНЦЕВСКИЕ ЧТЕНИЯ», посвященная 120-летию со дня рождения академика А.Л. Минца и 60-летию аспирантуры Радиотехнического института: труды конференции / Открытое акционерное общество «РТИ», Открытое акционерное общество «Радиотехнический институт им. Академика А.Л. Минца». М.: Издательство МГТУ им. Н.Э. Баумана, 2015. С. 101–115.
4. *Олюнин Н.Н., Виноградов А.Г., Сазонов В.В.* Фасеточная модель в задачах рассеяния радиолокационных сигналов. М.: ОАО РТИ, 2007. С. 21.

УДК 621.396.969

Возможности сопровождения орбитального космического объекта в разных системах координат

***Б.А. Китаева*[1,2]**

[1]ОАО «Радиотехнический институт им. академика А.Л. Минца»
[2]Московский физико-технический институт (государственный университет)

В данной работе рассмотрены возможности сопровождения орбитального космического объекта в разных системах координат. В качестве алгоритма сопровождения был рассмотрен линейный μ,ν-фильтр[1, 2].

Схема алгоритма основана на соотношении

$$a_n = f(a_{n-1}) + M_n\big(z_n - f(a_{n-1})\big), \quad (1)$$

где $z_n -$ измерение в момент времени t_n, $a_n -$ оценка по n измерениям, $M_n -$ весовой коэффициент. Коэффициент M_n выбирается из критерия $\max_{t_n}(t_n - t_{n-1})$ при условии $\delta(ae_n) + 3\sigma(ae_n) < \Delta$, где $ae_n = f(a_{n-1})$, $\delta(ae_n) -$ динамическая ошибка целеуказания,

$\sigma(ae_n)$ −среднеквадратическая ошибка, вызванная ошибками измерений, $\Delta -$ половина ширины диаграммы направленности по углам или строба по дальности [2].

В начальных условиях для работы алгоритма задаются априорно известные данные о максимальном ускорении на участке сопровождения по измеряемым координатам. По этим данным алгоритм выбирает приемлемый интервал $(t_n - t_{n-1})$, при котором обеспечивается надежное сопровождение, и на цель тратится необходимое ограниченное количество энергии станции.

На движение космических объектов действует сила притяжения Земли. Для орбитального космического объекта в алгоритме было вычислено ускорение свободного падения по известным формулам.

Расчет баллистического ускорения в сферической системе координат был произведен по формулам [3]:

$$\begin{aligned} &\ddot{R} = -\mu \cdot r^{-3}(R + \rho_з \cdot \sin\theta) + R(\dot{\theta}^2 + \dot{\varepsilon}^2 \cdot \cos^2\theta), \\ &\ddot{\varepsilon} = 2 \cdot \dot{\varepsilon}(\dot{\theta} \cdot \mathrm{tg}\theta - \dot{R} \cdot R^{-1}), \\ &\ddot{R} = -\mu \cdot \rho_з \cdot r^{-3} \cdot R^{-1} \cdot \cos\theta - 2 \cdot \dot{\theta} \cdot \dot{R} \cdot R^{-1} - \dot{\varepsilon}^2 \cdot \sin\theta \cdot \cos\theta, \end{aligned} \quad (2)$$

где $\mu = 398600{,}448\ \frac{км^3}{с^2}$ – гравитационная постоянная Земли, $\rho_з = 6378{,}245$ км $-$ экваториальный радиус Земли, r – расстояние от центра Земли до объекта.

Формула расчета баллистического ускорения в прямоугольной системе координат был выведен из формулы баллистического ускорения в инерциальной системе координат Земли [3]:

$$\vec{\ddot{x}} = -\mu \cdot r^{-3} \cdot \vec{x}, \quad (3)$$

где $\vec{x} -$ вектор состояния объекта в инерциальной системе координат.

Моделирование проводилось для искусственного спутника Земли (ИСЗ) с круговой орбитой. Предельные значения целеуказания в алгоритме задавались в сферической системе координат R, ε, θ, где $R -$ дальность, ε – азимут, отсчитываемый от оси z топоцентрической прямоугольной системы координат, $\theta -$ угол места (отсчитывается от горизонтальной плоскости до направления на цель) [3]. Участок траектории сопровождения за спутником начинался от линии горизонта до зенита относительно точки наблюдения. Высоты ИСЗ выбирались равными $H = 200$ км и 1000 км.

Литература

1. *Savrasov JU.S.* Algorithms of filtration and extrapolation for discrete-time dynamical systems // Acta Applicandae Mathematicae 30: 193–263, 1993.
2. *Саврасов Ю.С, Хвацкий О.К.* Алгоритм расчета целеуказаний при сопровождении гиперзвуковых летательных аппаратов //Инновации в радиотехнических информационно-телекомуникационных технологиях // Юбил. науч.-техн. конф.: Сб. докл. в 2-х частях. Часть 1 М.: Изд. ЗАО «Экстра Принт», 2006. С. 103–108.
3. *Саврасов Ю.С.* Алгоритмы и программы в радиолокации. М.: Радио и связь, 1985. 216 с.

УДК 004.89

Модель вычислений с памятью в условиях деструктивных возмущений

А.С. Петренко, С.А. Петренко

Московский физико-технический институт (государственный университет)
ОАО «Концерн «Радиотехнические и информационные системы»

Рассмотрена возможная модель вычислений с памятью, которая является самоприменимым транслятором. Допущение самоприменимости названного транслятора позволяет одновременно интерпретировать его как модель, средство и объект синтеза требуемых иммунитетов от массовых и групповых компьютерных атак на суперЭВМ высокой производительности.

Из теории абстрактных автоматов известны три операции, задающие допустимые трансляции: трансляция, перекодировка, композиция. Для построения гипотетического

транслятора, поддерживающего искомую процедуру синтеза иммунитетов вычислений к возмущениям, введем дополнительно еще две операции: наполнение (смысл этой операции состоит в формировании семантического содержания (системы знаний) транслятора) и настройка (операция осуществляет настройку системы знаний под цели трансляции).

Введенные операции (1) – (5) разрешают новый тип транслятора (назовем его самоприменимым), позволяющий формировать внутреннее содержание трансляторов и осуществлять их настройку на требуемую трансляцию. Применив операцию трансляция к указанному множеству языков, получаем девять типов требуемых трансляторов (6) – (14).

Дано: $L = \{L_{40}, L_{41}, L_{42}, L_{43}, L_{4s}, R\}$ – множество языков, где $L_{40}, L_{41}, L_{42}, L_{43}$ – языки спецификаций действующих лиц процесса синтеза; L_{4s} - промежуточный язык схем решений; R – язык машинной реализации.

Найти:

На множестве L универсальный транслятор T;

Унарная операция ТРАНСЛЯЦИЯ

$$T = L_{5'}, L_{5''}, L_{5'''} \quad (1)$$

Операция ПЕРЕКОДИРОВКА

$$L_{5*}, L_{5**}, L_5 (L_{5'}, L_{5''}, L_{5*}) = L_{5'}, L_{5''}, L_{5**} \quad (2)$$

Операция КОМПОЗИЦИЯ

$$L_{5*}, L_{5**}, L_* L_{5**}, L_{5***}, L = L_{5*}, L_{5***}, L \quad (3)$$

Операция НАПОЛНЕНИЕ

$$S = Ф (T) \quad (4)$$

Операция НАСТРОЙКА

$$T_{5*} = T (S_{5*}) \quad (5)$$

При этом столь малое количество получилось благодаря наличию промежуточного языка (этот прием известен в теории программирования [1,2]). Затем в смысловой последовательности к полученным трансляторам применим попарно операции четыре и пять. Получим тот же состав трансляторов, но выраженных как функции от единственного – самоприменимого. После этого проведем глобальную композицию с целью получения транслятора с промежуточного языка описания возмущенных вычислений на язык реализации самовосстанавливающихся вычислений, получим рекурсивную формулу гипотетического транслятора как функцию от самого себя. При этом в нее входят все (из заданного множества) типы языков, трансляторов, функций управления, семантических содержаний и исполнительных актов синтеза.

$$T_{40\,5'} = L_{4S}, L_{40}, R= S_{40}= Ф (T) \quad (6)$$

$$T_{40} = L_{40}, L_{4S}, R=T (S_{40}) = T (Ф (T)) \quad (7)$$

$$T_{41\,5'} = L_{4S}, L_{41}, R =S_{41}= F (T_{40}) = F (T (Ф (T))) \quad (8)$$

$$T_{41} = L_{41}, L_{4S}, R=T (S_{41}) = T (F (T (Ф (T)))) \quad (9)$$

$$T_{42\,5'} = L_{4S}, L_{42}, R=S_{42}= f (T_{41}) = f (T(F(T(Ф(T))))) \quad (10)$$

$$T_{42} = L_{42}, L_{4s}, R=T (S42) = T (7f... \quad (11)$$

$$T_{43\,5'} = L_{4s}, L_{43}, R=S_{43}= f (T_{42}) = f (T (f... \quad (12)$$

$$T_{43} = L_{43}, L_{4s}, R= T (S_{43}) = T (f... \quad (13)$$

$$T_{44\,5'} = L_{4s}, R, R=S_{44}= J (T_{43}) = J (T (f... \quad (14)$$

Трансляторная постановка задачи синтеза требуемой системы иммунитетов обращает к необходимости решения трех взаимосвязанных проблем: обоснования существования трансляторного универсума; доказательства возможности самоприменимости транслятора; формализации семантики. Поиск решения указанных

проблем в современной теории проектирования компиляторов искомых результатов не дал, так как используемые там сегодня абстракции – это параметрическая. Нас же в контексте структурированного синтеза иммунитетов к возмущениям вычислений интересуют семантически управляемая, а возможно, самоприменимая и/или универсальная трансляции. Это подтверждает принятую гипотезу о пяти уровнях вложенности типов решений задачи синтеза, сыгравшую в настоящей работе роль универсального классификатора типов (УКТ). Здесь представленные уровни строго вложены.

Теперь применим УКТ для типизации моделей трансляторов и получим следующую типизацию моделей (универсальная, семантически управляемая, синтаксически управляемая, параметрически управляемая, самоприменимая или структурированная).

Подводя промежуточный итог, сведем приведенные здесь рассуждения в рабочую гипотезу самоприменимой трансляции, позволяющую интерпретировать транслятор как модель, средство и объект автоматического синтеза сначала иммунитета вычислений к возможным возмущениям, а затем и собственно организации вычислений с памятью для обеспечения требуемой устойчивости вычислений.

Работа выполнена при поддержке грантов РФФИ (№ 16-29-04268 офи_м) и Президента РФ (НШ-6831.2016.8).

Литература

1. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Organization of the entrusted calculations in crucial objects of informatization under uncertainty // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 307–309. DOI: 10.1109/SCM.2017.7970566.
2. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Analysis of computer security incidents using fuzzy logic // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 349-352. DOI: 10.1109/SCM.2017.7970587

УДК 004.89

Идеология вычислений с памятью для привития иммунитета к возмущениям

А.С. Петренко[1,2], С.А. Петренко[1,2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Концерн «Радиотехнические и Информационные Системы»

Рассмотрен алгоритмический базис принципиально нового класса *самовосстанавливающихся вычислений* суперЭВМ высокой производительности в условиях групповых и массовых компьютерных атак. Раскроем характерные особенности единичных, групповых и массовых возмущений вычислений [1, 2] с помощью следующих определений.

Определение 1. Динамическая система самовосстанавливающихся вычислений в условиях деструктивных возмущений вычислительной среды Σ называется *стационарной* (*постоянной*) тогда и только тогда, когда

(a) T есть аддитивная группа (относительно обычной операции сложения вещественных чисел);

(b) Ω замкнуто относительно *оператора сдвига* z^{τ}: $\omega \to \omega'$, определяемого соотношением: $\omega'(t)=\omega(t+\tau)$ при всех τ, $t \in T$;

(c) $\varphi(t; \tau, x, \omega) = \varphi(t+s; \tau+s, x, z^{s}\omega)$ при всех $s \in T$;

(d) отображение $\eta(t, \cdot)$: $X \to Y$ не зависит от t.

Определение 2. Динамическая система самовосстанавливающихся вычислений в условиях деструктивных возмущений вычислительной среды Σ называется системой с *непрерывным временем* тогда и только тогда, когда T совпадает с множеством вещественных чисел, и называется системой с *дискретным временем* тогда и только тогда, когда T есть множество целых чисел.

Здесь различие между системами с непрерывным и дискретным временем несущественно и выбор между ними диктуется в основном соображениями математического удобства разработки соответствующих моделей вычислений. Системы самовосстанавливающихся вычислений в условиях деструктивных возмущений вычислительной среды с непрерывным временем соответствуют классическим непрерывным моделям вычислений, а названные системы с дискретным временем соответствуют дискретным моделям вычислительных процессов. Важной мерой сложности системы вычислений является структура её пространства состояния.

Определение 3. Динамическая система вычислений в условиях деструктивных возмущений вычислительной среды Σ называется *конечномерной* тогда и только тогда, когда X является конечномерным линейным пространством. При этом $\dim \Sigma = \dim X_{\Sigma}$. Система Σ называется *конечной* тогда и только тогда, когда множество X конечно. Наконец, система Σ называется *конечным автоматом* тогда и только тогда, когда все множества X, U и Y конечны и, кроме того, система стационарна и с дискретным временем. Предположение о конечномерности названной системы существенно с точки зрения получения конкретных численных результатов.

Определение 4. Динамическая система вычислений в условиях деструктивных возмущений вычислительной среды Σ называется *линейной* тогда и только тогда, когда

(a) пространства X, U, Ω, Y и Γ суть векторные пространства (над заданным произвольным полем K);

(b) отображение $\varphi(t; \tau, \cdot, \cdot): X \times \Omega \to X$ является K-линейным при всех t и τ;

(c) отображение $\eta(t, \cdot): X \to Y$ является K-линейным при любых t.

В случае необходимости использования математического аппарата дифференциального и интегрального исчислений необходимо, чтобы в определение системы Σ были включены некоторые допущения о непрерывности. Для этого необходимо предположить, что различные множества (T, X, U, Ω, Y, Γ) являются топологическими пространствами и что отображения φ и η непрерывны относительно соответствующей (*Тихоновской*) топологии.

Теперь определим модель абстрактного преобразователя вычислений в условиях деструктивных возмущений вычислительной среды следующим образом.

Определение 5. Абстрактным преобразователем вычислений в условиях деструктивных возмущений вычислительной среды Σ называется сложное математическое понятие, определяемое следующими аксиомами.

(a) Заданы множество *моментов времени* T, множество *состояний вычислений* X, множество *мгновенных значений входных величин* U, множество *допустимых входных величин* $\Omega = \{\omega: T \to U\}$, множество *мгновенных значений выходных величин* Y и множество допустимых *выходных величин* $\Gamma = \{\gamma: T \to Y\}$.

(b) *Направление времени*. Множество Y есть некоторое упорядоченное подмножество множества вещественных чисел.

(c) Множество входных величин Ω удовлетворяет следующим условиям.

- *Нетривиальность*. Множество Ω не пусто.
- *Сочленение входных величин*. Назовём *отрезком входного воздействия* $\omega = \omega_{(t_1,t_2]}$ для $\omega \in \Omega$ сужение ω на $(t_1, t_2] \cap T$. Тогда если ω, $\omega' \in \Omega$ и $t_1 < t_2 < t_3$, то найдётся такое $\omega'' \in \Omega$, что $\omega''_{(t_1,t_2]} = \omega_{(t_1,t_2]}$ и $\omega''_{(t_2,t_3]} = \omega'_{(t_{21},t_3]}$.

(d) Существует *переходная функция состояния* $\varphi: T \times T \times X \times \Omega \to X$, значениями которой служат состояния $x(t) = \varphi(t; \tau, x, \omega) \in X$, в которых оказывается система в момент времени $t \in T$, если в *начальный момент времени* $\tau \in T$ она была в *начальном состоянии* $x = x(\tau) \in X$ и если на её вход поступила *входная величина* $\omega \in \Omega$. Функция φ обладает следующими свойствами.

- *Направление времени.* Функция φ определена для всех $t \geq \tau$ и необязательно определена для всех $t < \tau$.
- *Согласованность.* Равенство $\varphi(t; t, x, \omega) = x$ выполняется при любых $t \in T$, любых $x \in X$ и любых $\omega \in \Omega$.

- *Полугрупповое свойство.* Для любых $t_1<t_2<t_3$ и любых $x\in X$ и $\omega\in\ \Omega$ имеем $\varphi\ (t_3;\ t_1,\ x,\ \omega)=\varphi(t_3;\ t_2,\ \varphi(t_2;\ t_1,\ x,\ \omega),\ \omega)$.
- *Причинность* Если $\omega,\ \omega''\in\ \Omega$ и $\omega_{(\tau,\ t]}=\omega'_{(\tau,\ t]}$, то $\varphi(t;\ \tau,\ x,\ \omega)=\varphi(t;\ \tau,\ x,\ \omega')$.

(е) Задано *выходное отображение* η: $T\times X\rightarrow Y$, определяющее выходные величины $y(t)=\eta\ (t,\ x(t))$. Отображение $(\tau,\ t]\rightarrow\ Y$, задаваемое соотношением $\sigma\mapsto\eta\ (\sigma,\ \varphi(\sigma;\ \tau,\ x,\ \omega))$, $\sigma\in(\tau,\ t]$), называется *отрезком входной величины*, т.е. сужением $\gamma_{(\tau,\ t]}$ некоторого $\gamma\in\Gamma$ на $(\tau,\ t]$.

Дополнительно пару $(\tau,\ x)$, где $\tau\ \in T$ и $x\in X$, назовем *событием* (или *фазой*) системы Σ, а множество $T\in X$ *– пространством событий* (или *фазовым пространством*) системы Σ. Переходную функцию состояний φ (или её график в пространстве событий) назовем *траекторией или кривой решения* и т.д. Здесь входное воздействие, или *управление* ω, *переносит, переводит, изменяет, преобразует* состояние x (или событие (τ,x)) в состояние $\varphi(t;\ \tau,\ x,\ \omega)$ (или в событие $(t,\ \varphi(t;\ \tau,\ x,\ \omega))$). Под *движением системы* понимается функция состояний φ.

Определение 6. В более общем виде модель абстрактного вычислителя в условиях возмущений $\Re$ с дискретным временем, m входами и p выходами над полем целых чисел K представляется сложным объектом $(\aleph,\wp,\Diamond)$, где отображения $\aleph:\ell\rightarrow\ell,\wp:K^m\rightarrow\ell,\Diamond:\ell\rightarrow K^p$ суть абстрактные K-гомоморфизмы, $\ell-$некоторое абстрактное векторное пространство над K. Размерность пространства $\ell(\dim\ell)$ определяет размерность системы $\Re(\dim\Re)$.

Выбранное представление позволяет сформулировать и доказать в работе утверждения, подтверждающие принципиальное существование искомого решения [1, 2]. Здесь приведенные понятия самовосстанавливающихся вычислений еще достаточно общие, но уже позволяют предложить единую идеологию *вычислений с памятью* в условиях возмущений вычислительной среды суперЭВМ пятого поколения для привития иммунитета к деструктивным возмущениям.

Работа выполнена при поддержке грантов РФФИ (№ 16-29-04268 офи_м) и Президента РФ (НШ-6831.2016.8).

Литература

1. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Organization of the entrusted calculations in crucial objects of informatization under uncertainty // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 307–309. DOI: 10.1109/SCM.2017.7970566.
2. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Analysis of computer security incidents using fuzzy logic // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 349–352. DOI: 10.1109/SCM.2017.7970587

УДК 004.89

Формирование понятия самовосстанавливающиеся вычисления

А.С. Петренко[1,2], Д.Д. Ступин[1,2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Концерн «Радиотехнические и Информационные Системы»

Рассмотрены концептуальные основы *самовосстанавливающихся вычислений* суперЭВМ высокой производительности в условиях групповых и массовых компьютерных атак. Предложен ряд базовых понятий, раскрывающих сущность принципиально нового класса *вычислений с памятью.*

Для формирования понятия *самовосстанавливающиеся вычисления* в условиях возмущений воспользуемся следующими понятиями: *система вычислений; поведение системы вычислений; целевое назначение системы вычислений; возмущение вычислений; состояние системы вычислений*. Перечисленные понятия относятся к числу первичных, неопределяемых понятий и используются в следующем смысле.

Под системой вычислений понимается некоторая совокупность аппаратно-программных компонент со связями по управлению и по данным между ними, предназначенная для выполнения требуемых функций вычислений. Под *поведением* системы вычислений понимается некоторая реализация вычислительного процесса во времени. При этом допускается проведение целенаправленных корректирующих действий для обеспечения устойчивости вычислений. Функциональная предназначенность системы вычислений называется *целевым назначением*, корректирующие мероприятия – *обнаружение и нейтрализация возмущений вычислений*. Другими словами, любая система вычислений создана или создается для определенного целевого назначения и может обладать некоторым защитным механизмом, настраиваемыми или регулируемыми средствами обеспечения устойчивости.

Возмущение вычислений – это единичный или множественный акт внешнего или внутреннего деструктивного воздействия внутренней и/или внешней среды на систему вычислений. Возмущение приводит к изменению параметров вычислительных процессов, препятствует или затрудняет выполнение целевого назначения системы вычислений. Совокупность возмущений образует *множество возмущений*.

Состояние системы вычислений есть некоторый набор числовых характеристик параметров вычислительных процессов. Числовые характеристики вычислительных процессов зависят от условий функционирования системы вычислений, возмущений, корректирующих действий по обнаружению и нейтрализации возмущений вычислений и, в общем случае, от времени. Совокупность всех корректирующих действий по обнаружению и нейтрализации возмущений вычислений называется *множеством корректирующих мероприятий*, совокупность всех состояний системы обработки данных – *множеством состояний*.

Таким образом, будем считать, что при отсутствии возмущений, а также корректирующих мероприятий по обнаружению и нейтрализации возмущений, система вычислений находится в работоспособном состоянии и отвечает некоторому целевому назначению. В результате возмущения система вычислений переходит в новое состояние, которое может не отвечать целевому назначению. В подобных случаях возникает две основные задачи:

1) обнаружение факта возмущения и, возможно, внесенных изменений в штатный процесс функционирования системы вычислений;

2) задание оптимальной в определенном смысле (исходя из заданного функционала приоритетов) организации вычислений с целью приведения системы вычислений в работоспособное состояние (вплоть до реконфигурации и/или полного перезапуска системы, если данное решение будет сочтено лучшим).

На основе введенных понятий раскроем содержание элементарного, сложного и возмущенного вычислений в терминах динамических взаимосвязей *Р.Е. Калмана*.

Под э*лементарным вычислением* будем понимать структуру, на вход которой в определенные моменты времени поступает некоторая входная величина, из которой в какие-то моменты времени выводится некоторая выходная величина. Приведенное понятие элементарного вычисления как системы Σ включает вспомогательное множество моментов времени T. В каждый момент времени $t \in T$ система Σ получает некоторую входную величину $u(t)$ и порождает некоторую выходную величину $y(t)$. При этом значения входных величин выбираются из некоторого фиксированного множества U, т.е. в любой момент времени t символ $u(t)$ принадлежит U. Отрезок входной величины системы представляет собой функцию вида $\omega:(t_1,t_2)\rightarrow U$ и принадлежит некоторому классу Ω, который определяется математическими потребностями вычислений. Значение выходной величины $y(t)$ принадлежит некоторому фиксированному множеству Y. Отрезок выходных величин представляет функцию вида $\gamma:(t_2, t_3) \rightarrow Y$.

Под *сложным вычислением* понимается обобщенная структура, компонентами которой являются элементарные вычисления со связями по управлению и по данным между собой. Дальнейшая конкретизация понятия сложного вычисления проведена в ходе анализа особенностей типов программирования: структурного, функционального,

логического, объектно-ориентированного и алгебраического [1, 2]. Кроме того, учтены следующие специфические особенности форм программирования: *синтезирующего, конкретизирующего* и *сборочного*.

Синтезирующее программирование – это метод пошагового уточнения программ от спецификации задачи через серию корректных преобразований к адекватному решению. При этом процесс приобретает характер доказательного конструктивного рассуждения о существовании программы, решающей поставленную задачу. Программа же является побочным результатом рассуждений, а совокупность доказательств становится сертификатом ее правильности. Математические аналоги доказательного программирования состоят в том, что спецификацию задачи можно рассматривать как неявное уравнение относительно программы, а пошаговое уточнение программы – как символический метод решения этого уравнения.

Конкретизирующее программирование – это принцип, метод и техника смешанных вычислений в сочетании с оптимизирующими преобразованиями. Его ранние аналоги – это макрообработка и условная компиляция. Содержанием является адаптация многопараметрической универсальной программы к конкретным условиям ее применения.

Сборочное программирование – метод и техника модульного программирования, а также идеология их многократного использования. В настоящее время развивается на основе понятия абстрактных типов данных.

Теперь определим понятие *предыстории* (*памяти*) *иммунитета* вычислений к деструктивным воздействиям. Будем считать, что в условиях деструктивных возмущений значение выходной величины системы Σ зависит как от исходных данных и алгоритма решения вычислительной задачи, так и от *предыстории (памяти) иммунитета* к деструктивным кибератакам. Другими словами, *возмущенное вычисление* это структура, в которой текущее значение выходной величины системы Σ зависит от состояния системы Σ с накопленной *предысторией* (*памятью*) *иммунитета* к деструктивным возмущениям вычислений. При этом будем предполагать, что множество внутренних состояний системы Σ позволяет вместить информацию о предыстории (памяти) иммунитета системы Σ.

Отметим, что рассмотренное содержание возмущенного вычисления позволяет описать некоторую «динамическую» систему самовосстанавливающихся вычислений в условиях возмущений, если знание состояния $x(t_1)$ и отрезка восстановленного вычисления $\omega = \omega_{(t_1,t_2]}$ является необходимым и достаточным условием для определения состояния $x(t_2)=\varphi(t_2; t_1, x(t_1), \omega)$, когда $t_1 < t_2$. Здесь множество моментов времени T упорядоченно, т.е. в нём определено направление времени.

Работа выполнена при поддержке грантов РФФИ (№ 16-29-04268 офи_м) и Президента РФ (НШ-6831.2016.8).

Литература

1. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Organization of the entrusted calculations in crucial objects of informatization under uncertainty // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 307–309. DOI: 10.1109/SCM.2017.7970566.
2. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Analysis of computer security incidents using fuzzy logic // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 349–352. DOI: 10.1109/SCM.2017.7970587

УДК 004.89

Метод распознавания ранее неизвестных кибератак на основе семейства многослойных контекстно-свободных грамматик

А.С. Петренко[1,2], Д.Д. Ступин[1,2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Концерн «Радиотехнические и информационные системы»

В работе рассмотрен новый метод распознавания ранее неизвестных кибератак на основе семейства многослойных контекстно-свободных грамматик. Это позволило впервые исследовать компьютерные атаки с разнородно массовым характером возмущения [1, 2].

Зададим язык описания типов возмущений семейством многослойных КС-грамматик G_P вида $G_p =< S_G, N_G, T_G, R_G, P_G >$, где S_G – конечное непустое множество аксиом, $S_G \subseteq N_G$, $|S_G| \geq 1; N_G = \{a_i | i \in I_N\}$ – конечное непустое множество типов деструктивных воздействий на машинные вычисления (нетерминалов), $T_G = \{x_i | i \in I_T\}$ – конечное непустое множество типов деструктивных воздействий на машинные вычисления (терминалов), $N_G \cap T_G = \varnothing; R_G = \{r_i : \alpha_i \to \beta_i | i \in I_R, \alpha_i, \beta_i \in (N_G \cup T_G)^*\}$ – конечное множество правил вывода, где $X_G = \{x_i | i \in I_X\}$ – конечное множество атрибутов, $(N_G \cup T_G) \to X_G$ – биекция, $P_G = \{p_i(.) | i \in I_P\}$ – конечное множество предикатов, X_G. G_P: $\mathrm{g}: M_G \times X^{g,j} \to G_P, \mathrm{g} =< \mathrm{g}_T, \mathrm{g}_N, \mathrm{g}_{R^0}, \mathrm{g}_{R^P}, \mathrm{g}_P, \mathrm{g}_S >$. Это позволило разработать новый метод порождения комбинаций сочетанных типов деструктивных воздействий на машинные вычисления, приводящих к разнородно массовым возмущениям вычислений. Для распознавания структуры типов воздействий был предложен второй метод, позволяющий при помощи семейства МП-распознавателей делать заключения по данным регистрации фактов групповых и массовых возмущений вычислений.

Приведем ряд определений для распознавания деструктивных воздействий на суперЭВМ высокой производительности.

Определение 1. Управляющим порождающим процессором типов воздействий назовем совокупность объектов P_c = (Q, Σ, Γ, Δ, $\Re$, δ, q_0, F), включающую конечное множество *состояний управления* (Q), алфавит *символов действий* (Σ), алфавит *магазинных символов* (Γ), алфавит *семантических символов* (Δ), алфавит *резольверных символов* ($\Re$), управляющую таблицу δ=(δ_2,δ_3), состоящую из двух частей, таблицы *управляющих элементов* δ_2:Q×$\Re$*→(Q∪{Sup})×Γ*×Δ*×(Σ∪{ε}) и таблицы *возвратных состояний* δ_3:Q×Γ×$\Re$*→Q, а также *начального состояния* $q_0 \in$ Q и множества *конечных состояний* F $\subseteq \subseteq$Q.

Здесь операционная среда E=(E,H,I$\Re$,I_Δ,I_Σ,e_0) включает *пространство состояний операционной среды* E (область определения предикатов и преобразований операционной среды), *объектное подпространство* H, *предикаты* I$\Re$={ι_ρ:E→{*false,true*},ρ∈$\Re$}, ассоциированные с резольверными символами, *преобразования операционной среды* I_Δ={ι_σ:E→E,σ∈Δ}, ассоциированные с семантическими символами, *преобразования операционной среды* I_Σ = {ι_a:E→E,*a*∈Σ}, ассоциированные с символами действий, *начальное состояние операционной среды* $e_0 \in$ E.

Работу порождающего процессора типов воздействий опишем в терминах конфигураций.

Определение 2. Под *конфигурацией процессора типов* воздействий будем подразумевать совокупность (*q*,*α*,*e*), где *q* — текущее состояние управления, *α*∈Γ*— содержимое магазина, *e*∈E — текущее состояние операционной среды, характеризующее деструктивные воздействия.

Определение 3. Начальной конфигурацией процессора типов воздействий назовем такую конфигурацию, в которой состояние управления — начальное ($q=q_0$): магазин пуст (α=ε), а состояние операционной среды равно начальному ($e = e_0$).

Определение 4. Конечная конфигурация процессора типов воздействий — это та, в которой текущее состояние управления — конечное ($q \in F$), а магазин пуст ($\alpha = \varepsilon$).

На множестве конфигураций введем отношение *непосредственного следования одной конфигурации после другой* ($\vdash$) следующим образом. Пусть (q_1,Z_α,e_1) — текущая конфигурация. Здесь $q_1 \in Q$ — текущее состояние управления, $Z \in \Gamma$ — текущий верхний символ магазина, $\alpha \in \Gamma^*$ — остаток магазинной цепочки, $e_1 \in E$ — текущее состояние операционной среды.

Для обоснования возможности представления типов воздействий для групповых и массовых возмущений семейством многослойных контекстно-свободных грамматик были сформулированы и доказаны следующие утверждения.

Утверждение 1 **(***описание типов* воздействий**).** Для контекстно-свободной грамматики $G=(V_N,V_T,P,S)$, порождающей непустой язык типов воздействий, можно найти эквивалентную контекстно-свободную грамматику G_1, в которой для любого нетерминала A существует терминальная цепочка x такая, что из $A \overset{*}{\underset{G_1}{\Rightarrow}} x$.

Определение 5. Нетерминалы из V_{N1} называются *продуктивными.*

В дополнение к исключению нетерминалов, из которых невозможно вывести ни одной терминальной цепочки, можно также исключать нетерминалы, которые не участвуют в выводах.

Утверждение 2 **(**с*уществование представления типов* воздействий**).** Для любой данной контекстно-свободной грамматики, порождающей непустой язык L типов воздействий, можно найти контекстно-свободную грамматику, порождающую язык L, такую, что для каждого ее нетерминала A существует вывод вида $S \overset{*}{\Rightarrow} x_1Ax_3 \overset{*}{\Rightarrow} x_1x_2x_3$, где $x_1,x_2,x_3 \in V_T^*$.

Работа выполнена при поддержке грантов РФФИ (№ 16-29-04268 офи_м) и Президента РФ (НШ-6831.2016.8).

Литература

1. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Organization of the entrusted calculations in crucial objects of informatization under uncertainty // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 307–309. DOI: 10.1109/SCM.2017.7970566.
2. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Analysis of computer security incidents using fuzzy logic // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 349–352. DOI: 10.1109/SCM.2017.7970587.

УДК 004.89

Модель организации устойчивых вычислений на основе теории многоуровневых иерархических систем

А.С. Петренко[1,2], Д.Д. Ступин[1,2]

[1]Московский физико-технический институт (государственный университет)
[2]ОАО «Концерн «Радиотехнические и информационные системы»

Для формирования модельного представления системы организации самовосстанавливающихся вычислений была разработана соответствующая двухуровневая модель на основе *теории многоуровневых иерархических систем М.Д. Месаровича*. При этом содержание названной модели было раскрыто в терминах *системы алгоритмических алгебр* (*САА) В.М. Глушкова*.

Для синтеза программ самовосстановления возмущенных вычислений потребовалось разработать систему знаний, которая позволила описать технологию порождения задач самовосстановления в соответствии с этапами *постановки задачи, планирования ее решения и последующей реализации*. В соответствии с этим формально

были определены *три информационные модели* и *одна модель управления процессом* решения задач.

Предложенный многомодельный подход принципиально отличается от известных одномодельных подходов и позволяет описать абстрактные программы самовосстановления возмущенных вычислений в *структурно-функциональном, логико-семантическом и прагматическом* аспектах. Такая многомодельная система организации управления самовосстановлением вычислений требует введения координации, позволяющей учесть специфику каждой названной функциональной модели, что, в свою очередь, приводит к необходимости построения соответствующей метамодели знаний. Исходя из структуры и содержания выделенных этапов прохождения задачи в качестве формализмов базовых моделей, в системе знаний целесообразно использовать *формальную грамматику, продукционную систему, автоматный преобразователь*.

При выборе аппарата метамоделирования предпочтение было отдано *системе алгоритмических алгебр (САА)*, предложенной *В.М. Глушковым*. Это позволило создать алгоритмическую систему, эквивалентную по своим изобразительным возможностям таким классическим алгоритмическим системам как машины *Тьюринга*, рекурсивные функции и алгоритмы *Маркова*. Преимуществами такого подхода, по сравнению с классическими алгоритмическими системами, являются возможность выражения структур абстрактных программ самовосстановления в дейкстровских типах (*последовательность, разветвление, цикл*), представление требуемых алгоритмов самовосстановления в виде алгебраических формул, совершенствование аппарата формальных преобразований, выражение алгоритма (технологии) самовосстановления в элементарных операторах, эффективное преобразование программ самовосстановления возмущенных вычислений в машинную реализацию [1, 2].

Предложенная адаптированная система алгебраических алгебр относится к числу многоосновных алгебраических систем и представляет собой пару базовых множеств $< A, L >$ с определенной сигнатурой операций Δ, где A – множество операторов, L – множество логических условий, принимающих значения из множества {*истина, ложь, неопределенность*}. Сигнатура операций САА $\Delta = \Delta_1 \cup \Delta_2$ состоит из системы Δ_1 логических операций, принимающих значение в множестве условий L, и системы Δ_2 операций, принимающих значения в множестве операторов A. В САА $< A, L >$ фиксируется система образующих $Ш$, представляющая собой конечную функционально полную совокупность операторов и логических условий. С помощью этой совокупности и посредством суперпозиции операций, входящих в Δ, порождаются произвольные операторы и логические условия из множества A и L. К логическим операциям системы Δ_1 относятся обобщенные булевы операции дизъюнкции, конъюнкции и отрицания, а также операция левого умножения условия на оператор $\beta=A\alpha$ и фильтрации. К множеству Δ_2 принадлежат следующие операции: композиция операторов $A * L$, последовательное выполнение операторов A и L, α-дизъюнкция операторов, альтернативное выполнение операторов A и L, т.е. $_{\alpha}(A \vee L) = A, если\ \alpha = 1$; $_{a}(A \vee L) = L, если\ \alpha = 0$; $_{a}(A \vee L) = J, если\ \alpha = o$. Здесь α-итерация оператора А по условию $\alpha_{\alpha}\{A\}$ состоит в проверке условия α; если это условие ложно, то осуществляется выполнение оператора A.

Отметим, что представление $< A, L >$ операторов из A посредством суперпозиции входящих в сигнатуру Δ операций позволяет выработать эффективные процедуры регуляризации (сведение к регулярной схеме (РС)) $F(Ш)$ и доказать теорему, которая определяет принципиальную возможность формального описания произвольного алгоритма, процедуры или технологии самовосстановления возмущенных вычислений в регулярной схеме. Таким образом, стало возможным формально описать технологические и процедурные знания самовосстановления возмущенных вычислений в виде регулярной

схемы, что принципиально обуславливает возможность синтеза абстрактных программ самовосстановления и их последующего использования.

Применение комбинированной модели требует различных представлений данных. Поэтому возникает необходимость нахождения общего механизма выражения *декларативных, декларативно-процедуральных, процедуральных* знаний и их совместного использования. В качестве такого механизма может быть использована *алгебра структур данных (АСД)*, которая базируется на теории САА и ориентирована на распознавание и порождение исходных, результирующих и промежуточных данных. Алгебра структур данных относится к числу многоосновных алгебраических систем и представляет собой пару базовых множеств $\langle \hat{O}, \hat{P} \rangle$ с определенной сигнатурой операций Ω, где $\hat{O} = O / O \subset F(T)$ – множество объектов, $T=S \bigcup W$, $S \cap W=$O, S – множество обрабатываемых данных, W – множество ограничителей, $F(T)$ – множество всех конечных последовательностей символов (конфигураций) в алфавите T; $\hat{P} = \{\alpha/0, 1, \mu\}$ – множество трехзначных логических условий. В сигнатуру Ω включены соответствующим образом интерпретированные операции сигнатуры САА, а также некоторые специальные операции над структурами данных. Для АСД $\langle \hat{O}, \hat{P} \rangle$ существует базис Σ, состоящий из элементарных объектов $O=\{o_i,\ i=1,\ldots,\ n\}$ и элементарных логических условий $P=\{a_i,\ i=1,\ldots,\ m\}$. Объектной регулярной схемой (ОРС) $F_q(\sum)$ называется представление объекта O и $\hat{O}$ в АСД $\langle \hat{O}, \hat{P} \rangle$ в виде суперпозиции операций, входящих в сигнатуру Ω, над элементами из Σ, где q – указание режима применения объекта и направления сканирования, $\Pi=\{\overleftarrow{\Pi}, \vec{\Pi}\}$ и $P=\{\overleftarrow{P}, \vec{P}\}$ при левостороннем и правостороннем порождении (распознавании) конфигурации схемой $F_q(\Sigma)$.

Для формализации структурированных процессов над стандартизированной памятью вычислений в терминах РС была использована форма представления АТП(n)-автоматов в виде управляющей грамматики.

В дальнейшем это позволило разработать ряд макро- и микромагазинных распознавателей структуры типов воздействий по данным регистрации фактов групповых и массовых возмущений вычислений. Разработать метод порождения комбинаций сочетанных типов воздействий, приводящих к разнородно массовым возмущениям вычислений современных вычислительных систем.

Работа выполнена при поддержке грантов РФФИ (№ 16-29-04268 офи_м) и Президента РФ (НШ-6831.2016.8).

Литература

1. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Organization of the entrusted calculations in crucial objects of informatization under uncertainty // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 307–309. DOI: 10.1109/SCM.2017.7970566.
2. *Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K.* Analysis of computer security incidents using fuzzy logic // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. V. 1. P. 349–352. DOI: 10.1109/SCM.2017.7970587.

УДК 519.688

Использование группы мобильных роботов для решения задач поиска людей на заранее заданной территории

Д.В. Яцкин

Московский физико-технический институт (государственный университет)

Введение

В настоящей работе рассматривается мониторинг пространства, ставится задача оперативного обнаружения заранее заданного объекта на определенной территории (при

его появлении). Среди таких задач наиболее интересной кажется задача поиска и распознавания человеческого лица на заранее заданной ограниченной территории, часто возникающие при ведении военных действий, ликвидации последствий катастроф и стихийных бедствий, мероприятий по освобождению заложников и так далее.

Задача делится на две принципиальные части: задачи распознавания и геометрического расположения.

Предлагается решать эту задачу децентрализованной сетью мобильных роботов. Такой подход имеет ряд преимуществ, среди которых масштабируемость, гибкость, оперативность развертывания и свертывания системы (а следовательно, перебазирования), самоорганизационная устойчивость к изменению факторов воздействия внешней среды (вплоть до факторов, выводящих из строя устройства), а также возможность создания за счет изменения количества роботов широкой области обзора, под чем понимается область, при появлении целевого объекта в которой обнаружение может быть осуществлено без изменения геометрического положения устройств.

Задача геометрического расположения

Ставится задача поиска такого расположения L(t) заданного числа роботов N, при котором обнаружение осуществляется наиболее быстро. Здесь возникает два принципиально разных случая, описание которых, а также подходы и алгоритмы для решения соответствующих задач содержатся в работе [1].

Экспериментальная часть

Для тестирования разработанных подходов и алгоритмов была использована модель сети, представляющая собой девять одинаковых мультироторов с установленным на них соответствующим оборудованием.

Задача, которую выполняет указанная сеть, сводится к следующему. Девятью мультироторами осуществляется облет заранее заданной территории с целью наиболее быстро детектировать человеческое лицо. При обнаружении объекта передается соответствующий сигнал десятому мультиротору, который подлетает к месту, в котором было обнаружено лицо, и кладет туда некий предмет, которым он снабжается изначально.

- Территории разного размера.

Было проведено исследование зависимости среднего времени выполнения задачи t_{av} от размера (площади) территории.

- Использование различных траекторий облета.

Мы сравнили два популярных алгоритма облета, которые условно можно назвать «змейкой» и «по спирали».

- Открытая и закрытая территории.

На открытой территории устройства ориентируются по GPS-координатам, на закрытой используется алгоритм визуальной одометрии.

Заключение

В работе были приведены и описаны модели, методы и алгоритмы патрулирования пространства на примере задачи обнаружении человеческого лица на заранее известной территории. Работоспособность описанных алгоритмов была подтверждена экспериментами, на их основании были сделаны выводы об эффективности и границах применимости подходов.

Работа выполнена при поддержке РФФИ (грант № 16-29- 04268) и гранта Президента РФ (НШ-6831.2016.8).

Литература

1. *Кочкаров А.А., Яцкин Д.В., Рахманов О.А.* Особенности решения задачи геометрического мониторинга// Известия ЮФУ. Технические науки. 2016. № 2(175). С. 158–168.

УДК 621.396.96

Повышение помехозащищенности РЛС дальнего обнаружения в зоне прямой видимости с помощью пассивной многопозиционной подсистемы

Х.Д. Гордеева

Московский физико-технический институт (государственный университет)
ОАО «НПК «НИИДАР»

Рассматривается один из возможных вариантов защиты РЛС дальнего обнаружения (РЛС ДО) от источников шумовых помех (ИШП) посредством создания многопозиционного пассивного радиолокационного комплекса (МПРК), определяющего координаты помехи. Приводится описание структуры МПРЛК и численный расчет потенциально достижимых точностных характеристик и их сравнение с аналогичными характеристиками однопозиционной РЛС.

В качестве ИШП рассматриваются непрерывные маскирующие помехи, которые могут быть неподвижными или подвижными. Положение ИШП относительно РЛС может быть произвольным в пределах зоны действия МПРЛК.

В предлагаемом МПРЛК одна приемная позиция находится в месте расположения РЛС ДО, вокруг на воображаемой окружности радиусом L равномерно распределены еще четыре вынесенных приемных позиции (ВПП). Антенны всех приемных позиций подсистемы являются всенаправленными.

Для определения координат ИШП используется разностно-дальномерный (гиперболический) метод. С помощью корреляционной обработки оценивается разность задержек прихода двух сигналов по трассам «помеха – ВПП» и «помеха – центральная позиция».

Зона действия МПРК :

- по дальности: от точки стояния РЛС ДО до предела прямой видимости (обычно не более 30 км);
- по углу места: от 0^0 до максимального значения, совпадающего с аналогичным значением угла места РЛС ДО;
- по азимуту: от 0^0 до 360^0.

При получении выражений для потенциально достижимых точностных характеристик предполагается, что измерения осуществляются на фоне белого гауссовского шума и отношение сигнал/шум одинаковы для всех приемных позиций.

Точные выражения для СКО оценки координат ИШП достаточно громоздки, поскольку в них входят нелинейные зависимости от угловых координат ИШП. Однако в двух предельных случаях, когда отношение R/L либо велико, либо, наоборот, мало, можно воспользоваться линейным приближением по параметру R/L. Первый случай $(R/L >> 1)$ рассмотрен в [1]. Во втором случае $(R/L << 1)$ выражения для СКО оценки дальности σ_R, азимута σ_β и угла места σ_ε ИШП для рассматриваемого МПРЛК в единичном измерении примут вид [2,3]:

$$\sigma_R = \sqrt{\frac{2}{m}}\frac{\sigma(\Delta R)}{\sqrt{2+cos^2\varepsilon}}, \tag{1}$$

$$\sigma_\beta = \sqrt{\frac{2}{m}}\frac{\sigma(\Delta R)}{R\cos\varepsilon}, \qquad \sigma_\varepsilon = \sqrt{\frac{2}{m}}\frac{\sigma(\Delta R)}{R\sin\varepsilon}. \tag{2}$$

Для сравнения приведем СКО оценки координат однопозиционной РЛС. При учете шумовых ошибок и увеличения ширины луча при отклонении от нормали к антенной решетке СКО оценки азимута $\sigma_{\beta 0}$ и угла места $\sigma_{\varepsilon 0}$ имеют вид [4]:

$$\sigma_{\beta 0} \approx \frac{0{,}1\theta_\beta}{\cos\beta} \qquad \sigma_{\varepsilon 0} \approx \frac{0{,}1\theta_\varepsilon}{\cos\varepsilon}, \tag{3}$$

где θ_β и θ_ε – ширина луча РЛС по азимуту β и углу места ε.

СКО σ_R оценки дальности R до цели в единичном измерении определяется как [4]:

$$\sigma_{R0} = 0{,}1\Delta R. \quad (4)$$

где ΔR – разрешающая способность РЛС по дальности.

Для получения численных оценок использовались следующие параметры: радиус окружности, на которой располагаются ВПП L=5 км; разрешающая способность РЛС ДО по дальности ΔR = 10 м; ширина луча РЛС ДО $\theta_\beta = \theta_\varepsilon = 3^0$; зона действия по азимуту β от 0^0 до 50^0 и по углу места ε от 2^0 до 50^0; расстояние от ИШП до ВПП R от 0 до 5 км.

В таблице 1 представлены результаты вычисления относительных СКО оценок координат в соответствии с формулой

$$\delta X = \frac{\sigma_X}{\sigma_{X0}}, \quad (5)$$

где $X = R, \beta, \varepsilon$.

Прежде всего отметим, что зависимость $\sigma_R(\varepsilon)$ является более сложной, хотя и менее выраженной, чем зависимости $\sigma_\beta(R, \varepsilon)$ и $\sigma_\varepsilon(R, \varepsilon)$ от угла места.

Значение СКО оценки дальности не зависит от дальности до объекта, что выгодно отличает большебазовый МПРЛК ($R/L << 1$) от малобазового ($R/L >> 1$) при прочих равных условиях.

Значения СКО оценки угловых координат быстро возрастают по мере приближения ИШП к центральной позиции МПРЛК, что, впрочем, не касается значений линейных угловых СКО, которые не зависят от R. Кроме того, значения СКО угла места для МПРЛК превышают аналогичные величины для однопозиционной РЛС при малых значениях углах места.

Таким образом, показана возможность посредством пассивного МРЛК с достаточно высокой точностью определять координаты ИШП, в том числе находящиеся в непосредственной близости от РЛС ДО.

Таблица 1

Зависимость относительной СКО оценки дальности δR и угловых координат $\delta\beta(\beta,\varepsilon)$, $\delta\varepsilon(\varepsilon)$ от угла места (азимут $\beta = 0^0$, расстояние до ИШП R = 1 км)

ε ,град.	4	6	8	12	18	24	34	50
$\delta R(\varepsilon)$	0,817	0,818	0,819	0,822	0,83	0,84	0,863	0,91
$\delta\beta(R,\beta,\varepsilon)$	0,271	0,272	0,272	0,276	0,28	0,3	0,33	0,42
$\delta\varepsilon(R,\varepsilon)$	3,86	2,57	1,92	1,27	0,83	0,6	0,4	0,23

Литература

1. *Гордеева Х.Д.* Малобазовая подсистема определения координат источника шумовых помех находящихся с зоне прямой видимости РЛС дальнего обнаружения // Труды IV Всероссийской научно-технической конференции «РТИ Системы ВКО — 2016». 2017. С. 49–54
2. *Черняк В.С.* Многопозиционная радиолокация. – М.: Радио и связь, 1993. 416 с.
3. *Градштейн И.С., Рыжих И.М.* Таблицы интегралов, сумм, рядов и произведений. – М.: Физматгиз, 1963. 1100 с.
4. *Бартон Д., Вард Г.* Справочник по радиолокационным измерениям: пер. с англ. под ред. М.М. Вейсбейна. – М.: Сов. Радио, 1976. 392 с.

УДК 004.724

Комбинированный метод множественного доступа в сети тактических беспилотных летательных аппаратов

А.Р. Володкин, Р.А. Шевченко

ОАО «Радиотехнический институт им. академика А.Л. Минца»

На сегодняшний день существует множество беспилотных летательных аппаратов (БЛА) различных по своим тактико-техническим характеристикам. Основными параметрами их классификации согласно ассоциации UAV International являются: взлетная масса, предельные дальность (R), высота и продолжительность полета. Но независимо от их типа, до появления технологий, позволяющих БЛА осуществлять полностью автономные полеты без участия оператора, каждому из них требуется радиолиния, предоставляющая управление и контроль над их перемещением для обеспечения безопасности их полетов.

В настоящее время для малых БЛА (классификации Nano, Micro, Mini (R < 10 км)), а также для БЛА ближнего радиуса действия (классификаций close range, short range, R< 70 км, максимальная скорость полета V < 130 км/ч) достаточно существующих современных стандартов связи из группы семейства IEEE 802.xx.xx. В свою очередь для обеспечения связи с наземным пунктом управления (НПУ) тактических БЛА на дальностях 70 – 500 км (классификации: medium range (MR), medium range endurance (MRE) и low altitude deep penetration (LADP)) требуется либо применение спутниковых каналов радиосвязи, либо разработка специализированных радиоэлектронных комплексов командно-информационного взаимодействия, работающих посредством радиолинии прямой радиовидимости (LOS – Line of Sight).

При построении LOS- радиоканалов для высокомобильных БЛА возникает ряд специфических требований (массогабаритные, работа при больших смещениях по Доплеру, дальность работы, скорость передачи данных), накладывающих ограничения на организацию сетевого взаимодействия нескольких БЛА в пределах одного НПУ.

Одной из основных проблем, возникающих в ходе создания сети комплекса БЛА, является сложность организации множественного доступа (ОМД) сети БЛА к НПУ. К сожалению, базовые методы ОМД [1, 2] слабо применимы в случаях создания комплекса БЛА с LOS радиоканалом.

Рассмотрим преимущества и недостатки применения каждого из них.

1. Частотное разделение канала (FDMA) требует создания двух каналов: uplink и downlink для каждого БЛА и НПУ, также требуется разнесение частотных каналов для избегания межканальной интерференции, в результате для организации FDMA требуется больший частотный диапазон при увеличении количества БЛА в сети. С другой стороны, FDMA упрощает создание сетевого взаимодействия, так как в результате для каждого абонента сети у нас имеется фиксированный и независимый частотный канал радиосвязи.

2. Временное разделение канала (TDMA) позволяет всем абонентам сети работать в одной частотной полосе сигнала. В свою очередь требовательно к временной синхронизации сети также при большом количестве абонентов возникают дополнительные задержки передачи данных в моменты ожидания своего временного слота.

3. Кодовое разделение канала (CDMA) чувствительно к разности мощности принимаемого сигнала от различных абонентов, которая образуется из-за большого разброса дальности участников сети от базовой станции (в нашем случае НПУ). Например, в случае работы НПУ с одним БЛА в зоне аэродрома (порядка 1 – 5 км) и с другим БЛА на предельном удалении (свыше 250 км) разность в мощности принимаемого на НПУ сигнала превышает 34 дБ. Что делает данный метод ОМД малоприменимым в случаях сетевого взаимодействия тактических БЛА.

4. Пространственное разделение канала (SDMA) реализуется путем формирования независимых радиоканалов на разных угловых направлениях БЛА относительно НПУ. Предъявляет жесткие требования к ширине ДН антенн, также делает малоудобным

эксплуатацию комплекса, так как накладывает ограничение на пространственное применение БЛА.

5. Поляризационное разделение канала (PDMA) малоприменимо в комплексах с летательными аппаратами, так как при различных углах крена, тангажа и ракурса БЛА относительно НПУ будет меняться направление вектора поляризации, что требует дорогостоящей пространственной стабилизации антенн.

Таким образом, стоит отметить, что при организации сетевого взаимодействия в группе тактических беспилотников принципиальное значение имеет физический облик радиоканала (частота, полоса, ДН антенн и массогабаритные требования к терминалам связи). Рассмотрим создание комбинированного метода ОМД для сети из 4 БЛА, работающих на двух независимых и динамически меняющихся тактических направлениях (угловое расстояние в азимутальной плоскости превышает ширину ДН наземной антенны) по два БЛА в каждом. При этом для обеспечения больших дальностей работы и высокой скорости обмена на земле используются антенны, работающие в направленном режиме.

Работа групп БЛА на различных тактических направлениях и использование направленных антенн на НПУ вынуждает обеспечивать пространственное разделение канала SDMA.

Следующим этапом ОМД является его организация внутри каждой группы из двух БЛА. SDMA и PDMA здесь не применимы, так как работа группы ведется в пределах ширины ДН наземного антенного комплекса, а БЛА являются высокомобильными объектами. CDMA также малоприменим, ввиду возможности работы БЛА в группе на большой разности удалений от НПУ. Таким образом, остаются TDMA и FDMA, при этом предлагается разнесение групп методом частотного разделения для избегания межканальной интерференции на наземном пункте управления, внутри группы реализуется временное разделение, которое позволяет избежать межканальной интерференции внутри группы.

В результате для решения задачи по обеспечению множественного доступа двум группам БЛА на независимых тактических направлениях предлагается комбинированный метод, состоящий из последовательного применения SDMA, FDMA и TDMA.

Литература

1. *Lou Frenzel*. Fundamentals of Communications Access Technologies: FDMA, TDMA, CDMA, OFDMA, and SDMA // Electronic Design. 2013.
2. *Rom Raphael; Sidi Moshe* Multiple Access Protocols: Performance and Analysis// Springer-Verlag/University of Michigan (1990) P. 176.

УДК 62-50

Разработка модели фазированной антенной решетки 3D в MATLAB

Нгуен Ван Кхыонг

Московский физико-технический институт (государственный университет)

Основной особенностью антенны с фазированной решеткой является ее способность управлять амплитудным и фазовым возбуждением каждого излучающего элемента для формирования и сканирования главного лепестка электронным управлением без каких-либо механических вкладов. В данной работе рассматривается разработанная модель антенных решёток. Представлена модель расчёта диаграммы направленности антенн в виде 2D и 3D в MATLAB. Программа создана для автоматизации задачи получения диаграммы направленности антенн, в 2D- и 3D- форматах. Разработана модель фазированных антенных решёток (ФАР) со случайным расположением элементов решетки и с равноудалёнными элементами решетки. Решение этой работы важно с точки зрения практического приложения, так как позволяет создавать системы приемопередачи с высокой скрытностью и высокой помехозащищенностью сигналов.

В данной работе проводятся исследования по анализу линейных антенн решеток (а также плоских) и уменьшению боковых лепестков в линейных и плоских антенных решетках с изменением различных параметров антенны и сигналов. Формирование главного луча и введение в диаграмму направленности провала осуществляется с использованием синтеза комплексных амплитуд токов в излучателях. Также стоит отметить, что процедура синтеза предполагает довольно большие вычисления и занимает достаточное количество времени. Чтобы сократить продолжительность процедуры подготовки системы к формированию требуемой формы диаграммы направленности, соответствующие распределения амплитуд и фаз токов в излучателях должны быть посчитаны заранее и сохранены в памяти соответствующих блоков управления фазированной антенной решетки.

Литература

1. *Нефедов Е.И.* Антенно-фидерные устройства и распространение радиоволн: учебник, М.: Издательский центр «Академия», 2006.
2. *Пистолькорс А.А., Литвинов О.С.* Введение в теорию адаптивных антенн. М.: Наука, 1991.
3. Устройства СВЧ и антенны: учебник для вузов / *Д.И. Воскресенский, В.Л. Гостюхин, В.М. Максимов, Л.И. Пономарев*; под ред. *Д.И. Воскресенского*. М.: Радиотехника, 2006.
4. *Шифрин Я.С.* Вопросы статистической теории антенн: учебник / Я.С. Шифрин. – М.: Советское радио, 1970.
5. *Appelbaum S.P.* // IEEE Trans. on AP. 1996. V. AP-24. N 5. P. 585–598.
6. *Monzingo R.A., Miller T.W.* Adaptive Arrays. John Wiley and Sons, New York, 1980.
7. *Mailloux R.J.* Phased Array Antenna Handbook. Boston, London Artech House, 1994.

УДК 629.3.051

Исследование методов распределенной локальной навигации при взаимодействии гетерогенных роботов

И.А. Калинов

Московский физико-технический институт (государственный университет)
Сколковский институт науки и технологий

Рой роботов стал новой исследовательской парадигмой за последние десять лет, которая предлагает новые подходы такие как: самоорганизация, саморепликация, самоподготовка и самообучение для решения комплекса распределенных задач. До настоящего времени большинство существующих роевых технологий для роботов были разработаны и внедрены с однородным аппаратным обеспечением. Лишь некоторые из них имеют гетерогенных роботов, но такие система чаще всего ограничены физически и поведенчески. Из-за отсутствия методов и инструментов разработчики роя роботов не могут достичь требуемой сложности для приложений реального мира. На данный момент вопрос решения задач с помощью мультиагентной системы роботов не решен до конца. В большинстве таких систем применяются однотипные роботы для решения определенной задачи путем дробления ее на мелкие, однотипные подзадачи и распределение этих подзадач каждой конкретной робоединице в системе. Большинство таких работ посвящено алгоритмам распределения функций роботов в группе, разработке протоколов обмена данными или решения задач поиска и мониторинга. В данной работе ключевым моментов исследований является распределенный подход в локальной навигации группы гетерогенных роботов, в ходе реализации работы также проведено комплексное исследование методов решения задачи распределенной навигации с использованием различных сенсоров.

Изучаемые вопросы являются фокусом современных исследований в области построения мультиагентных систем роботов, но тем не менее на данный момент не предложено ни одного универсального подхода параллельного построения карты с использованием алгоритмов локальной навигации при помощи одного беспилотного наземного робота (БНР) и нескольких беспилотных летательных аппаратов (БЛА) и

верификации полученных данных с взаимокалибровкой. Разработка универсального подхода в области распределенной локальной навигации при участии гетерогенных роботов позволит масштабировать его на любые другие проекты, связанные с роевыми технологиями. Также стоит отметить, что работы в этой области по большей части затрагивают только построение 2D-карт, нежели 3D, которые более близки к выполнению реальных задач. Для обработки изображений с внешних камер в работе планируется применять алгоритм визуальной одометрии, который объединяет преимущества прямых и функциональных методов. Будет использован алгоритм выравнивания разреженного изображения, эффективный прямой подход к оценке движения кадра к раме, который минимизирует фотометрическую ошибку признаков, лежащих на краях интенсивности. 3D-точки, соответствующие функции получены с помощью надежного рекурсивного байесовского, а затем будет уточнена структура изображения для достижения максимальной точности.

Работа выполнена при поддержке РФФИ (грант № 16-29-04268) и гранта Президента РФ (НШ-6831.2016.8).

Литература

1. *Preiss A., James, Honig, Wolfgang, Sukhatme, Gaurav, Ayanian, Nora.* Crazyswarm: A large nanoquadcopter swarm // IEEE International Conference on Robotics and Automation. 2017. P. 3299–3304.
2. *Bandala, Argel, Maningo, Jose Martin, Faelden, Gerard Ely & Christian S. Nakano, Reiichiro & Dadios, Elmer.* Obstacle Avoidance for Quadrotor Swarm Using Artificial Neural Network Self-Organizing Map // International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management, 2015. P. 1–7.
3. *Philipp Fleck, Clemens Arth, Christian Pirchheim, Dieter Schmalstieg* Tracking and Mapping with a Swarm of Heterogeneous Clients IEEE International Symposium on Mixed and Augmented Reality, 2015. P. 136–139.

УДК 681.2

Применение интегрированного оптико-электронного сенсора для оценки вариабельности сердечного ритма

М.Ф. Файзуллин, И.В. Гончар

Московский физико-технический институт (государственный университет)

Изменчивость продолжительности интервалов последовательных циклов сердечных сокращений за определенные промежутки времени – вариабельность сердечного ритма (ВСР) – имеет важное значение при оценке психофизиологического состояния человека [1, 2]. Основной способ исследования ВСР – это анализ интервалограмм, получаемых при считывании сигнала электрокардиограммы (ЭКГ) [2] с выделением из него так называемых R-зубцов – ярко выраженных однополярных импульсов значительной амплитуды [3].

В некоторых случаях считывание ЭКГ бывает затруднительным или невозможным: электромагнитные помехи, неудобство подключения электродов и транспортировки оборудования. В таких случаях альтернативой электрокардиографии может стать фотоплетизмография – метод исследования кровенаполнения живых тканей организма, основанный на регистрации пульсовых колебаний оптической ткани, обусловленных функцией сердца [4].

В работе описывается структура оптико-электронного сенсора [5] в составе носимого наручного браслета, считывающего сигналы фотоплетизмограммы (ФПГ), электрической активности кожи и ускорения. Также производится оценка результатов анализа ВСР по сигналу ФПГ и сравнение полученных результатов с аналогичными для сигнала ЭКГ, выясняются принципиальные ограничения использования метода фотоплетизмографии и делается вывод о возможности применения фотоплетизмографии для анализа ВСР.

Минимальной рекомендуемой частотой дискретизации сигнала ЭКГ для анализа ВСР принята частота 500 Гц [6]. Этот выбор связан прежде всего с малой длительностью QRS-комплекса сигнала ЭКГ, составляющего менее 0,1 с [7]. При этом анализ ВСР по сигналу ФПГ производится с помощью выделения пиков этого сигнала, которые имеют бо́льшую длительность [8, 9], чем QRS-комплекс сигнала ЭКГ, поэтому частота дискретизации сигнала ФПГ может быть выбрана меньшей. В работе оценивается оптимальная частота дискретизации сигнала ФПГ для конкретного сенсора.

Литература

1. *Родионов А.В.* Клиническое значение исследования вариабельности сердечного ритма. М., 2002. Режим доступа: http://www.medicus.ru/cardiology/specialist/klinicheskoe-znachenie-issledovaniya-variabelnosti-serdechnogo-ritma-21369.phtml
2. Физиология человека / под ред. профессора В.М. Смирнова. 1-е изд. М.: Медицина, 2002. 608 с.
3. Heart Rate Variability. Standards of Measurement, Physiological Interpretation, and Clinical Use. Task Force of the European Society of Cardiology the North American Society of Pacing Electrophysiology // Circulation. 1996. V. 93, N 5. P. 1043–1065.
4. *Yanowitz F.G.* Characteristics of the Normal ECG. University of Utah School of Medicine, 2006. https://ecg.utah.edu/lesson/3
5. *Shelley K., Shelley S. Pulse*. Oximeter Waveform: Photoelectric Plethysmography. Clinical Monitoring/Carol Lake, R. Hines, and C. Blitt, Eds. W.B. Saunders Company, 2001. P. 420–428.
6. MAX30102 High-Sensitivity Pulse Oximeter and Heart-Rate Sensor for Wearable Health https://datasheets.maximintegrated.com/en/ds/MAX30102.pdf
7. *James J.* [*et al*.]. Recommendations for Standardization andSpecifications in Automated Electrocardiography: Bandwidth and Digital Signal Processing.
8. *Jeyhani V. Jeyhani V., Mahdiani S., Peltokangas M., Vehkaoja A.* Comparison of HRV parameters derived from photoplethysmography and electrocardiography signals // 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) P. 5952–5955.
9. *Lin Wan-Hua* [*et al.*]. Comparison of Heart Rate Variability from PPG with That from ECG. The International Conference on Health Informatics // 2014. IFMBE Proceedings. V. 42. Springer. Cham.

УДК 519.1:004.94

Структурно-динамический подход к изучению сетевого противоборства

А.А. Кочкаров

Московский физико-технический институт (государственный университет)
Финансовый университет при Правительстве РФ
ОАО «РТИ»

Достижения современной радио- и микроэлектроники за последние 15–20 лет существенно изменили отраслевую структуру мировой экономики. Это произошло вследствие двух инженерных, в смысле появления новых технологий, революций. Во-первых, миниатюризация бытовой электроники привела к постоянному нахождению ее с пользователем, т.е. бытовая электроника, в первую очередь средства связи, стали носимыми. Во-вторых, широкое распространение (покрытие) беспроводных сетей связи позволило пользователям носимой электроники постоянно находиться в зоне доступа сети, а значит, быть вовлеченным в постоянное сетевой общение. Тенденцией последней декады стало объединение операторов сотовой связи, интернет-провайдеров и их последующая глубокая интеграция с сектором финансовых (банковских) услуг. Это фактически создало новый формат мировой экономики, названной сначала сетевой экономикой [1], а потом и цифровой. Второе понятие является более широким, которое включает в себя не только новые сетевые модели отраслей и отдельных предприятий на основе современных инфокоммуникационных технологий, но и денежно-товарные отношения на основе обращения криптовалют. Такая глубокая интеграция сетевых систем (информационных, коммуникационных и финансовых) несомненно упрощает доступ для пользователей к различным услугам, но и создает новые вызовы и угрозы [2].

Производными от понятия «сетевая экономика» в содержательном контексте стали понятия «сетевые медиа», «сетевая конкуренция» [3], «сетевые войны и кибербезопасность» [4]. Последнее понятие является предметом исследования настоящего проекта как одного из ключевых вызовов современной цифровой реальности постиндустриального общественного уклада. Несомненно, одними из ключевых инструментариев в таком исследовании должны стать подходы компьютерного моделирования (для проведения эксперимента) и дискретной математики (как основы компьютерных наук) и синергетики (как идеологической основы для междисциплинарных исследований).

Сетевое пространство, рассматривая его в виде интеграции различных отраслевых и инженерных сетей, перечисленных ранее (и не только их), следует рассматривать как неоднородную среду. С позиций компьютерного и/ или математического моделирования, точнее сказать, дискретную динамическую среду (по сути – нелинейную среду). Для моделирования такой среды целесообразно использовать абстрактный математический объект – динамический граф. Динамический граф представляет собой последовательность «классических» графов, переход между которыми описывается различными теоретико-графовыми операциями (удаление/добавление ребра, удаление/ добавление вершины, замена вершины затравкой, приоритетное присоединение вершин и ребер и т.д.). Динамический граф может описывать изменчивость сетевого пространства, но не взаимодействие (жизнедеятельность) участников сетевой среды – сетевого пространства. Описание взаимодействия участников сетевой среды разумно описать на основе теории многоагентных систем, в упрощенном варианте – на основе клеточных автоматов. Такой модельный симбиоз нескольких классических теорий в комплексе позволит формировать уникальный подход для описания сложного взаимодействия агентов (иначе, акторов или участников) сетевого пространства. Одним из ключевых достоинств этого подхода является взаимное влияние друг на друга сетевой среды и поведения ее участников, т.е. четкая связь между структурой сетевого пространства в каждый момент дискретного времени и поведением (правилами взаимодействия) агентов. Под агентами в данном подходе подразумеваются различные участники сетевого пространства – как программы (автономные, самообучаемые и др), так и люди. Как известно, одним из ключевых явлений в сетевом пространстве, требующим детального исследования, является сетевое противоборство (информационные войны, сетевые войны, сетевая или информационная конкуренция).

Предложенный подход позволит формализовать несколько конкретных направлений в области сетевого противоборства и кибербезопасности таких, как идентификация сетевого противоборства (конкуренции) и его этапов, идентификация сторон противоборства (конкуренции), идентификация сценариев протекания противоборств (конкуренции) и т.п.

Исследования в области сетевого противоборства или кибервойн в мировой науке не имеют достаточно широкого обсуждения. Но о важности исследований в этой области свидетельствуют в первую очередь государственные документы международного и национального уровня [5–9].

По доступной научной литературе напрашивается вывод о превалировании в исследованиях по проблемам сетевого противоборства и кибервойн инженерно-механистического [10–11] и описательного семантического, а также правового подходов [12–13], нежели строго математического и компьютерно-модельного подходов.

Именно на восполнение этого пробела в изучении сетевого противоборства и направлена настоящая работа.

Работа выполнена при поддержке РФФИ (грант № 16-01-00342) и РГНФ (грант № 16-23-01005).

Литература

1. *Бугорский В. Н.* Сетевя экономика. М.: Финансы и статистика, 2008. 256 с.
2. *Катасонов В.Ю.* Цифровые финансы. Криптовалюты и электронная экономика. Свобода или концлагерь? М.: Книжный мир, 2017. 320 с.

3. *Castells M*. The Rise of the Network Society: // The Information Age: Economy, Society, and Culture. Volume I. WILEY-BLACKWELL A John Wiley & Sons, Ltd., Publication. 2010. 625 p.
4. *Петренко С.А., Ступин Д.Д.* Национальная система раннего предупреждения о компьютерном нападении. – Иннополис: «Издательский дом «Афина», 2017. 440 с.
5. Двусторонний проект Россия – США по кибербезопасности. Основы критически важной терминологии. 2011 Изд. 1; [Электронный ресурс]. – Режим доступа: http://iisi.msu.ru/UserFiles/File/Terminology %20IISI %20EWI/Russia-U %20S %20 %20bilateral %20on %20terminology %20RUS.pdf.
6. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 года № 646).
7. *Клабуков И.Д., Алехин М.Д., Нехина А.А.* Исследовательская программа DARPA на 2015 год. М, 2014.
8. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12 декабря 2014 года, № К 1274).
9. An evaluation Framework for National Cyber Security Strategies [Electronic resource] / European Union Agency for Network and Information Security. 2014. Режим доступа: https://www.enisa.europa.eu/activities/ResilienceandCIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1.
10. *Петренко С.А., Ступин Д.Д.* Национальная система раннего предупреждения о компьютерном нападении. Иннополис: «Издательский дом «Афина», 2017. 440 с.
11. Military Perspectives on Cyberpower / Edited by L. Wentz, C. Barry, S. Starr. – CreateSpace Independent Publishing Platform, 2012. 128 p.
12. *Libicki M.* Cyberdeterrence and Cyberwar / RAND Corporation, 2009. 214 p [Электронный ресурс]. Режим доступа: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
13. *Clarke R.* Securing Cyberspace Through International Norms / Good Harbor Security Risk Management Режим доступа: http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf.

Секция инфокоммуникационных систем и интеллектуальных информационных технологий

УДК 621.391.037.372

Расширение набора распознаваемых видов манипуляции в задаче автоматического распознавания вида цифровой модуляции

В.Н. Дам

Московский физико-технический институт (государственный университет)

Вид модуляции является одной из важнейших характеристик, которые используются для идентификации и мониторинга радиосигналов. Распознающее устройство должно правильно классифицировать вид модуляции входящих сигналов при наличии шумов. Одним из перспективных направлений является расширение набора распознаваемых видов модуляции.

В настоящее время потребность в беспроводных мультимедийных услугах связи быстро растет. Поэтому весьма перспективным становиться применение мультиплексирования с ортогональным частотным разделением (OFDM). Примерами этой тенденции являются семейства стандартов IEEE 802.11 и IEEE 802.16 для беспроводных локальных сетей WLAN. Включение OFDM в набор распознаваемых видов модуляции представляет собой актуальную задачу. В [1, 2] предложен способ и устройство, которое позволяет распознавать сигналы с одночастотной модуляцией (single carrier) от сигналов с многочастотной модуляцией (OFDM).

OFDM (Orthogonal frequency division multiplexing) является цифровой схемой модуляции, состоящей из большого количества близко расположенных ортогональных поднесущих. Каждая поднесущая модулируется по обычной схеме модуляции (например, частотная, квадратурная амплитудная модуляция) на низкой символьной скорости, сохраняя общую скорость передачи данных, как и у обычных схем модуляции одной несущей в той же полосе пропускания [3].

Исходными данными являются синфазная и квадратурная составляющие OFDM для разных видов модуляции с выходов согласованных фильтров. Синфазная и квадратурная составляющие используются для вычисления оценок кумулянтов (признаков) [4], которые в качестве входа поступают в обученную нейронную сеть для распознавания. Таблица 1 представляет результаты распознавания видов модуляции при отношении сигнала к шуму 20 дБ.

Результаты тестирования показывают, что включение вида OFDM в набор видов модуляции не влияет на вероятности распознавания других видов. При этом вероятность распознавания вида OFDM практически равна 100%. Дальнейшие исследования будут направлены на применение результатов в конкретной реальной системе коммуникации.

Таблица 1.

Результаты распознавания вида модуляции (в процентах) при ОСШ = 20 дБ

Вид модуляции	2-PSK	4-PSK	8-PSK	2-FSK	8-QAM	16-QAM	64-QAM	OFDM
Вероятность распознавания	100	100	100	100	100	85.6	87.9	100

Литература

1. *Аджемов С.С., Терешонок М.В., Чиров Д.С.* Способ и устройство автоматического распознавания типов манипуляции радиосигналов: патент RU2510077C2. 2014. Бюл. № 8.
2. *Liu P., Zou L.* Apparatus and method for classifying modulations in multipath environments**:** patent No. US8385473B2, April 2010.
3. *Бакулин М.Г., Крейнделин В.В., Шлома А.М., Шумов А.П.* Технология OFDM: учебное пособие для вузов. – Горячая линия – Телеком. 2017. С. 352.
4. *Дам В.Н.* Автоматическое распознавание видов цифровой модуляции радиосигналов с помощью многослойной нейронной сети по кумулянтным признакам // Информационные технологии. 2016. № 7. Т. 22. С. 555–560.

УДК. 00.004

Процедуры оптимального голосования в многоэкспертных бинарных системах

Э.Д. Аведьян [1,2,3], Ле Тхи Чанг Линь [1]

[1]Московский физико-технический институт (государственный университет)
[2]Центр информационных технологий и систем органов исполнительной власти
[3]Международный центр по информатике и электронике

Потребность повышения точности решения задачи классификации привела к созданию систем, содержащих несколько алгоритмов решения задачи классификации и интегральный блок – блок анализа решений каждого алгоритма (эксперта), в задачу которого входит нахождение решения задачи с точностью, превышающей точность решения каждого из экспертов системы, например, в [1]. Идея интеграции решений отдельных экспертов нашла свое воплощение при создании систем обнаружения атак, см., например, обзорную статью [2] со списком из 75 цитированных работ.

В докладе представлены подходы к оптимизация многоэкспертных систем, основанных на принципах голосования как при равной, так и при различной вероятности обнаружения каждого статистически взаимно независимого и зависимого эксперта. Доклад состоит из следующих частей.

1. Многоэкспертная бинарная система голосования (БСГ) по большинству при равной условной вероятности обнаружения каждого статистически взаимно независимого эксперта.

2. Оптимальная многоэкспертная БСГ при равных и неравных значениях условных вероятностей принятия гипотезы H_0 и H_1 каждого статистически взаимно независимого эксперта.

3. Оптимальная многоэкспертная БСГ при неравных значениях условных вероятностей принятия гипотез H_0 и H_1 каждого статистически взаимно зависимого эксперта на основе метода статистических испытаний.

Для оптимизации многоэкспертной БСГ вводится функционал в виде линейной комбинации вычисляемых системой условных вероятностей правильного принятия гипотез БСГ, как, например, в [3].

Наиболее интересные выводы из проведенного исследования, подтвержденные результатами моделирования на ЭВМ.

1. Если условная вероятность правильного решения эксперта БСГ с независимыми равной квалификации экспертами $p(0/0) > 0.5$, то найдется такое число экспертов, что вероятности правильного решения многоэкспертной БСГ $p_{\text{эксп}}(0/0)$ окажется как угодно близкой к единице.

2. Если вероятность правильного решения эксперта $p(0/0) < 0.5$, то с увеличением числа экспертов результирующая вероятность правильного решения многоэкспертной БСГ $p_{expsys}(0/0)$ стремится к нулю.

3. Характеристики БСГ с четным и нечетным числом экспертов при небольшом числе экспертов значительно отличаются и сближаются только при большом количестве экспертов.

4. Основным параметром оптимизации БСГ является число голосов за ту или иную гипотезу, которое определяет вероятности правильного оптимального принятия гипотезы.

5. В случае, когда в БСГ имеются статистически зависимые эксперты разной квалификации, оптимизация выполняется на основе метода статистических испытаний.

Литература

1. *Xu L., Amari Shun-Ichi.* Combining classifiers and learning mixture-of-experts // Encyclopedia of Artificial Intelligence (3 volumes). Eds. Dopico J.R.R., Dorado J., Pazos A., IGI Global publishing company. 2009. P. 319–326.
2. *Aburomman A.A., Reaz M.B.I.* A survey of intrusion detection systems based on ensemble and hybrid classifiers // Computers & Security. 2016. http://dx.doi.org/doi: 10.1016/j.cose.2016.11.004.
3. *Аведьян Э. Д., Ле Т.Ч.Л.* Двухуровневая система обнаружения DoS-атак и их компонентов на основе нейронных сетей CMAC // Информационные технологии. Т. 29. 2016. № 9. С. 711–718.

УДК 51-77

Альтруистические стратегии при голосовании в стохастической среде

В.А. Малышев

Московский физико-технический институт (государственный университет)
Институт проблем управления им. Трапезникова РАН

В работе с помощью математической модели социальной динамики, определяемой голосованием в стохастической среде (модель ViSE) [1], исследуется парадокс «ямы ущерба», заключающийся в том, что серия демократических решений может систематически приводить общество к состояниям, неприемлемым для всех голосующих. Анализируется возможность обойти парадокс с помощью альтруситической (т.е. исходящей не из интересов своих членов, а всего общества в целом) группы, способной регулировать свой порог принятия предложений и голосующей солидарно. Получены формулы, описывающие социальную динамику в случае наличия классической альтруистической группы, либо альтруистической группы с порогом принятия предложений, голосующей солидарно, и эгоистов.

Рассмотрим модель голосования в стохастической среде [1] в случае, когда общество состоит из n участников, среди которых l – эгоисты, а $a = n - l$ – члены альтруистической группы. Пусть $\alpha \in [0, 1]$ – строгий порог голосования, т.е. число, превышение которого долей общества, проголосовавшей «за», необходимо и достаточно для принятия предложения; $\delta = l/n$ – доля эгоистов.

Каждый участник характеризуется текущим значением капитала. Предложение есть вектор приращений капиталов участников. Эгоист голосует за те и только те предложения, которые увеличивают его капитал. Солидарно голосующая альтруистическая группа поддерживает предложения, которые выгодны в определенном смысле для всего общества и отвергает иные. Выгодными для общества можно считать предложения, в которых либо а) среднее приращение капитала участников превышает определенный порог притязаний t (который не обязательно положителен) либо б) доля членов общества, получающих положительные приращения капитала, превышает заданный порог принятия предложения альтруистической группой, ψ (такая стратегия имеет смысл, когда этот порог отличается от порога голосования α). Предложение рассматривается в модели как реализация вектора

независимых одинаково распределенных случайных величин, в простейшем случае, – нормальных с параметрами μ (среднее) и σ (среднеквадратическое отклонение).

Сначала аналитически было найдено математическое ожидание приращений капиталов эгоистов и членов альтруистической группы обоих типов. Затем было замечено, что альтруистическая группа типа б) может выбрать такой порог (назовем его оптимальным), при котором среднее приращение капитала участника максимально.

Результаты выражены через математическое ожидание голосующей нормальной выборки объема l с параметрами (μ, σ) [2].

Для обоих типов альтруистических стратегий характерно наличие интересного эффекта в некоторых средах, когда отказ всей альтруистической группы от своей стратегии в пользу эгоизма (ввиду того, что их среднее приращение капитала ниже, чем у эгоистов) приводит к ухудшению их положения (рис. 1).

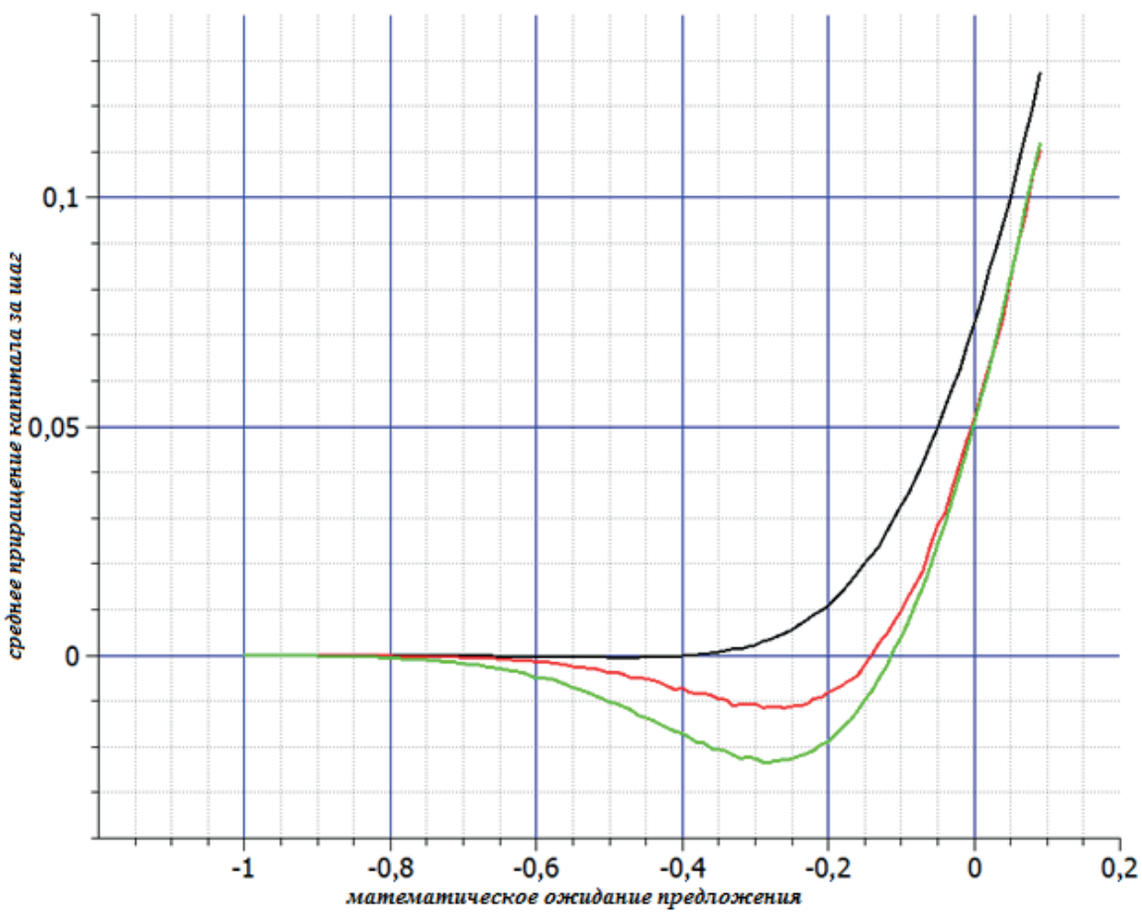


Рис. 1. Средние приращения капиталов эгоиста при наличии альтруистов (верхний график, 25 человек), альтруиста при наличии эгоистов (средний график, 5 человек) и эгоиста без альтруистов (нижний график, 30 человек) за 1 шаг: σ = 1, α = 0,45

Литература

1. *Чеботарев П.Ю.* [*и др.*] Модель социальной динамики, управляемой коллективными решениями // Российская Академия наук, Институт проблем управления, Труды Института. Т. XXIII. – М., 2004. С.102–109.
2. *Чеботарев П.Ю.* Аналитическое выражение ожидаемых значений капиталов при голосовании в стохастической среде // Автоматика и телемеханика. 2006. № 3. С. 152–165.

УДК 519.718.2:004.052.2

Расчет двоичных кодов сетей связи

К.А. Батенков

Академия ФСО России

Описание структур сети связи на основе диаграмм графов является достаточно удобным, однако имеет серьезный недостаток, связанный с существенными требованиями при их хранении на память запоминающих устройств [1], [2]. Именно поэтому поиск инвариантов, способных, по сути, сжимать информацию о структуре сети, оказывается весьма востребованным [3]. Одними из них являются мини-код и макси-код соответствующих графов, вычисление которых (кодов) можно производить на основе метода, рассмотренного в данной работе [4].

Ввиду симметричности матрицы смежности $\mathbf{A}$ (в случае неориентированных графов) для ее задания достаточно выписать в определенном порядке лишь те элементы, которые расположены над главной диагональю, т.е. на основе матрицы смежностей $\mathbf{A}$ задать *вектор смежностей* $\mathbf{a}$: $\mathbf{A} \to \mathbf{a}$:

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,v} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,v} \\ \vdots & \vdots & \ddots & \vdots \\ a_{v,1} & a_{v,2} & \cdots & a_{v,v} \end{bmatrix} \to \mathbf{a} = \left[a_{1,2}, a_{1,3}, \dots, a_{1,v}, a_{2,3}, a_{2,4}, \dots, a_{2,v}, \dots, a_{v-1,v}\right]^{\mathrm{T}}.$$

Длина вектора равна $C_v^2 = \frac{v!}{(v-2)!2!}$, где C_i^j – число сочетаний из j по i. Заметим, что данный порядок записи элементов матрицы смежностей несколько отличается от порядка, используемого в [5]. Это связано, во-первых, с произвольностью выбора элементов над главной диагональю, а, во-вторых, как будет показано ниже, подобный порядок позволяет проще формировать коды графов.

Кроме того, согласно теореме Эйлера, число ребер можно рассчитать исходя из вектора смежностей $l = \mathbf{a}^{\mathrm{T}}\mathbf{1}_{C_v^2}$.

Представление бинарного вектора смежностей $\mathbf{a}$ в десятичной форме позволяет сформировать *двоичный код* матрицы $\mathbf{A}$:

$$\mu'(\mathbf{A}) = a_{1,2}2^{C_v^2-1} + a_{1,3}2^{C_v^2-2} + \cdots + a_{1,v}2^{C_v^2-v} + a_{2,3}2^{C_v^2-v+1} +$$
$$+a_{2,4}2^{C_v^2-v+2} + \cdots + a_{2,v}2^{C_v^2-2v-1} + \cdots + a_{v-1,v}2^0 = \sum_{i=1}^{v-1}\sum_{j=i+1}^{v} a_{i,j}2^{\frac{(i-v-1)(i-v)}{2}+k-j+1}.$$

Таким образом, двоичный код μ матрицы $\mathbf{A}$ представляет собой запись, в которой количество единиц равно $a_{v-1,v}$, количество двоек $a_{v-2,v}$, количество четверок $a_{v-2,v-1}$ и т. д. Двоичные коды матриц смежностей одного и того же графа, отвечающих разным нумерациям его вершин, различны, поэтому определяют двоичный код матрицы, но не графа.

Наименьший из этих кодов (при всевозможных $v!$ нумерациях) называют *мини-кодом* $\dot{\mu}(G)$, а наибольший – *макси-кодом* $\mu(G)$ графа G. Оба эти кода очевидно инварианты и, более того, по любому из них и количеству вершин легко восстанавливается одна из матриц смежностей графа, а значит, и сам граф с точностью до изоморфизма. Следует заметить, что формирование мини-кода $\dot{\mu}$ и макси-кода μ графа G упрощается, если пронумеровать вершины в порядке невозрастания или неубывания, т.е. использовать вектор степеней $\mathbf{v}$ или обращенный вектор степеней $\mathbf{v}'$ соответственно. Алгоритм расчета мини-кода $\dot{\mu}$ можно представить следующим образом. Первоначально формируется вектор размера $\left((v-1)\times 1\right)$, соответствующий первой строке элементов матрицы смежностей над главной диагональю (первому столбцу под главной диагональю) $\mathbf{a}_1 = \left[a_{1,2}, a_{1,3}, \dots, a_{1,v}\right]^{\mathrm{T}}$ согласно условию

$$\mathbf{a}_1 = \left\{ \mathbf{a}_1 : \mathbf{a}_1 = \arg\min_{\mathbf{a}_1} \left(\sum_{j=2}^{v} a_{1,j} 2^{v-j} \right), [\mathbf{v}]_1 = [\mathbf{v}_1]_1, \mathbf{v}_1 \le \mathbf{v}, \right\}, \quad (1)$$

где вектор степеней имеет форму $\mathbf{v}_1 = \mathbf{A}_1 \mathbf{1}_v$, а матрица смежностей заполнена только вектором $\mathbf{a}_1$ (все остальные ее элементы равны нулю):

$$\mathbf{A}_1 = \begin{bmatrix} 0 & \mathbf{a}_1^{\mathrm{T}} \\ \mathbf{a}_1 & \mathbf{0} \end{bmatrix}.$$

Далее последовательно находятся все векторы $\mathbf{a}_i$ размером $\big((v-i)\times 1\big)$:

$$\mathbf{a}_i = \left[a_{1,i+1}, a_{1,i+1}, \dots, a_{1,v} \right]^{\mathrm{T}}, i = 2, 3, \dots, v-1,$$

согласно условию

$$\mathbf{a}_i = \left\{ \mathbf{a}_i : \mathbf{a}_i = \arg\min_{\mathbf{a}_i} \left(\sum_{j=i+1}^{v} a_{i,j} 2^{v-j} \right), [\mathbf{v}]_i = [\mathbf{v}_i]_i, \mathbf{v}_i \le \mathbf{v}, \right\}, \quad (2)$$

где вектор степеней имеет форму

$$\mathbf{v}_i = \mathbf{A}_i \mathbf{1}_v,$$

а матрица смежностей заполнена только векторами от $\mathbf{a}_1$ до $\mathbf{a}_i$ включительно (все остальные ее элементы равны нулю)

$$\mathbf{A}_i = \begin{bmatrix} 0 & & & \mathbf{a}_1^T & \\ & 0 & & \mathbf{a}_2^T & \\ & & 0 & \ddots & \\ \mathbf{a}_1 & \mathbf{a}_2 & \ddots & 0 & \mathbf{a}_i^T \\ & & & \mathbf{a}_i & \mathbf{0} \end{bmatrix}.$$

В результате формируется матрица смежностей $\mathbf{A}_{v-1}$, соответствующая мини-коду μ̇ исходного графа.

Для определения макси-кода μ следует использовать ту же последовательность вычислений, за исключением того, что в условиях (1) и (2) требуется вместо вектора степеней $\mathbf{v}$ использовать его обращение $\mathbf{v}'$ и поменять минимизацию на максимизацию, т. е. использовать равенство

$$\mathbf{a}_i = \arg\max_{\mathbf{a}_i} \left(\sum_{j=i+1}^{v} a_{i,j} 2^{v-j} \right), i = 1, 2, \dots, v-1.$$

Количество вершин можно не сообщать, если заранее известно, что у графа нет изолированных вершин. При задании же графа его макси-кодом ясно, что если последний отличен от нуля, то он точно содержит единицу старшего разряда $2^{\mathrm{C}_{\mathrm{v}}^2-1}$, т.е. отвечает такой нумерации вершин графа, при которой пара $\big((v-1), v\big)$ является ребром, в силу чего число вершин v однозначно определяется из условия $C_v^2 - 1 = \lceil \log_2 \mu \rceil$, где $\lceil x \rceil$ – округление в большую сторону до ближайшего целого числа x. Отсюда $v = \frac{1}{2} + \sqrt{2\lceil \log_2 \mu \rceil + \frac{1}{4}}$.

Следует отметить, что лишь в случае $\mu = 0$, т.е. когда рассматривается безреберный граф, число v его вершин может быть любым.

Литература

1. *Батенков К. А.* Об анализе живучести сетей связи на основе вероятностного подхода // Неделя науки СПбПУ Материалы научной конференции с международным участием. Институт физики, нанотехнологий и телекоммуникаций. 2016. С. 6–8.
2. *Батенков К. А.* К вопросу оценки надежности двухполюсных и многополюсных сетей связи // Современные проблемы радиоэлектроники : сб. науч. тр. [Электронный ресурс] / науч. ред. А. И. Громыко ; отв. за вып. А. А. Левицкий. Электрон. дан. (31,5 Мб). Красноярск : Сиб. федер. ун-т, 2017. С. 604–608.
3. *Батенков К. А.* Общие подходы к анализу и синтезу структур сетей связи // Современные проблемы телекоммуникаций : Материалы Российской научно-технической конференции. 2017. С. 19–23.

4. *Батенков К. А.* Числовые характеристики структур сетей связи // Труды СПИИРАН. 2017. № 4 (53). С. 5–28.
5. *Зыков А. А.* Основы теории графов. М.: Наука, Гл. ред. физ.-мат. лит., 1987. 384 с.

УДК 621.396

Разнесенный прием в условиях многолучевого распространения для OFDM-модулированных сигналов

В.А. Иртюга, М.Г. Столяренко, К.С. Митягин

Московский физико-технический институт (государственный университет)

Основным требованием, предъявляемым к современным цифровым системам связи, является высокая скорость и надежность передачи информации в условиях сложной помеховой обстановки. При проектировании цифровых систем связи широкое применение получила техника ортогонального частотного разделения каналов (orthogonal frequency division multiplexing, OFDM), которая обеспечивает высокую спектральную эффективность и помехоустойчивость при передаче радиосигналов в мобильных каналах с многолучевым распространением [1]. Технология OFDM-модуляции успешно применяется в современных системах цифрового телерадиовещания (DVB-T2, ATSC 3.0, DAB, РАВИС), утверждена в стандартах беспроводных локальных сетей (Wi-Fi, WiMax) и широкополосной мобильной связи (LTE).

Канал передачи для мобильной беспроводной связи характеризуется наличием нестационарных замираний, обусловленных явлением многолучевого распространения радиосигналов, наличие которых затрудняет процесс демодуляции сигнала [2]. Схема разнесенного приема используется для достижения максимальной достоверности и надежности работы канального декодера в приемном устройстве [3]. Основная идея данного подхода заключается в том, что решения о передаваемых информационных символах данных принимаются на основе рассмотрения нескольких сигналов с приемных антенн, разнесенных в пространстве и имеющих вследствие этого различный характер замираний.

Целью данного исследования является оценка потенциального выигрыша в использовании схемы пространственного разнесенного приема в условиях многолучевого распространения для OFDM-модулированных сигналов. Анализ эффективности проводился с помощью имитационного моделирования с применением разработанной программной модели цифровой системы наземного мультимедийного вещания РАВИС [4]. Для сравнительного анализа были выбраны и реализованы следующие методы демодуляции сигнала: метод сочетания максимального отношения (maximal ratio combining) и метод селективного выбора (selection diversity) [3].

Результаты имитационного моделирования показали, что метод сочетания максимального отношения демонстрирует наибольшую эффективность работы при разнесенном пространственном приеме. Энергетический выигрыш составляет около 3–4 дБ для различных моделей многолучевых каналов.

Проведенный анализ показал, что метод сочетания максимального отношения позволяет существенно повысить эффективность цифровой демодуляции OFDM-сигналов и снизить вероятность возникновения битовой ошибки при передаче в мобильных каналах связи.

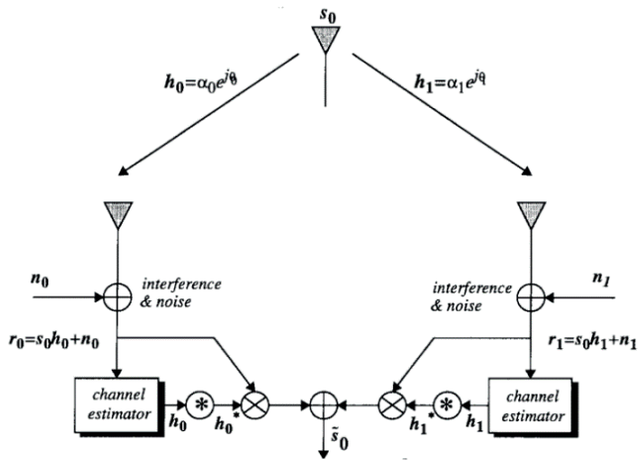


Рис. 1. Схема разнесенного пространственного приема. Используются следующие обозначения: *h*0, *h*1-характеристики каналов передачи; *s*0 – передаваемый информационный символ; *r*0, *r*1 – принятые информационные символы; *n*0, *n*1 – искажения аддитивного гауссовского шума

Литература

1. *Nee R., Prasad R*. OFDM for wireless multimedia communications. Artech House, Inc., 2000.
2. *Cho Y. S*. MIMO-OFDM wireless communications with MATLAB. John Wiley & Sons, 2010.
3. *Скляр Б*. Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом «Вильямс», 2004.
4. *ГОСТ Р 54309-2011*. Аудиовизуальная информационная система реального времени (РАВИС). Процессы формирования кадровой структуры, канального кодирования и модуляции для системы цифрового наземного узкополосного радиовещания в ОВЧ диапазоне. Технические условия.

УДК 00.004

Оптимизация нейросетевой многоэкспертной системы обнаружения атак на современной базе данных UNSW-NB15

Ле Тхи Чанг Линь

Московский физико-технический институт (государственный университет)

В настоящее время экспертные системы используются во многих областях (медицина, вычислительная техника, геология, математика, сельское хозяйство, управление, электроника, юриспруденция). Они также применяются в качестве систем обнаружения атак, описание таких систем можно найти во многих работах [1–5].

В докладе приводятся результаты применения многоэкспертной системы для распознавания типа компьютерной атаки на основе набора многослойных нейронных сетей (МНС), моделированных в среде Matlab Neural Network Toolbox. Каждая нейронная сеть выступает в роли эксперта многоэкспертной системы. Система состоит из трех МНС, каждая нейронная сеть использует разное число нейронов и обучается методом Levenberg – Marquardt. Режим обучения offline, максимальное число эпох обучения 1000. Для обучения и тестирования этой системы используется современная база данных UNSW-NB15 [6], [7]. После удаления повторов 80% случайно выбранных данных используются для обучения и 20% для тестирования, обучающие данные случайно разделены на 3 равные части.

В данной нейросетевой многоэкспертной системе, предназначенной для обнаружения атаки типа Reconnaisanse, используется принципы голосования по большинству и оптимальные принципы голосования. В случае применения принципы голосования по большинству система сообщает об обнаружении атаки, если два или три эксперта сообщают, что происходит атака. Если же два или три эксперта сообщают, что

имеет место нормальное соединение, то система сообщает, что атака отсутствует, имеет место нормальное соединение. При таком подходе распознается 81,25% Reconnaisanse-атак и 96,78% случаев отсутствия атак.

Оптимизация многоэкспертной системы голосования выполнена путем изменения принципа голосования следующим образом: если три эксперта показывают, что имеет место нормальное соединение, то система сообщает об отсутствии атаки Reconnaisanse, в остальных случаях система сообщает об обнаружении атаки. Результат для такой системы: распознается 93,05% атак и 91,98% случаев отсутствия атак.

Таким образом, после оптимизации многоэксперной системы голосования процент обнаружения атак повысился на 11,8%, причем процент обнаружения нормальных соединений уменьшился на 4,8%. В системах, для которых приоритетным является обнаружение атак, оптимизированная система является наилучшей.

Литература

1. *Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang.* A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering // Expert Systems with Applications 37. 2010. P. 6225 – 6232.
2. *Kesavulu Reddy E.* Expert system for intrusion detection and its application // International conference on innovative applications in engineering and information technology, ICIAEIT. 2017. P.61–65.
3. *Sodiya A.S., Ojesanmi O.A., Akinola O.C.* Neural network based intrusion detection systems. International Journal of computer applications, 2014. P. 19–24.
4. *Anderson, D., Frivold, T. & Valdes, A.*. Next-generation Intrusion Detection Expert System (NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07(May, 1995).
5. *H. Debar, M. Becker, D. Siboni.* A Neural network component for an intrusion detection system // Proceedings of the 1992 IEEE Symposium on Security and privacy. P. 240.
6. https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys?path=%2F
7. *Ле Т.Ч.Л.* Обнаружение атак в современной базе данных UNSW-NB15 с применением многослойной нейронной сети // Информатизация и связь. 2017. № 1. С. 61 – 66.

УДК 004.627

Применение вейвлет-преобразований в сжатии изображений.

П.А. Кононюк

Московский физико-технический институт (государственный университет)

В современном мире возрастают объемы передачи данных, а значит, требуются большие степени сжатия. Нужны более эффективные алгоритмы работы с данными, в том числе с изображениями и видео. Вейвлет-преобразования отвечают этим требованиям, совмещая высокую скорость работы и степень сжатия [1].

Рассматриваются основные преимущества вейвлет-преобразования над преобразованием Фурье для непрерывного и дискретного случая.

Приведены примеры воздействия вейвлет-преобразования на изображения и показана высокая эффективность сжатия с его помощью [3].

Показаны примеры стандартов, использующих вейвлет-преобразование в сжатии изображений.

Приведен алгоритм составления цифровых банков фильтров для вейвлетов первого и второго поколения с необходимыми свойствами [2], [5].

Показан принцип факторизации произвольного банка фильтров с условием идеального восстановления, в том числе для случая количества фильтров более двух [4], [5].

Приведены преимущества и принципы построения банков фильтров на основе вейвлетов второго поколения.

Показаны дальнейшие возможные пути улучшения сжатия изображений, в том числе рассмотрены случаи неидеального восстановления.

Автором работы приведены примеры факторизации банков фильтров в лифтинг-схему, которая в дальнейшем будет использоваться в вейвлет-кодеке реального времени, разрабатываемом в лаборатории мультимедийных систем и технологий МФТИ.

Также данный материал будет в дальнейшем использоваться для лабораторных работ в курсе систем связи кафедры мультимедийных систем и технологий ФРТК.

Литература

1. *Штарк Г.* Применение Вейвлетов для ЦОС. М.: Техносфера, 2007.
2. *Дворкович В.П., Дворкович А.В.* Цифровые видеоинформационные системы. М.: Техносфера, 2016.
3. *Сэломон Д.* Сжатие данных, изображений и звука. М.: Техносфера, 2004.
4. *Daubechies I., Wim Sweldens.* Factoring Wavelet transform into lifting steps, 1996.
5. *Ying-Jui Chen, Amaratunga K.S.* M-channel lifting factorization of perfect reconstruction filter banks and reversible M-band wavelet transforms// IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing. 2003.

УДК 621.396.13

Разработка и исследование специального символа идентификации и синхронизации для системы «РАВИС»

Я.И. Львович

Московский физико-технический институт (государственный университет)

В связи с тем, что в настоящий момент времени осуществляется переход на цифровое вещание, возникает множество проблем, связанных с особенностями передачи данных в радиоканале. Одна из главных проблем – проблема синхронизации. По этой причине вводится система наземного мультимедийного вещания реального времени «РАВИС» [1].

Система РАВИС включает в себя полный тракт передачи цифрового вещания [2]. Однако в работе будет рассматриваться только блок синхронизации. На данный момент в системе РАВИС реализована обычная OFDM синхронизация. Показано, что специальный символ идентификации и синхронизации, взятый из стандарта DVB-T2, обеспечивает более эффективную синхронизацию, при этом затрачивает меньше ресурсов.

В настоящее время мультиплексирование с ортогональным частотным разделением каналов (OFDM) является схемой модуляции, широко используемой для различных типов цифровой передачи, например, для наземного цифрового вещания и в стандарте IEEE 802.11a. Применение OFDM делает особенно эффективным использование частот путем мультиплексирования с частотным разделением множества узкополосных модулированных в цифре сигналов, используя взаимно-ортогональные поднесущие.

Более того, в OFDM-модуляции один символ содержит как полезный интервал, так и защитный интервал. По существу, защитный интервал является копией завершающей части полезного интервала, вставляемой перед полезным интервалом (циклический префикс). Таким образом, уменьшается влияние межсимвольной интерференции, вызванной многолучевым распространением.

Аналоговое телевизионное вещание прекращается по всему миру. В Европе растет потребность в вещательных службах телевидения HD (Высокой четкости) в дополнение к вещательным службам телевидения SD (Стандартной четкости), использующим доступный в настоящее время стандарт DVB-T (Наземное цифровое телевидение) [3]. Соответственно продвинулась стандартизация системы цифрового наземного телевизионного вещания второго поколения DVB-T2 [4]. Исходя из стандарта системы цифрового наземного телевизионного вещания второго поколения, модель блока синхронизации системы РАВИС может быть доработана с использованием новаций стандарта DVB-T2.

Система РАВИС предназначена для вещания в I–II полосах ОВЧ диапазона частот, в частности, для обеспечения радиовещания на мобильные устройства на территории

России в диапазонах частот 65,8-74 МГц и 87,5-108 МГц при сохранении частотных распределений. Выбранный диапазон частот, используемый для вещания РАВИС, позволяет на одной и той же частоте в разных городах передавать различные программы. При этом радиус покрытия передатчиком является достаточным для обеспечения приёма в отдалённых населённых пунктах, где другим способом осуществить вещание невозможно.

Символ P1 передает пять бит в закодированном виде. Первые два бита от [0 0] до [1 1] образуют набор S1, а остальные три бита образуют набор S2. Так как набор S1 расположится на 16 несущих частотах, набор S2 на 64, но набор S1 будет продублирован, поэтому всего понадобится 96 несущих. Таким образом, существует всего 32 возможные комбинации с длиной 96. Автокорреляционной функцией этих несущих является дельта-функция с коэффициентом 96, в то время как кросс-корреляция остальных несущих всегда равна нулю. Эти несущие частоты будут промодулированы и расположены на частотном отрезке, равном полосе OFDM символа. Полученный сигнал в частотной области преобразуется в его эквивалент во временной области:

$$p_A(i) = \frac{\sum_{n=0}^{1023} Xp(n) e^{j2\pi \frac{ni}{1024}}}{\sqrt{96}}, i = [0 \sim 1023]. \quad (1)$$

Во временной области символ P1 имеет длину в 2048 отсчетов, так как помимо центральной части p_A с длинной $T_A = 1024$, имеются две частотно-смещенные копии каждой из половин центральной части с длинами $T_C = 542$ и $T_B = 482$.

Таким образом, символ P1 во временной области можно представить в виде:

$$p(i) = \begin{cases} p_C(i) & i \in [1 \sim T_c] \\ p_A(i) & i \in [(T_c + 1) \sim (T_C + T_A)] \\ p_B(i) & i \in [(T_c + T_A + 1) \sim (T_C + T_A + T_B)] \end{cases} \quad (2)$$

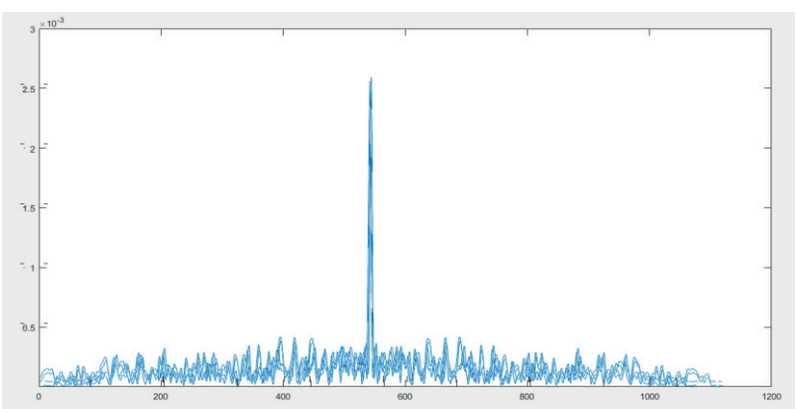


Рис. 1. Результат перемножения частей C и B символа P1

Как видно из рис. 1, для 16 наборов максимумы перемножения корреляций расположены строго посередине. Следовательно, можно сделать вывод, что для всех 32 наборов максимумы перемножения корреляций будут расположены также строго посередине.

Проверка распределения несущих производится с помощью функции корреляции между полученным распределением и априорно известным. По смещению номера максимума мы можем судить о смещении частоты.

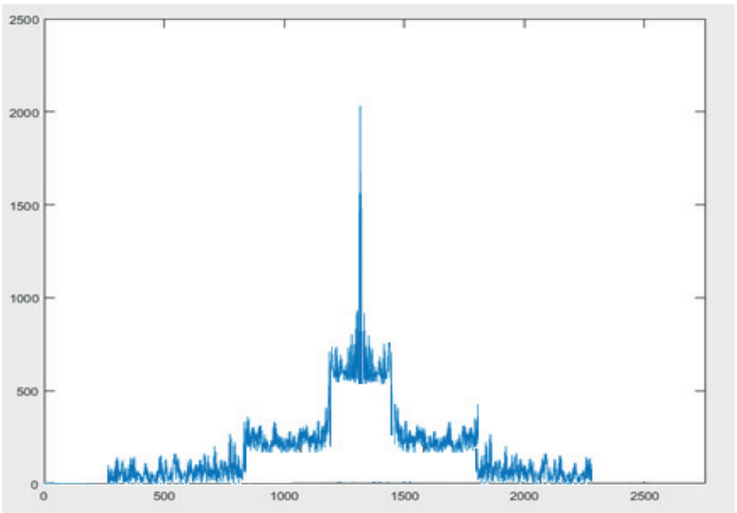


Рис. 2. Корреляция между заданным и полученным распределением

Литература

1. *Дворкович А.В., Дворкович В.П., Зубарев Ю.Б, Соколов А.Ю., Чернов Ю.А.* Способ трансляции информационного телевидения: патент РФ № 2219676, 08.11.2000.
2. ГОСТ Р 54309–2011. Аудиовизуальная информационная система реального времени (РАВИС). Процессы формирования кадровой структуры, канального кодирования и модуляции для системы цифрового наземного узкополосного радиовещания в ОВЧ-диапазоне. Технические условия.
3. ETSI EN 302 755 V. 1.1.1: Digital Video Broadcasting (DVB); Frame structure, channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2), June 2008.
4. DVB Document A133: Implementation Guidelines for a Second Generation Digital Terrestrial Television Broadcasting System (DVB-T2), Feb. 2009, www.dvb.org.

УДК 519.872.7

Управление передачей данных по флуктуирующему каналу связи при неточной информации о его состоянии

***Д.В. Мясников*[3], *К.В. Семенихин*[1,2,3]**

[1]Московский авиационный институт (национальный исследовательский университет)
[2]Московский физико-технический институт (государственный университет)
[3]Институт радиоэлектроники им. В.А. Котельникова РАН

Для многих сетей передачи данных актуальна проблема неполноты информации о состоянии отдельных узлов. Например, непосредственному измерению могут быть доступны лишь времена кругового обращения сегментов данных или сообщения об их потере [1, 2]. Такая ситуация особенно отчетливо проявляется для систем связи, установленных на транспортных средствах, работающих в автоматическом режиме. С одной стороны, для подобных систем необходимо периодически передавать телеметрию, а с другой – учитывать ограничения, возникающие из-за использования автономных источников питания [3, 4]. Указанные приложения делают весьма востребованными исследования в области оптимального стохастического управления инфокоммуникационными системами по неточной измерительной информации. Для этих задач предлагается применить подход, сочетающий в себе фильтрацию вектора состояния сети и оптимизацию ее контролируемых параметров с использованием онлайн вычисляемой оценки ненаблюдаемого состояния.

Рассматриваемая инфокоммуникационная система описывается моделью одноканальной системы массового обслуживания, на вход которой подается нестационарный пуассоновский поток заявок. Каждая заявка представляет собой пакет

(унифицированный блок данных), подлежащий дальнейшей передаче по каналу связи. Пара «число заявок»–«состояние канала» описывается марковским процессом с заданными интенсивностями переходов. Однако состояние канала связи (в отличие от количества заявок) в текущий момент времени неизвестно. Косвенная измерительная информация о состоянии канала содержится в потоке сообщений об успешной доставке пакетов. Интенсивность обслуживания предполагается пропорциональной уровню загрузки канала с коэффициентом, зависящим от состояния канала. Скорость передачи данных является контролируемым параметром, который требуется выбрать из условия минимума среднего числа потерянных пакетов с учетом ограничения на энергетические ресурсы передатчика на фиксированном промежутке времени. Потери пакетов происходят при переполнении очереди, а энергозатраты считаются пропорциональными уровню загрузки канала. Для оптимизации стратегий передачи данных на классе управлений с обратной связью предлагается использовать подход, сочетающий в себе три основных метода:

- метод оптимальной фильтрации скрытого марковского состояния по считающим наблюдениям [1];
- синтез оптимального управления по полной информации в стохастической системе, описываемой марковским процессом с конечным множеством состояний [5];
- метод стохастической оптимизации [6] с использованием специально смоделированных наблюдений.

Разработанная стратегия управления загрузкой определяется текущим значением числа заявок и оценкой фильтрации состояния канала относительно имеющегося потока измерений. Качество разработанной стратегии было проанализировано посредством ее сравнение с двумя другими стратегиями, первая из которых является оптимальным управлением по полной информации, а вторая представляет собой результат осреднения первой по априорному распределению состояния канала. Разработанное управление продемонстрировало лишь небольшой проигрыш оптимальной стратегии, использующей точную информацию о состоянии канала. Вместе с тем, управление, основанное лишь на априорных данных о канале связи, приводит к большому количеству потерь пакетов и заметному перерасходу энергии передатчика. Полученные результаты свидетельствуют о том, что разработанный метод управления загрузкой флуктуирующего канала связи может быть использован на практике для разработки новых транспортных протоколов, предназначенных для передачи данных при отсутствии полной информации о состоянии инфокоммуникационной сети.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект №16-07-00677-а).

Литература

1. *Миллер Б.М. Авраченков К.Е., Степанян К.В., Миллер Г.Б.* Задача оптимального стохастического управления потоком данных по неполной информации // Проблемы передачи информации. 2005. Т. 41, № 2. С. 89–110.
2. *Rieder U., Winter J.* Optimal control of Markovian jump processes with partial information and applications to a parallel queueing model // Math. Meth. Oper. Res. 2009. V. 70. P. 567–596.
3. *Choi D.H., Kim S.H., Sung D.K.* Energy-Efficient Maneuvering and Communication of a Single UAV-Based Relay // IEEE Trans. Aerosp. Electron. Syst. 2014. V. 50, N. 3. P. 2319–2326.
4. *Кузнецов Н.А., Мясников Д.В., Семенихин К.В.* Оптимизация двухфазной системы массового обслуживания и ее применение к управлению передачей данных между двумя агентами робототехнической системы // Информационные процессы. 2017. Т. 17, № 1. С. 19–42.
5. *Мясников Д.В., Семенихин К.В.* Управление параметрами одноканальной системы массового обслуживания при наличии ограничений // Известия РАН. Теория и системы управления. 2016. № 1. С.66–85.
6. *Граничин О.Н., Поляк Б.Т.* Рандомизированные алгоритмы оценивания и оптимизации при почти произвольных помехах. М.: Наука, 2003.

УДК 004

Современные системы промышленного беспроводного Интернета

В.Ф. Петухов

Московский физико-технический институт (государственный университет)

В современном мире всё чаще говорят о наступлении «четвёртой индустриальной революции». Её особенность заключается в переводе компаний и предприятий из состояния «чёрных ящиков», в которых связь между процессами работы, контроля и производства осуществляется с помощью персонала, в элементы открытых экосистем, которые взаимодействуют между собой с помощью единого сервера или облака, способного производить сколь угодно сложные вычисления. Данный переход к использованию Промышленного Интернета вещей сопровождается развитием и стандартизацией новых технологий. Одной из главных особенностей такого перехода является адаптация систем связи для межмашинного взаимодействия: абонентами сетей будут являться устройства, а не люди, причем их количество уже сегодня приближается к 1 миллиарду и продолжает экспоненциально расти. [3]

Приведена подробная информация о переходе от АСУ ТП к Промышленному Интернету.

Рассматриваются основные технологии, применяемые в Интернете вещей.

Приведена характеристика основных типов сетей и их реализаций, применяемых в Промышленном Интернете. Рассмотрены следующие типы сетей: персональные (PAN) [4]; локальные сети (LAN); городские сети (MAN), применяемые для реализации территориально-распределенных сетей с низким энергопотреблением (LPWAN) [2]; сети с глобальным покрытием (WAN). Среди множества реализаций каждого типа сети для описания выбраны наиболее популярные на данный момент.

Проведён сравнительный анализ технологий – лидеров мирового рынка LPWAN-сетей: LoRa (США), SigFox (Франция), «Стриж» (Россия). [5]

Описаны современные проблемы в развитии Промышленного Интернета, а также пути решения данных проблем [1].

В результате исследования были сформированы наборы требований для LPWAN-сетей, которым будет в лучшей степени соответствовать та или иная технология: для систем телеметрии с большим количеством (несколько тысяч) неподвижных датчиков лидерами являются SigFox и «Стриж»; в реализации систем мониторинга из нескольких сотен подвижных датчиков, либо систем управления, в которых необходим прямой канал передачи (например, система управления наружным освещением), лидирует LoRa.

Литература

1. Sadeghi A. R., Wachsmann C., Waidner M. Security and privacy challenges in industrial internet of things //Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015. P. 1–6.
2. Dujovne D. et al. 6TiSCH: deterministic IP-enabled industrial internet (of things) //IEEE Communications Magazine. 2014.V. 52. N. 12. P. 36–41.
3. Posada J. et al. Visual computing as a key enabling technology for industrie 4.0 and industrial internet //IEEE computer graphics and applications. 2015. V. 35. N. 2. P. 26–40.
4. Hossain M. S., Muhammad G. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring //Computer Networks. 2016. V. 101. P.192–202.
5. Adelantado F. et al. Understanding the limits of LoRaWAN //IEEE Communications Magazine. 2017. V. 55. N. 9. P. 34–40.

УДК 004.75

Об оптимальном размещении однотипных сетевых функций в распределенной операторской сети

Е.А. Свихнушина[1], А.А. Ларионов[2]

[1]Московский физико-технический институт (государственный университет)
[2]Институт проблем управления им. В.А. Трапезникова РАН

Рассмотрена задача об оптимальном размещении однотипных виртуальных функций в распределенной сети как задача минимизации общей стоимости итогового решения, учитывающая ограничения на пропускную способность, задержки каналов, производительность узлов и виртуальных функций. Виртуализация сетевых функций – это технология виртуализации физических сетевых элементов телекоммуникационной сети, когда сетевые функции исполняются программными модулями, работающими на стандартных серверах и виртуальных машинах в них. На практике при внедрении данной технологии операторы часто сталкиваются с задачей определения месторасположения виртуальных функций одного типа для предоставления пользователям базовых сервисов, таких как антивирус. Данная задача нетривиальна, так как зависит от многочисленных параметров, поэтому она представляет большой исследовательский интерес и рассматривается в данной работе. Схожие исследования производились в работах [1], [2], где рассматривалась задача о размещения виртуальных машин в рамках одного ЦОД, и [3], [4], [5], где также изучался вопрос о размещении виртуальных машин в распределенной сети, но с отличными от настоящей работы ограничениями.

Для постановки задачи предложена следующая математическая модель. Опорная инфраструктурная сеть представляется в виде простого неориентированного графа $G(V,E)$, где узлы V и ребра E соответствуют площадкам оператора и соединяющим их каналам связи. Суммарные ресурсы одной площадки выражаются через максимальное число виртуальных функций $\bar{m}_v$, которое в ней можно разместить. Каждая площадка характеризуется стоимостью ее аренды $c_v^{(0)}$ и ценой $c_v^{(1)}$ за размещение в ней одной виртуальной функции, то есть если на площадке v установлено m_v сетевых функций, то общая стоимость ее использования составит $c_v = c_v^{(0)} + m_v c_v^{(1)}$. Каждый канал связи между двумя площадками $(v,u) \in E$ характеризуется значением задержки δ_{vu}. Площадки, через которые пользователи получают доступ в сеть, называются граничными, а площадка, обеспечивающая выход в Интернет, называется стоком.

Виртуальные функции имеют ограничения на максимальное количество пользователей η, которое они могут обслужить, и максимальную пропускную способность β. Общее количество виртуальных функций для размещения в сети можно выразить как $M = \sum_V \bar{m}_v$.

S – множество пользователей. Пользовательский трафик характеризуется ограничением на максимальную задержку d_s и требуемую пропускную способность b_s.

Задача ставится как задача поиска минимума функционала:

$$f = \underset{F}{\operatorname{argmin}}\, c(f), \tag{1}$$

где F – множество всех функций $f: S \to V$, определяющих отображение между пользователями и узлами, $c(f) = \sum_V c_v$ – итоговая стоимость общего решения. Поиск решения должен производиться при учете ограничений на производительность узлов, виртуальных функций и условий на задержку.

В ходе работы было доказано, что рассматриваемая задача является NP-полной. С одной стороны, было показано, что задача входит в класс NP. С другой стороны, из нее можно выделить подзадачу, к которой полиномиально сводится известная NP-полная задача о рюкзаке. Следовательно, рассматриваемая задача является NP-полной [6].

Для получения точного решения задача была сформулирована в терминах целочисленного линейного программирования (ЦЛП). Независимые переменные задают отображение виртуальных функций на площадки и пользователей на виртуальные функции:

- $x_{kv} = 1$ тогда и только тогда, когда виртуальная функция k располагается на площадке v $\forall k = \overline{1, M},\ v = \overline{0, |V|}$.
- $y_{sk} = 1$ тогда и только тогда, когда пользователь s назначен виртуальной функции k $\forall s = \overline{1, |S|},\ k = \overline{1, M}$.

Введенные ограничения устанавливают правила корректного размещения виртуальных функций и подключения пользователей к ним. Должны соблюдаться ограничения на производительность площадок и виртуальных функций. Каждый пользователь должен быть подключен к одной функции при условии требований на пропускную способность и задержку.

Задача ЦЛП также ставится как задача поиска минимума итоговой стоимости:

$$c(x) = \sum_{v=0}^{|V|} (c_v^{(0)} u_v(x) + c_v^{(1)} \sum_{k=1}^{M} x_{kv}), \tag{2}$$

где u_v – зависимая переменная, показывающая, есть ли на площадке v хотя бы одна виртуальная функция.

Поскольку задача является NP-полной, был разработан эффективный жадный алгоритм для получения решений на больших топологиях. На первом шаге для каждого пользователя производится поиск узлов, удовлетворяющих ограничениям на задержку. Далее алгоритм итеративно подключает самых приоритетных пользователей с целью максимизации общей прибыли. Приоритет пользователя определяется по числу возможных узлов для подключения и разнице в стоимости между самым выгодным вариантом и последующим.

Для оценки качества предложенного эвристического алгоритма был проведен ряд экспериментов. В ходе их проведения многократно генерировалась случайная сеть, имеющая топологию типа «звезда». Варьируемыми параметрами выступали количество граничных узлов и связность между ними. Эвристический алгоритм был реализован на языке Python3, а задача ЦЛП была написана на языке MathProg и решалась с помощью пакета GLPK.

Для проверочных входных параметров, при которых задача оказывалась выпуклой и локальный и глобальный минимумы совпадали, решение задачи оптимизации и выполнение эвристического алгоритма давали идентичный результат, что обосновывало корректность алгоритма. Для более сложных топологий было установлено, что точные и эвристические результаты коррелированы, однако эвристические значения отличаются от точных в среднем на 15%. Поведение эвристического алгоритма для больших топологий оправдало ожидания: с увеличением связности графа значение общей стоимости падало, а время выполнения алгоритма возрастало. Однако порядок времени работы алгоритма находился в пределах секунды.

Литература

1. *Adamuthe A.C., Pandharpatte R.M., Thampi G.T.* Multiobjective virtual machine placement in cloud environment // IEEE International Conference on Cloud and Ubiquitous Computing and Emerging Technologies. 2013. P. 8–13.
2. *Shi W., Hong B.* Towards profitable virtual machine placement in the data center // IEEE Fourth International Conference on Utility and Cloud Computing. 2011. P. 138–145.
3. *Chen K.y., Xu Y., Xi K., Chao H.J.* Intelligent virtual machine placement for cost efficiency in geo-

distributed cloud systems // IEEE International Conference on Communications. 2013. P. 3498–3503.
4. *Jemaa F.B., Pujolle G., Pariente M.* QoS-Aware VNF Placement Optimization in Edge-Central Carrier Cloud Architecture // IEEE Global Communications Conference. 2016.
5. *Bouet M., Leguay J., Conan V.* Cost-based placement of vDPI functions in NFV infrastructures // IEEE First Conference on Network Softwarization. 2015.
6. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи / пер. с англ. М.: Мир, 1982. С. 85–88.

УДК 621.397, 621.391.837, 519.25

Вычисление функции оценки субъективного качества восприятия QoE мультимедийной информации

А.В. Ивченко

Московский физико-технический институт (государственный университет)

Анализ качества передаваемого и воспроизводимого мультимедийного контента – необходимое условие эффективного функционирования систем цифровой передачи информации. Оценка качества, базирующаяся на субъективном восприятии человека, называется качеством восприятия – QoE (Quality of Experience). В свою очередь на восприятие влияют объективные показатели, определяющие оценку, называемую качеством сервиса – QoS (Quality of Service). Тем не менее до сих пор нет единых методик оценки QoS и QoE.

Существующие системы в лучшем случае дают некоторую усреднённую оценку, которая не учитывает особенности конкретной мультимедийной системы и воспроизводимый контент. Другим недостатком является неуниверсальность методик – при отсутствии возможности анализа одного из предполагаемых методикой параметров системы оценка в принципе невозможна [2–5]. В данной работе предлагается универсальный метод оценки QoE на основе объективных параметров.

В работе приводится метод восстановления функции оценки QoE как функции многомерной нелинейной регрессии, а также приводится способ оценки перечня параметров с целью анализа их взаимной корреляции и его возможного уменьшения. Действительно, ещё одним узким местом методик является оценка достаточного перечня параметров для получения оценки заданной точности. Анализ параметров дополнительно позволяет уменьшить количество собираемой информации, тем самым упрощая методику.

Согласно результатам работы комиссии МСЭ 2004 года [1], в общем виде функция зависимости QoE выглядит следующим образом: $\mathrm{QoE} = b_1 / \left[1 + \exp\left(b_2\left(V - b_3\right)\right)\right]$, где $V = \sum_{i=1}^{n} w_i(W,P)\psi_i$, $W = \{w_i\}$, $i = 1, \ldots, n$, $P = \{p_j\}$, $j = 1, \ldots, k$, w_i – вычисляемые весовые коэффициенты, ψ_i – значения объективных показателей, p_j – характерные особенности контента, b_1, b_2, b_3 – масштабирующие коэффициенты, n – количество используемых показателей, k – количество особенностей. В качестве интегрального показателя V используются величины, полученные с помощью анализа различных наборов параметров, включая как простые (такие как размер экрана или процент потерь пакетов сети), так и сложные (количество движения в кадре или доля блочных искажений) [6-7].

Перед нами стоит задача многомерной нелинейной регрессии. Решение может быть сведено к последовательности решения линейных задач. В данном случае предлагается применение алгоритма Backfitting [8]. На первом шаге находится начальное приближение в виде констант, близкое к взвешенному среднему коэффициентов каждой функции показателей, далее итерационно все значения рассматриваются как известные с предыдущего шага константы, кроме одного, которое рассматривается как некоторая неизвестная нелинейная функция. На каждом шаге выбранная случайным образом функция подстраивается до тех пор, пока весь набор функций не стабилизируется.

Алгоритм Backfitting

Вход: матрица F «объекты-признаки» и вектор ответов y.

Выход: $\varphi_j(x)$ – функции преобразования признаков, в общем случае нелинейные.
Алгоритм на псевдокоде:

1. Берётся нулевое приближение a, как решение задачи многомерной линейной регрессии с признаками $f_j(x)$;

   $\varphi_j(x) = a_j f_j(x), j = 1, \ldots, n$;
2. **повторять**
3. **для** $j = 1,\ldots,n$
4. $z_i = y_i - \sum_{k=1,k\neq j}^{n} \varphi_k(f_k(x_i)), i = 1,...,l;$
5. $\varphi_j = \arg\min_{\varphi} \sum_{i=1}^{l} (\varphi(f_j(x)) - z_i);$
6. **пока** значения Q_j не стабилизируются.

Метод основан на итерационном уточнении функций ϕ_j. На первом шаге они полагаются линейными, $\phi_j(x) = \alpha_j f_j(x)$, и неизвестные коэффициенты α_j настраиваются методами многомерной линейной регрессии, один из которых описан выше. На каждом последующем шаге выбирается одна из функций ϕ_j, все остальные фиксируются, и выбранная функция строится заново. Для этого решается стандартная задача наименьших квадратов:

$$Q(\varphi_j, X^l) = \sum_{i=1}^{l} (\varphi_j(f_j(x_i)) - \underbrace{(y_i - \sum_{k=1,k\neq j}^{n} \varphi_k(f_k(x_i)))}_{z_i = \text{const}(\varphi_j)})^2 \to \min_{\varphi_j}$$

с обучающей выборкой $Z_j^l = (f_j(x_i), z_i)_{i=1}^l$. Для решения данной подойдёт метод ядерного сглаживания.

Решение проблемы мультиколлинеарности наборов параметров функции QoE заключается в том, чтобы подвергнуть исходные признаки функциональному преобразованию, гарантировав линейную независимость новых признаков и, возможно, сократив их количество, то есть уменьшив размерность задачи. В методе главных компонент (principal component analysis, PCA) строится минимальное число новых признаков, по которым исходные признаки восстанавливаются линейным преобразованием с минимальными погрешностями. PCA относится к методам обучения без учителя (unsupervised learning), поскольку матрица объекты–признаки F преобразуется без учёта целевого вектора y.

Разрабатываемая методика решает проблемы неуниверсальности и усреднённости оценки других методик QoE. Механика её применения включает в себя возможность настройки под конкретную систему и набор параметров. Помимо этого, в методику включён алгоритм оценки QoS на основе вейвлет-анализа, позволяющий оценивать качество вдоль линий передачи контента и автоматически выявлять проблемые участки инфраструктуры.

Работа выполнена при поддержке РФФИ, номер гранта 16-07-00571.

Литература

1. ITU-T Tutorial. Objective perceptual assessment of video quality: Full reference television. – ITU-T, 2004. 218 p.
2. *В.П. Дворкович, А.В. Дворкович* Цифровые видеоинформационные системы. М Техносфера, 2016 г.
3. *Марков М. В*. Сравнительный анализ метрик оценки качества восприятия потокового видео // Журнал Сервис в России и за рубежом. 2011. №1(20). С. 138–142.
4. *Маколкина М.А.* Учёт параметра Хёрста при формировании субъективных оценок качества восприятия видео и значений // Журнал Информационные технологии моделирования и управления. 2016. №3 (99). С. 197–204.
5. *Julie Kunstler, Angel Dobardziev, Wireline* Video QoE Using U-vMOS, Режим доступа https://ovum.informa.com/resources/product-content/2016/11/11/15/09/analyst-white-paper-wireline-video-qoe-using-u-vmos
6. Recommendation ITU-T G.1080. Quality of experience requirements for IPTV services. – ITU-T, 12/2008. 44 p.
7. ITU-T Tutorial. Objective perceptual assessment of video quality: Full reference television. – ITU-T, 2004. 218 p.
8. *E. Mammen, B. U. Park* A Simple Smooth Backfitting Method for Additive Models //The Annals of Statistics №5 2006 P. 2252–2271.

УДК 537.86, 621.373

Экспериментальное исследование генератора хаотических колебаний дециметрового диапазона частот

А.В. Гриневич, М.Д. Ушаков

Московский государственный технический университет им. Н.Э. Баумана

Изучение возможности получения хаотических колебаний в радиоэлектронных системах ведет свою историю, начиная с 60-х годов XX века. С тех пор наработаны различные методы формирования хаотических сигналов с помощью генераторов хаоса в различных частотных диапазонах. Вместе с тем развитие современных телекоммуникационных технологий ставит задачи по освоению новых частотных диапазонов и использованию на вторичной основе уже занятых. Один из подходов к решению этой задачи – разработка методов передачи при помощи широкополосных хаотических сигналов [1], что, в свою очередь, требует разработки генераторов хаотических колебаний. В данной работе речь идет о создании экспериментального макета генератора хаоса в диапазоне от 0.1 до 1 ГГц.

Структура генератора аналогична структуре семейства генераторов [2], [3] и включает в себя активный элемент – транзистор и частотно-избирательную систему. Теория предсказывает, что в таких генераторах возможно возникновение хаотических колебаний в достаточно широком частотном диапазоне, который соответствует полосе частот линейной колебательной системы, входящей в генератор.

Схема генератора приведена на рис. 1. За основу взята автоколебательная система с 2,5 степенями свободы [2]. В качестве активного нелинейного элемента использована модель биполярного транзистора BFP620 в корпусе. Пассивной колебательной системой, задающей диапазон, в котором формируются хаотические колебания, является линейная автоколебательная система, реализованная на сосредоточенных элементах. К схеме были добавлены конденсатор C7 и сопротивление R2 (рис. 1) для того, чтобы избавиться от постоянной составляющей в спектре выходного сигнала и учесть входное сопротивление реальной нагрузки в экспериментальном макете.

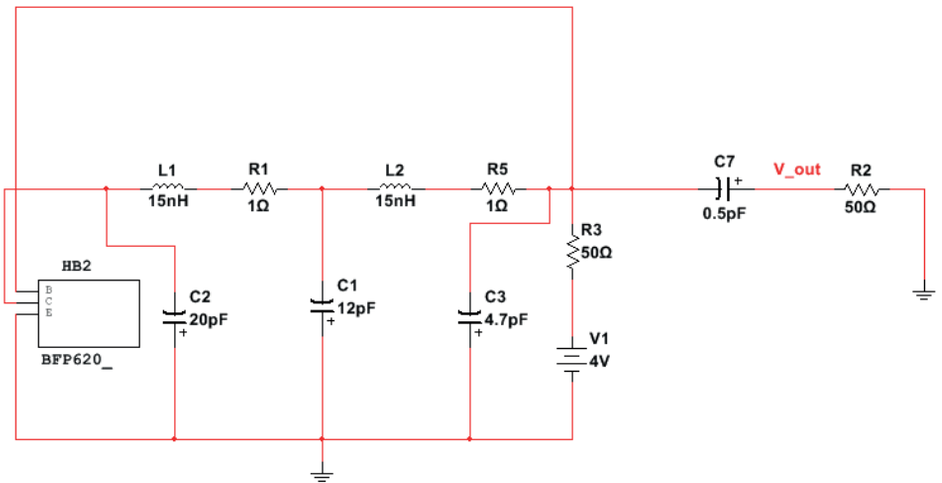


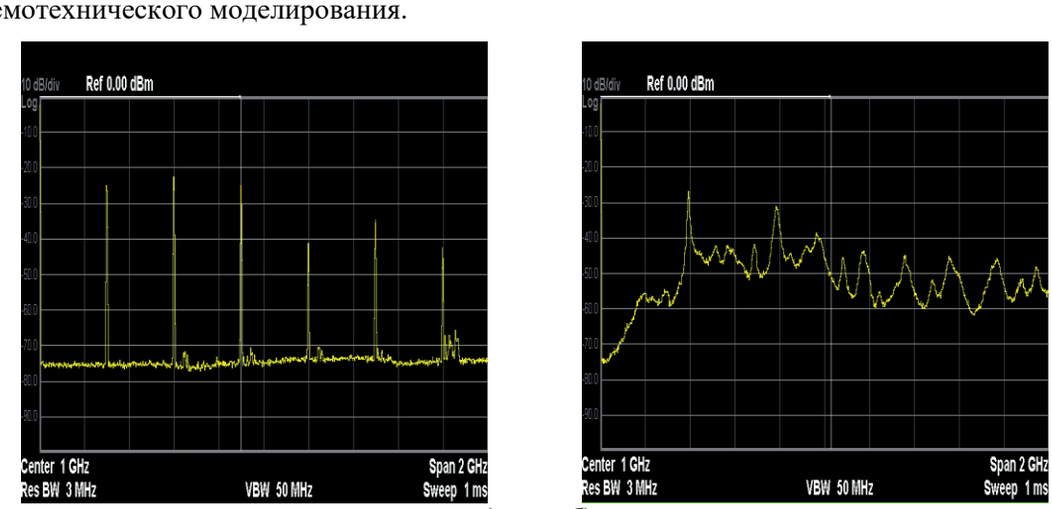
Рис. 1. Схема генератора хаотических колебаний

Создание экспериментального образца генератора включало несколько этапов. На основе результатов математического моделирования динамической системы, описывающей генератор, был определен диапазон значений параметров, в пределах которых имеет смысл искать хаотические режимы колебаний. Далее режимы генератора исследовались при помощи его схемотехнической модели, реализованной в пакете Multisim с тем, чтобы учесть влияние свойств схемотехнических моделей радиоэлементов. Параметры системы были выбраны таким образом, чтобы обеспечить формирование хаотических колебаний в диапазоне до 1 ГГц.

В соответствии со схемой (рис. 1.) был реализован экспериментальный макет генератора.

Управление режимами колебаний генератора осуществлялось при помощи изменения напряжения питания. Для напряжения до 5 В в генераторе возникают колебания периода 1 (рис. 2а). При дальнейшем увеличении напряжения осуществляется переход к хаосу через каскад бифуркаций удвоения периодов, т.е. возникают колебания периода 2, 4 и т.д. При значении напряжения питания 8.3 В (рис. 2б) происходит переход к хаотическому режиму, и спектр колебаний становится сплошным.

Основная мощность колебаний сосредоточена в области от 0.1 до 1 ГГц, что соответствует поставленной задаче и предварительным расчетам, сделанным в ходе схемотехнического моделирования.



а) б)

Рис. 2. Спектр колебаний периода 1 и последующий спектр перехода к хаосу при увеличении напряжения

В работе экспериментально реализован макет генератора хаотических колебаний на основе автоколебательной структуры с 2,5 степенями свободы [2] с напряжением питания до 8,5 В, диапазоном частот 0.1–1 ГГц, мощностью колебаний 0.5 мВт. Данный макет может быть использован как прототип для исследований в области широкополосной радиосвязи на основе хаотической несущей.

Литература

1. *Дмитриев А.С.*, *Клецов А.В.*, *Лактюшкин А.М.*, *Панас А.И.*, *Старков С.О.* Сверхширокополосная беспроводная связь на основе динамического хаоса // Радиотехника и электроника. 2006, Т. 51, №10. С. 1193–1209.
2. *Дмитриев А.С.*, *Ефремова Е.В.*, *Максимов Н.А.*, *Григорьев Е.В.* Генератор хаотических колебаний сверхвысокочастотного диапазона на основе автоколебательной системы с 2,5 степенями свободы // Радиотехника и электроника. 2007. Т. 52. № 10. С. 1232–1240.
3. *Дмитриев А.С.*, *Ефремова Е.В.*, *Максимов Н.А.*, *Панас А.И.* Генерация хаоса. М.: Техносфера, 2012.

УДК 621.37

Применение перекрывающихся оконных функций в сигнале OFDM-систем

К.К. Янситов

Московский физико-технический институт (государственный университет)

В современных системах цифрового телерадиовещания используется OFDM модуляция. Такой метод модуляции позволяет эффективно формировать и передавать битовые потоки информации. При формировании OFDM-символа используется прямоугольный импульс [1]. Но сигнал состоит из последовательно соединённых символов, а значит, на стыке символов будут наблюдаться скачки амплитуд и фаз. При передаче подобного сигнала на передатчике будет наблюдаться ухудшение спектрограммы с появлением внеполосных компонент, то есть будет наблюдаться возрастание амплитуд боковых лепестков.

Можно накладывать другую оконную функцию [2], [3] на символ, но тогда либо исказится полезный участок символа, либо удлинять сам символ и применять окно уже на удлинённый символ.

В работе предлагается подавлять боковые лепестки при помощи оконных функций, вводя перекрытие между OFDM-символами, благодаря чему сигнал не будет удлинён, и при этом повысится спектральная эффективность. Пример работы алгоритма указан на рис. 1.

Было проведено исследование эффективности алгоритма в зависимости от типа оконной функции, ширины оконной функции и других параметров оконных функций.

Исходя из полученных результатов моделирования, можно сделать выводы, что данный алгоритм эффективнее подавляет внеполосовые компоненты, по сравнению с формированием сигнала OFDM с прямоугольным окном и защитным интервалом. Но такой сигнал становится менее защищённым от межсимвольной интерференции, так как искажается некоторая часть защитного интервала. Также было показано (рис. 2), что наилучшим окном для сглаживания является оконная функция Ханна.

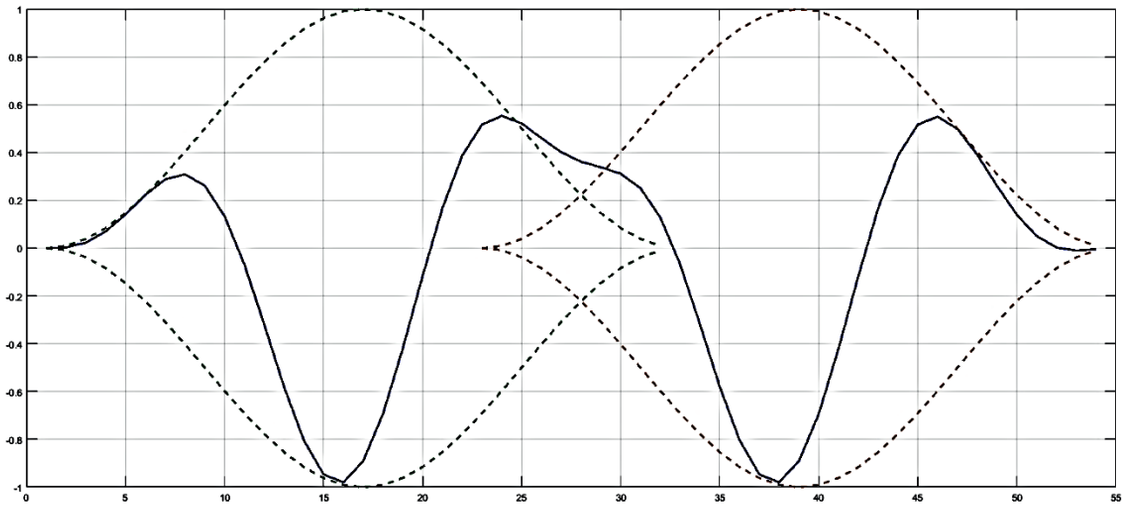


Рис. 1. Пример работы алгоритма на примере стыка двух синусоид. Прерывистой линией указана оконная функция, сплошная линия – это синусоида

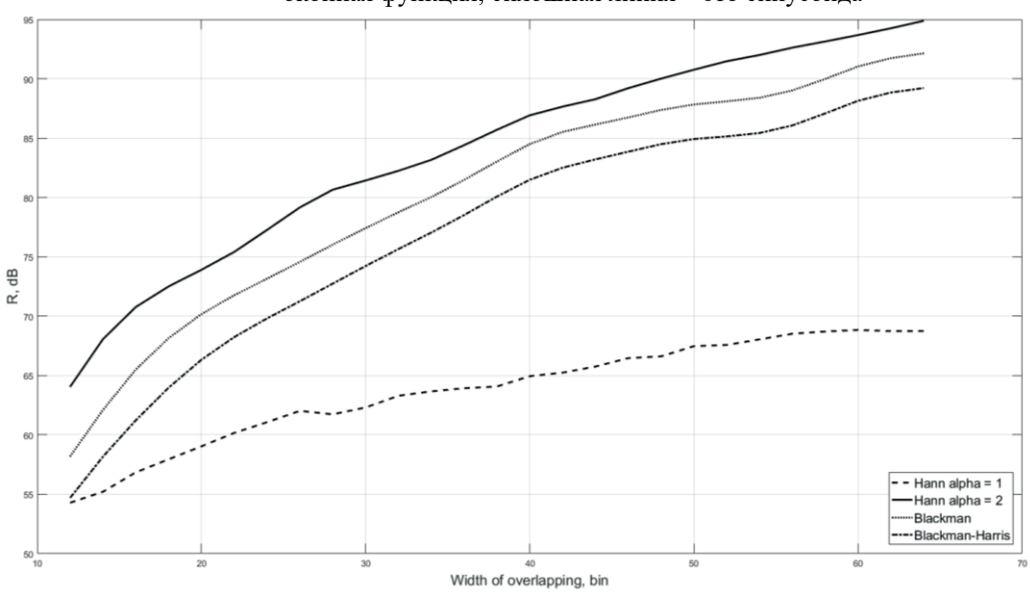


Рис. 2. График зависимости отношения средних мощностей внутри полосы к внеполосовой средней мощности спектра при использовании нескольких оконных функций

Литература

1. *Fedosov V.P.*, *Kovtun D.G.*, *Legin A.A.*, *Lomakina A*. Research of model OFDM-signal with small level of out-of-band radiation // Izvestiya sfedu. Engineering Sciences
2. *Behrouz Farhang-Boroujeny*. Development of broadband communication systems. OFDM Versus Filter Bank Multicarrier // IEEE SIGNAL PROCESSING MAGAZINE [92] MAY, 2011.
3. *Gentile K.* Digital Pulse-Shaping Filter Basics. Analog devices AN–922.

УДК 537.86, 621.373

Модель генератора хаотических колебаний дециметрового диапазона на основе автоколебательной системы с 2,5 степенями свободы

М.Д. Ушаков, А.В. Гриневич

Московский государственный технический университет им. Н.Э. Баумана

Применение хаотических колебаний для передачи информации в беспроводных системах связи и сенсорных сетях [1] требует разработки генераторов хаоса в различных

диапазонах частот. В частности, для ряда приложений представляет интерес диапазон дециметровых длин волн.

В работе проведен анализ твердотельного источника хаотических колебаний в дециметровом диапазоне на основе модели автоколебательной системы с 2,5 степенями свободы [2]. В качестве активного элемента используется высокочастотный транзистор BFP620.

Математическая модель генератора описывается системой обыкновенных дифференциальных уравнений, основанной на законах Кирхгофа. Вольт-амперная характеристика транзистора описывается экспоненциальной функцией. Однако математической модели недостаточно для построения адекватной высокочастотной модели генератора. Поэтому для анализа работы данного генератора использованы пакеты схемотехнического моделирования Multisim и LabVIEW.

На рис. 1 приведена схема генератора. Блок BFP620 представляет собой транзистор в корпусе. Параметры транзистора выбраны в соответствии с моделью Гуммеля-Пуна.

Исследована зависимость напряжения V_out от значения бифуркационного параметра. В качестве бифуркационного параметра выбрано напряжение источника питания V2.

При построении бифуркационной диаграммы с целью получить достаточно тонкую структуру диаграммы значение параметра менялось адиабатически по формуле

$$V_{in}(t) = b_{start} + \left(b_{stop} - b_{start}\right) \cdot \frac{t - t_{start}}{t_{stop} - t_{start}}, \quad (1)$$

где $V_{in}(t)$ – напряжение источника питания, b_{start} – начальное значение бифуркационного параметра, b_{stop} – конечное значение бифуркационного параметра, t_{start} – начальное время симуляции, t_{stop} – конечное время симуляции.

Результаты расчётов приведены на рис. 2, 3. На рис. 2 приведён фрагмент бифуркационной диаграммы в диапазоне напряжений 1,7÷1,8 В. При V_in≈1,733 В наблюдается бифуркация удвоения периода и рождаются 2-циклы. Из графика видно, что при значении V_in≈1,755 В бифуркационная картина начинает повторяться, то есть последовательность значений сигнала представляет собой самоподобную, фрактальную структуру. Дальнейшее увеличение параметра приводит к возникновению хаотического режима через каскад бифуркаций удвоений периода колебаний. При V_in>1,9 V регулярные режимы чередуются с хаотическими.

На рис. 3 приведен спектр мощности колебаний, соответствующий хаотическому режиму при напряжении V_in=2.95 В.

Разработана и исследована модель генератора хаоса. В модели получены хаотические колебания в диапазоне частот 0–1 ГГц.

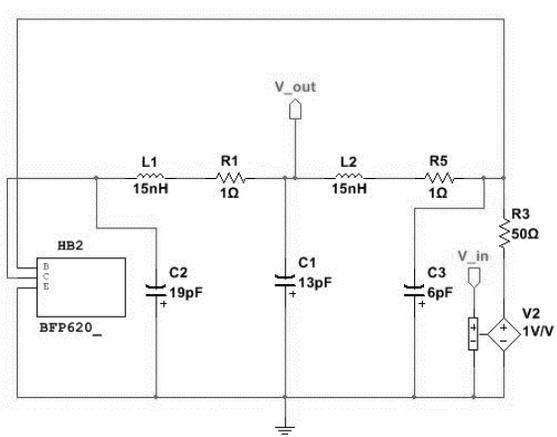


Рис. 1. Схема генератора в Multisim

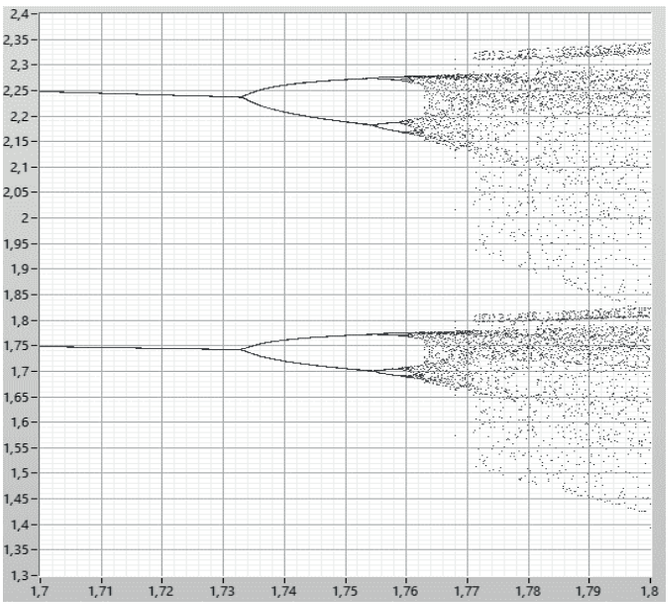


Рис. 2. Фрагмент бифуркационной диаграммы в диапазоне напряжений 1,7÷1,8 В

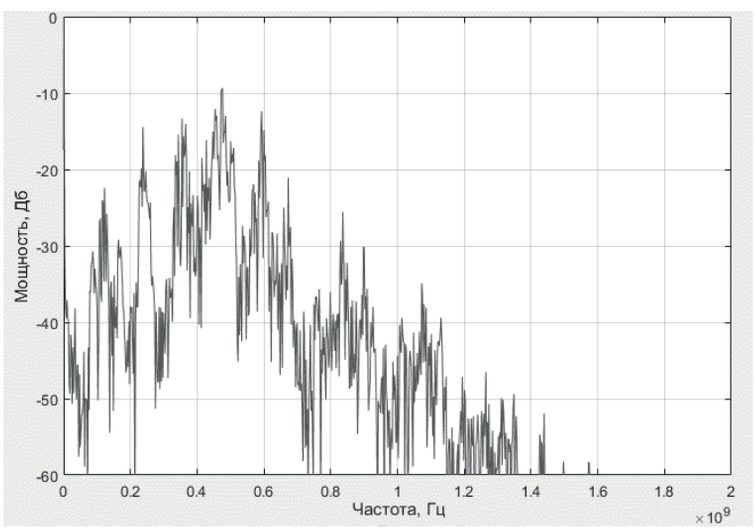


Рис. 3 Спектр мощности при V_in=2.95 В

Литература

1. *Дмитриев А.С., Ефремова Е.В., Клецов А.В., Кузьмин Л.В., Лактюшкин А.М., Юркин В. Ю.* Сверхширокополосная беспроводная связь и сенсорные сети // Радиотехника и электроника. 2008. Т. 53. №10. С. 1278–1289.
2. *Дмитриев А.С., Ефремова Е.В., Максимов Н.А., Панас А.И.*. Генерация хаоса. М.: Техносфера. 2012.

УДК 004.932.2

Смешанная поляризация в задаче трехмерного сканирования объектов

В.А. Таамазян

Московский физико-технический институт (государственный университет)

Рассмотрена задача уточнения трехмерной формы объекта, а также разделения света, отраженного от объекта на зеркально отраженную и рассеянную компоненты с использованием информации о поляризации света, захваченной камерой с поляризатором с

нескольких ракурсов. Классический подход к Форме из Поляризации (ФиП) полагается на отраженный зеркально от объекта свет. С целью использовать также рассеянный свет Аткинсон и Хэнкок предложили метод, базирующийся исключительно на рассеянном от объекта свете (отсюда и далее рассеянная ФиП) [1]. Тем не менее большая часть объектов в реальном мире отражает свет не исключительно рассеяно или зеркально, а в виде композиции двух этих типов отражения. Таким образом, «смешанное отражение» случается, когда и рассеянная, и зеркальная компоненты достигают камеры, делая использование методов ФиП непригодным.

Интенсивность света, отраженного от определенной точки объекта и поступившая в пиксель матрицы камеры, пройдя предварительно через поляризатор, может быть выражена в следующем виде:

$$I\left(\phi_{pol}\right)=\frac{I_{\max}+I_{\min}}{2}+\frac{I_{\max}-I_{\min}}{2}\cos\left(2\left(\phi_{pol}-\phi\right)\right), \tag{1}$$

где ϕ – фаза поляризованного света, ϕ_{pol} – угол поляризатора, $I_{\max}$ и $I_{\min}$ – максимальная и минимальная интенсивности света. В дихроматической модели отражения интенсивность отраженного света содержит две ключевые компоненты:

$$I=I^{d}+I^{s}, \tag{2}$$

где I^{d} и I^{s} – относятся к интенсивности рассеянного и зеркально отраженного света соответственно. Можно предположить, что вариации зеркально отраженной компоненты много больше вариаций рассеянной компоненты для поверхности со смешанным отражением, и поэтому измеренная степень поляризации света:

$$\rho=\frac{I^{s}_{\max}-I^{s}_{\min}}{I^{s}_{\max}+I^{s}_{\min}+I^{d}}=\tilde{\rho}\frac{I^{s}}{I}=\tilde{\rho}\frac{I-I^{d}}{I} \tag{3}$$

где $I^{\text{s}}_{\min}$ и $I^{\text{s}}_{\max}$ соответствуют максимуму и минимуму интенсивности зеркально отраженной компоненты света. Таким образом,

$$I^{d}=I\left(1-\rho\frac{n^{2}-\sin^{2}\theta+\tan^{2}\theta}{2\sin\theta\tan\theta\sqrt{n^{2}-\sin^{2}\theta}}\right). \tag{4}$$

В данном уравнении две неизвестных: интенсивность рассеянной компоненты света, I^{d} и коэффициент преломления n. В предположении ламбертовского отражения интенсивность рассеянной компоненты света не зависит от угла обзора. Коэффициент преломления как свойство материала объекта также не зависит от угла обзора. Таким образом, предлагаемый метод предполагает захват данных о поляризации отраженного света с нескольких ракурсов:

$$I^{d}=f(n,\theta,I_{i},\rho_{i})\triangleq I_{i}\left(1-\rho_{i}\frac{n^{2}-\sin^{2}\theta_{i}+\tan^{2}\theta_{i}}{2\sin\theta_{i}\tan\theta_{i}\sqrt{n^{2}-\sin^{2}\theta_{i}}}\right) \tag{5}$$

для i-го положения камеры среди N ракурсов. Для поиска I^{d} решается нелинейная оптимизационная задача в следующей форме:

$$\left\{I^{d},n,\right\}=\underset{I^{d},n}{\operatorname{argmin}}\sum_{i=1}^{N}\left(I_{d}-f\left(n,\theta_{i},I_{i},\rho_{i}\right)\right)^{2}. \tag{6}$$

Оптимизация производилась с помощью метода последовательного квадратичного программирования.

На рис. 1 приведены примеры результатов экспериментов. Неподвижный глянцевый шар фотографируется с трех ракурсов с расстояния 50 см с помощью камеры Canon Rebel T3i с объективом EF-S 18mm–55mm f/3.5–5.6 IS II SLR и линейным

поляризатором, а также четвертьволновой пластинкой, Hoya CIR-PL. Угол между точками съемки – 10 градусов. С каждого ракурса захватывается три фотографии с разными углами поворота поляризатора. На рис.1 приведена фотография камеры и объекта, а также результаты реконструкции нормалей объекта с использованием методов ФиП [2], а также предложенного метода. Результаты наглядно показывают, что предложенный метод лучше всего справляется с задачей разделения компонент и оценкой ориентации нормалей, снизив MSE практически в 2 раза.

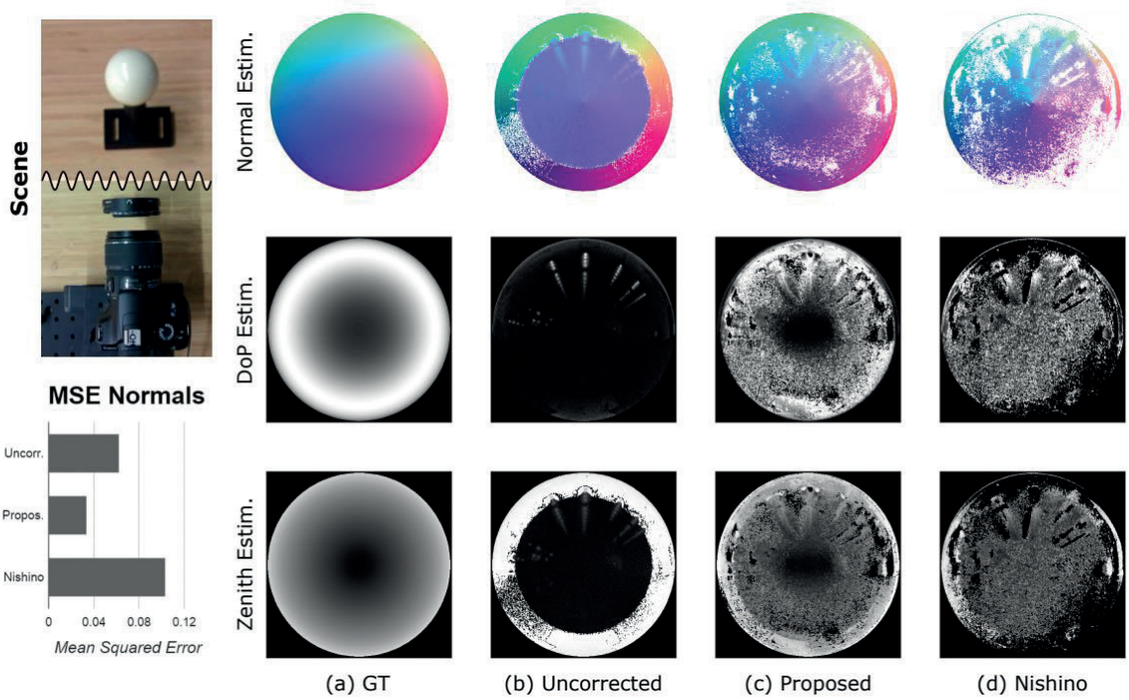


Рис. 1. Результаты экспериментов с использованием предложенного метода для оценки карты нормалей

Литература

1. *Atkinson G.A.*, *Hancock E.R.* Recovery of surface orientation from diffuse polarization // Image Processing, IEEE Transactions on 15(6) (2006) 1653–1664.
2. *Nishino K.*, *Zhang Z.*, *Ikeuchi K.* Determining reflectance parameters and illumination distribution from a sparse set of images for view-dependent image synthesis // In: Computer Vision, 2001. ICCV 2001. Proceedings. Eighth IEEE International Conference on. Volume 1. IEEE (2001) 599–606.

УДК 519.173.5

Эффективность графовых мер близости в задачах выявления структуры сетей

В.С. Ивашкин

Московский физико-технический институт (государственный университет)
Институт проблем управления им. Трапезникова РАН

Определение расстояний и близостей между узлами графа на основе его структуры — одна из важнейших задач в анализе сетевых данных. Зачастую сеть представлена в виде матрицы смежности или списка смежности, которые сложно интерпретировать непосредственно. Получение значимой информации из таких данных требует сложных методов, которые часто должны быть выбраны на основе контекста.

Получение информации о расстояниях между вершинами обеспечивает фундаментальный способ интерпретации сети. Действительно, имея информацию о расстояниях между узлами, можно применить традиционные методы многомерного статистического анализа или методы машинного обучения.

Ребра графа, как правило, предоставляют локальную информацию, например, расстояния между очень «близкими» вершинами. В задачах классификации и кластеризации мы часто заинтересованы в расстояниях или близостях между любой парой объектов. Для этого требуется ввести функцию близостей / расстояний на графе. Эта функция каждой паре вершин ставит в соответствие вещественное число. Наиболее распространенные способы определения расстояния между вершинами графа - кратчайший путь (Shortest Path) и ожидаемая длина случайных блужданий (Commute Time).

В этой работе рассматривается набор графовых ядер, мер близости и относящихся к ним расстояний, применяемых к кластерным вершинам в случайных графах и датасетах. Меры включают в себя диффузионное ядро фон Неймана (Walk kernel) [1], регуляризованное лапласовское ядро (Forest kernel) [2], экспоненциальное диффузионное ядро (Communicability kernel) [3], лапласовское экспоненциальное диффузионное ядро (Heat kernel) [4] и другие. Для генерации случайных графов используется стохастическая блочная модель (Stochastic block model) [5], в которой сначала задаются вершины и кластеры, которым они принадлежат, а после проставляются ребра с различными внутрикластерными и межкластерными вероятностями.

Основной результат текущей работы в том, что в некоторых простых случаях логарифмические меры (т.е. меры, которые получаются при взятии логарифма из матрицы близостей) подходят лучше для разделения классов, чем «плоские» меры. Прямое сравнение внутрикластерных и межкластерных расстояний в терминах ROC-кривых подтверждает это заключение. Тем не менее существуют исключения из этого правила. В большинстве экспериментов лидером является новая мера logarithmic Communicability.

Литература

1. *Buckley F., Harary F*. Distance in Graphs. — Redwood City, CA: Addison-Wesley, 1990.
2. *Chebotarev Pavel*, *Shamis Elena*. The Forest Metrics for Graph Vertices // Electronic Notes in Discrete Mathematics. 2002. V. 11. P. 98–107.
3. *Estrada Ernesto*. The communicability distance in graphs // Linear Algebra and its Applications. 2012. V. 436, N 11. P. 4317–4328.
4. *Chung Fan*, *Yau Shing-Tung*. Coverings, heat kernels and spanning trees // Journal of Combinatorics. 1998. V. 6. P. 163–184.
5. *Mossel E*., *Neeman J*., *Sly A*. Stochastic block models and reconstruction //arXiv preprint arXiv:1202.1499. 2012.

УДК 004.8

Рекурсивная нейроморфологическая сеть для классификации текстов

Ле Мань Ха[1], Чан Ань Дык[1]

[1]Московский физико-технический институт (государственный университет)

В данной работе рассматривается применение морфологического анализа при классификации текстов. Так же была предложена рекурсивная нейроморфологическая сеть, которая состоит из двух частей – первая объединяет два вектора словоформ, а вторая объединяет два вектора морфологических характеристик.

1. Введение

Классификация текстов — одна из важнейших задач обработки естественных текстов, заключающаяся в определении категории текста, список категорий может быть известен или нет [1] . В последнее время количество электронных документов резко возросло, в связи с чем классификация текстов является одной из основных задач компьютерной лингвистики. К ней сводится ряд других задач: *распознавание спама,*

сортировка новостей, снятие неоднозначности при автоматическом переводе текстов, контекстная реклама, подбор ключевых слов, автоматическое аннотирование и др.

2. Нейросетевые подходы к классификации текстов на основе морфологического анализа

2.1.Морфологический анализ – процесс поиска морфологических характеристик словоформ. Для реализации морфологического словаря используется структура данных префиксное дерево - это тип дерева поиска для хранения ассоциативного массива из элементов (ключ, значение), где ключи являются префиксами словоформ [2].

2.2. Рекурсивная нейроморфологическая сеть, которая состоит из двух частей – первая объединяет два вектора лемм, а вторая объединяет два вектора морфологических характеристик. Морфологическая часть рекурсивного автоэнкодера позволяет повышать точность выбора векторов слов в процедуре формирования векторного представления текста.

Нейроморфологическая сеть объединяет две пары векторов (лемма; морфологические характеристики) $(x_1; m_1), (x_2, m_2)$ в одну пару (y, m):

$$y = f\left(W_w^{(1)}[x_1, x_2] + b_w^{(1)}\right), \quad (1)$$

$$m = f\left(W_m^{(1)}[m, m_2] + b_m^{(1)}\right), \quad (2)$$

где $W_w^{(1)}, W_m^{(1)}$ – матрицы весов, $b_w^{(1)}, b_m^{(1)}$ - вектора смещения входного слоя сети для лемм и морфологических характеристик.

Чтобы вычислить ошибки объединения, нужно восстанавливать исходные векторы $x1, x2$ из вектора y:

$$[x_1', x_2'] = W_w^{(2)} y + b_w^{(2)}, \quad (3)$$

$$[m_1', m_2'] = W_m^{(2)} m + b_m^{(2)}, \quad (4)$$

где $W_w^{(2)}, W_m^{(2)}$ – матрицы весов, $b_w^{(2)}, b_m^{(2)}$ – векторы смещения скрытого слоя сети для лемм и морфологических характеристик.

Этот процесс повторяется N – 1 раз для текста, состоящего из N слов. В результате получается итоговый вектор – семантическое векторное представление текста, этот вектор используется как вход для системы обучения.

Распределение вероятностей для классификации векторного представления текста y вычисляется слоем Softmax [3]:

$$d(y; \theta) = Soft\max(W^{Soft\max} y) \quad (5)$$

3. Эксперимент и оценка результата реализуемого метода

Для оценки алгоритма был использован метод K-Fold Cross-validation [4] с параметром K= = 10 и обучающая выборка текстов Wikinews на русском (7233 текста в 8 категориях) и английском языках (23588 текстов в 11 категориях).

Классификация баз данных Wikinews

Метод	Wikinews-Ru	Wikinews-En
Naive Bayes	66.4	81.1
Nearest Centroid	68.6	86.3
KNN	72.5	87.3
KNN с двоичным деревом	71.7	88.9
Рекурсивная нейроморфологическая сеть	**74.3**	**90.2**

Заключение

Учитывая результаты экспериментов, можно прийти к выводу, что морфологические признаки словоформ и рекурсивная нейроморфологическая сеть позволяют повышать качество классификации текстов.

Литература

1. *Lee JY, Dernoncourt F.* Sequential Short-Text Classification with Recurrent and Convolutional Neural Networks. InProceedings of NAACL-HLT 2016. P. 515–520.
2. *Knuth D.E.* The Art of Computer Programming: Volume 3: Sorting and Searching. AddisonWesley Professional; 1998 Apr 24.
4. *Memisevic R, Zach C, Pollefeys M, Hinton G.E.* Gated softmax classification. In Advances in neural information processing systems 2010. P. 1603–1611.
5. *Efron B, Tibshirani R.* Bootstrap methods for standard errors, confidence intervals, and other measures of statistical accuracy. Statistical science. 1986 Feb 1. 54–75.

УДК 004.3

Двухфакторная аутентификация в браузере

П.А. Мульцын

Московский физико-технический институт (государственный университет)

В настоящее время при разработке СЗИ существует класс задач, которые целесообразно решать внедрением веб-интерфейсов в продукты. Примером такой задачи может быть реализация подсистемы управления СЗИ. Одним из требований к таким системам является наличие двухфакторной аутентификации пользователя [1]. Существующие решения двухфакторной аутентификации подразумевают использование специального кода в виде SMS, одноразовые пароли, USB-ключи и смарт-карты.

Universal second factor (U2F) – протокол двухфакторной аутентификации, предназначенный для усиления парольной аутентификации за счет использования физических устройств (токенов), основанный на криптосистеме с открытым ключом [2]. U2F является открытым протоколом, задействует интерфейс USB HID, который поддерживается в ОС по умолчанию, не требует установки дополнительного ПО и плагинов, в связи с чем является привлекательным вариантом для реализации.

На данный момент уже выпускаются устройства, поддерживающие U2F. Однако серьезным минусом их устройств для российского рынка является отсутствие реализации протокола с использованием отечественных криптографических алгоритмов [3], [4].

Объектами протокола U2F (рис. 1) являются клиент и сервер, связь между которыми осуществляется по сетевому протоколу передачи данных посредством использования U2F JS API.

В связи с этим работа над поддержкой протокола велась в двух направлениях – реализация логики протокола на готовой аппаратной платформе ШИПКА [5] с высокопроизводительным основным компонентом – микроконтроллером LPC1820 [6] и разработка соответствующей серверной библиотеки, обеспечивающей функциональность работы протокола для семейства операционных систем Windows.

По итогу работы был получен прототип U2F устройства и серверная библиотека, использующие российские криптографические алгоритмы, что позволяет использовать устройство как второй фактор аутентификации пользователя на онлайн-ресурсе или в любом сервисе, поддерживающем логику протокола U2F, в том числе как аутентификатор в мобильном приложении.

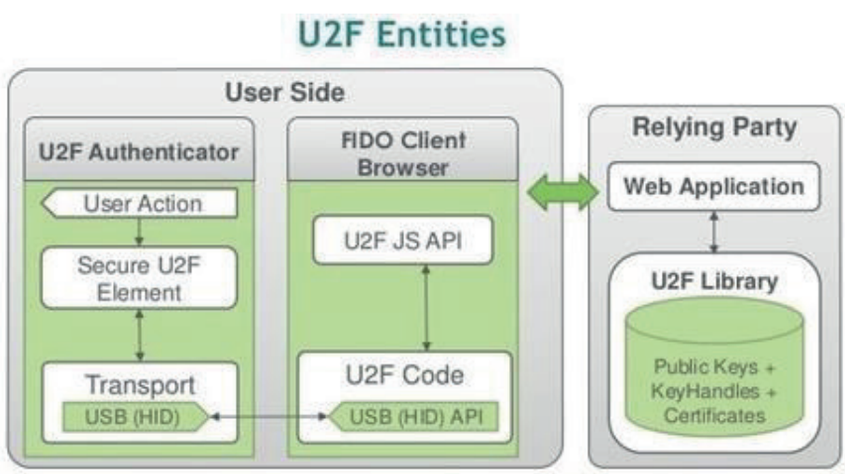


Рис. 2. Схема взаимодействия объектов протокола

Литература

1. Методический документ. Меры защиты информации в государственных информационных система: утвержден ФСТЭК России 11 февраля 2014 г.
2. *Malte Kahrs, Dr. Kim Nguyen.* Future Ecosystems for Secure Authentication and Identification // ISSE 2015. — Springer Vieweg, 2015. P. 12–21. 315 p.
3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования. – Введ. 2012-08-07. – М.: Стандартинформ, 2012.
4. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Введ. 2012-08-07 – М.: Стандартинформ, 2012.
5. Аппаратные идентификаторы [Электронный ресурс]. Режим доступа: http://www.accord.ru/shipka-pi.html, свободный.
6. LPC1850/30/20/10 [Электронный ресурс] / 32-bit ARM Cortex-M3 flashless MCU; up to 200 kB SRAM; Ethernet, two HS USB, LCD, and external memory controller; Rev. 6.7 — 14 March 2016 Product data sheet – Режим доступа: https://www.nxp.com/docs/en/data-sheet/LPC1850_30_20_10.pdf, свободный.

УДК 004.94

Исследование современных методов классификации сетевых атак

Т.А. Хахулин, С.А. Татарских, А.А. Нагапетян, Д.Э. Копосов

Московский физико-технический институт (государственный университет)

За последние годы компьютерные сети сильно развились и стали частью многих современных экономических, социальных, медицинских и многих других систем. С их развитием все больше возникает необходимость в предотвращении нежелательного вторжения с внешней стороны. Одним из таких решений является система обнаружения вторжений (IDS – Intrusion detection system), которая в режиме реального времени будет следить за компьютерными сетями. Такие системы начали использоваться еще в 1980-х годах, но большинство из них имело высокие значения false positive и false negative срабатываний.

Системы обнаружения вторжений расположены внутри сети и отслеживают пакеты, проходящие через коммутаторы. Функции, которые IDS должны выполнять, заключаются в обнаружении угроз, принятии необходимых мер при их обнаружении и записи всех важных событий, происходящих внутри сети.

В этой работе мы строим модель IDS, используя различные алгоритмы машинного обучения, для решения задачи классификации сетевых атак по статистическим данным о соединениях, а также оцениваем качество работы этих алгоритмов.

Наша система является хост-основанной (HIDS – Host-based IDS) по типу расположения и аномально-основанной (ABD – Anomaly based detection) по типу алгоритма распознавания.

Для построения нашей модели мы использовали данные KDD99. Признаки делятся на три категории (всего 41 признак).

1. Признаки, полученные из индивидуальных TCP-подключений.
2. Признаки, полученные во время двухсекундного временного окна.
3. Признаки, предполагаемые исходя из знаний о домене.

На этапе предобработки данных были выявлены признаки, которые не оказывают влияния на целевую переменную. Также мы удалили несколько признаков, имеющих высокую корреляцию, и убрали множественное количество дубликатов.

Все данные по подключениям делятся на «плохие» и «хорошие». «Плохие» подключения в свою очередь делятся на 4 типа атак

1. DOS – (denial-of-service) – отказ в обслуживании.
2. R2L – неавторизированный доступ с удаленного компьютера (например, перебор паролей).
3. U2R – неавторизированный доступ получения локальных прав суперпользователя (root) (например, "buffer overflow" атака).
4. Probing – наблюдение и зондирование (например, сканирование портов).

Чтобы оценить качество модели, была использована F1-мера, для того, чтобы минимизировать количество false-negative. Именно ошибки второго рода представляют наибольшую опасность, так как означают пропущенную сетевую атаку и могут нанести вред системе.

Опишем основные аспекты методов, использованных для построения модели.

K ближайших соседей (K Nearest Neighbors)

Один из простейших алгоритмов для автоматической классификации объектов. Объект присваивается тому классу, который является наиболее распространённым среди K соседей данного элемента, классы которых уже известны. Кроме простоты, алгоритм не имеет особых преимуществ. Он медленный и потребляет большое количество памяти. Однако он послужил хорошим стартом для анализа и получили приемлемое качество классификации.

Наивный байесовский классификатор (Naive Bayes)

Простой вероятностный классификатор, основанный на применении теоремы Байеса со строгими (наивными) предположениями о независимости, которые выполняются для наших данных. Основная причина использования наивного байесовского классификатора – малое количество данных, необходимых для обучения модели, необходимых для оценки параметров. Тем не менее алгоритм медленно работает на данных с большим количеством признаков и плохо проявил себя на нашем датасете и показал самые низкие результаты.

Случайный лес (Random Forest)

Алгоритм, являющийся композицией нескольких решающих деревьев, обученных на случайных подвыборках исходного датасета. Является одним из лучших подходов к анализу данных, в которых есть явная зависимость от некоторых параметров, которую мы вытащили на препроцессинге данных.

Метод опорных векторов (Support Vector Machine)

Алгоритм обучения с учителем, использующийся для задач классификации и регрессионного анализа. Особым свойством метода опорных векторов является непрерывное уменьшение эмпирической ошибки классификации и увеличение зазора (межклассового расстояния), поэтому метод также известен как метод классификатора с максимальным зазором. Основная идея метода — перевод исходных векторов в пространство более высокой размерности и поиск разделяющей гиперплоскости с максимальным зазором в этом пространстве.

Многослойная нейронная сеть (Multilayer neural network)

В последнее время стали популярны архитектуры глубоких нейронных сетей. Для данного датасета было предложено использовать полносвязную трехслойную нейронную сеть. В качестве регуляризации была использована техника дропаут, которая помогла алгоритму не переобучаться.

Литература

1. *Sravan R.P.R.I., Kumar Jonnalagadda* A. Literature Survey and Comprehensive Study of Intrusion Detection // J. Comput. Appl. 2013. V. 11. N. 81(16). P. 40–47.
2. *Mukherjee B., Heberlein L. T. and Levitt K. N.* Network intrusion detection // IEEE Netw. 1994. V. 8. N. 3. Pp. 26–41.
3. *Chand N., Mishra P., Krishna C. R., Pilli E. S. and Govil M. C.* A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection (ICACCA). 2016. Pp. 1–6.

4. *Kozushko H.* Intrusion detection: Host-based and network-based intrusion detection systems. 2003. V. 11.
5. *Teng L., Teng S., Tang F., Zhu H., Zhang W., Liu D., Liang L.* A Collaborative and Adaptive Intrusion Detection Based on SVMs and Decision Trees // IEEE International Conference on Data Mining Workshop, 2014. P. 898–905.

УДК 004.457

Blockchain-messenger

***И.А.Бескровный*[1,2], *А.С.Парамонов*[1], *И.А.Барашкина*[1]**

[1]Московский физико-технический институт (государственный университет)
[2]Институт радиотехники и электроники им. Котельникова РАН

В современном мире практически отсутствует тайна переписки. Ключи шифрования в большинстве популярных решений хранятся на сервере, откуда могут быть украдены из-за небрежного подхода к защите, украдкой проданы или принудительно раскрыты государственным организациям. Решения на основе асимметрического шифрования, даже если не полагаются на ненадежные сторонние средства для установления соединения, допускающие атаку вида «человек посередине», и не содержат умышленные закладки, всё равно не дают полной анонимности, так как сопоставление объемов, времени получения и отправления входящего и исходящего трафика у клиентов может указать на их связанность между собой.

В рамках курса по защите информации был реализован прототип мессенджера с распределенной базой данных на основе технологии блокчейн, ставящий во главу угла анонимность и защищенность.

В данной работе описана схема применения технологии блокчейн, ассиметричного шифрования на основе эллиптических кривых и симметричного шифрования AES для создания децентрализованного анонимного мессенджера с зашифрованными сообщениями, а также разработан реализующий эту идею прототип для семейства операционных систем Windows NT. Разработка проводилась на языке C#, в силу особенностей архитектуры приложение может быть перенесено на мобильные платформы.

Были проанализированы достоинства и недостатки, возникающие при использовании указанной комбинации технологий, и предложены теоретические способы улучшения качества работы этой связки.

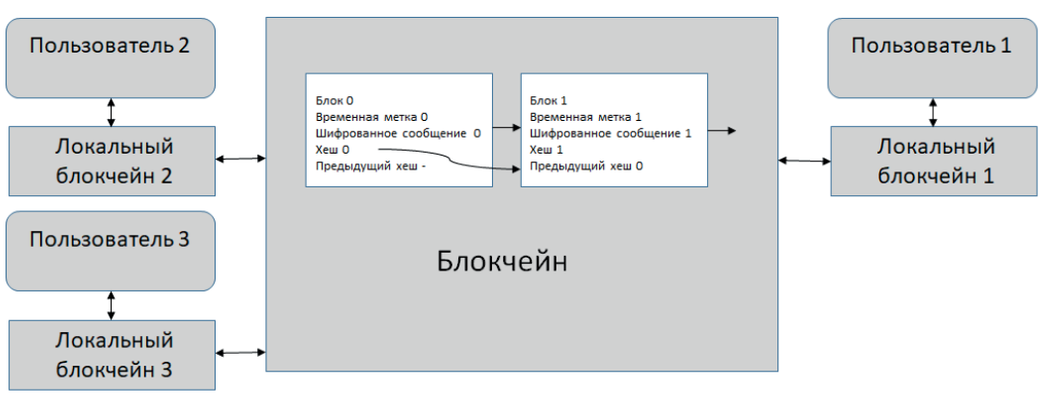


Рис. 1

Литература

1. *Langley A., Hamburg M., Turner S.* Elliptic Curves for Security // IETF, 2016.
2. *Rescorla E.* Diffie-Hellman Key Agreement Method // IETF, 1999.
3. *Whitfield Diffie, Martin E. Hellman* New Directions in Cryptography // IEEE Trans. On Inf. Theory. 1976. V. IT-22. N. 6. P. 644–654.
4. *Martin E. Hellman* An Overview of Public Key Cryptography // IEEE Communications Magazine. 2002. N 5. P. 42–49.

5. *Whitfield Diffie* The First Ten Years of Public-Key Cryptography // Proceedings of the IEEE. 1988. V. 76. N 5. P. 560–577.

УДК 004.98

Генератор действительно случайных чисел на FPGA

О.А. Дикарев, М.Д. Тордия, А.М. Шашев, А.О. Яшухин

Московский физико-технический институт (государственный университет)

Генераторы истинно случайных чисел (TRNG) крайне важны для криптографических систем. Обычно их оценивают с помощью такого понятия, как энтропия. В общем случае энтропия оценивается с помощью стохастической модели и отражается на статистических параметрах полученной последовательности. Генератор, основанный на кольцевом осцилляторе, широко применяется в существующих криптографических системах, потому что он имеет простую структуру, и его стохастическая модель хорошо изучена.

Целью данной работы является рассмотрение некоторых уже существующих алгоритмов для FPGA, основанных на быстром изменении сигнала, поиск, реализация и тестирование алгоритма, позволяющего получить наиболее оптимальную скорость генерации истинно случайных значений.

Рассмотрим основную часть существующих решений. Для этого остановимся подробнее на понятии кольцевой осциллятор. Кольцевой осциллятор – это нечётное количество инверторов или D-защёлок, закольцованных и соединённых последовательно. Теперь рассмотрим в общем алгоритмы.

Алгоритм Open Loop. Для создания истинно случайного сигнала используется дребезг при переключении clock-сигнала (сигнала синхронизации). Дребезг часов передаётся на D-защёлки (DFF), причём на каждую следующую защёлку он передаётся с возрастающей задержкой. Для работы системы необходимо, чтобы время дребезга часов было больше, чем задержки. Далее сигналы с каждой защёлки суммируются по модулю 2, и это число фиксируется как результат. Скорость выдачи таким алгоритмом случайной последовательности достигает 20Mb/s, однако есть два минуса: задержки зависят от температуры и необходимо использовать очень короткие задержки (около 20 пс).

Алгоритм Metastable Rings Oscillator. Рассмотрим отдельно каскад кольцевого осциллятора. Он состоит из мультиплексора с двумя входами, управляющего сигнала от синхронизирующего генератора и соединения выхода мультиплексора и инвертора, замкнутого на один из входов текущего мультиплексора и на следующий каскад. Другой же вход мультиплексора того же каскада замкнут на предыдущий каскад. Последний каскад замыкается на первый и на вход D-триггера. Обязательно, чтобы схема состояла из чётного количества каскадов. Clock-сигнал подаётся с задержкой на управляющий вход триггера. Подав сигнал с задержкой на вход триггера, по положительному фронту clock-сигнала получим отсчёт реализации случайного процесса. Хотя для реализации данного алгоритма требуется минимум памяти, у него малое энергопотребление, и скорость выдачи данных составляет примерно 10 Mb/s, но по факту получить метастабильные состояния крайне трудно.

Алгоритм Fibbonacci and Galois Rings Oscillator. Источником случайного сигнала является кольцевой осциллятор, у которого некоторые из инверторов соединены со входами других через сложение по модулю два. Номера соединяемых инверторов определяются числами Фибоначчи. Если снять сигнал с каждого из инверторов и интерпретировать эти сигналы как двоичное число, то все возможные числа будут иметь одинаковое распределение (белый шум). Зафиксировав число в момент срабатывания clock-сигнала, получим истинно случайное число. Этот алгоритм также потребляет мало ресурсов.

Алгоритм Transition Effect RO-based (RO – Ring Oscillator). Источником случайного сигнала является элемент, представляющий собой два сложения по модулю 2,

где выходы из каждого из сложений подаются на вход другого, а на незадействованные входы подаётся одинаковый сигнал. Продолжительность колебаний зависит от симметрии структуры.

Алгоритм Multi-rings Oscillators. Несколько независимых кольцевых осцилляторов складывают свои значения по модулю два. Результат значения фиксируется с помощью D-триггера. Кольцевые осцилляторы состоят из разного (нечетного) количества инверторов, что обеспечивает разную задержку сигнала. Но количество используемых элементов выше в разы, чем у алгоритмов, представленных выше.

Для верификации всех представленных алгоритмов требуются тесты. Одним из стандартных тестирующих пакетов является NIST-пакет статистических тестов, разработанный Лабораторией информационных технологий, являющейся главной исследовательской организацией Национального института стандартов и технологий (NIST). В его состав входят 15 статистических тестов, целью которых является определение меры случайности двоичных последовательностей, порождённых либо аппаратными, как в нашем случае, либо программными генераторами случайных чисел. Эти тесты основаны на различных статистических свойствах, присущих только случайным последовательностям. Данный пакет позволит понять эффективность синтезируемого нами алгоритма.

Литература

1. *Danger J.-L., Guilley S., Hoogvorst P.* High Speed True Random Number Generator Based on Open Loop Structures in FPGAs, Elsevier, Microelectronics Journal. 2009.
2. *Vasyltsov E., Hambardzumyan Y., Kim S., Karpinskyy B.* Fast Digital TRNG Based on Metastable Ring Oscillator. // CHES. 2008.
3. *Golic J.*: New Methods for Digital Generation and Post-processing of Random Data. // IEEE TC 55(10), 2006.
4. *Sunar B., Martin W. J., Stinson D. R.*: A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks // IEEE TC. 2007.

УДК 004.056.53

Обеспечение целостности файлов журналов с помощью usb-накопителя с контролируемым доступом

Д.А. Эпиктетов[1], А.А. Алтухов[1, 2, 3]

[1]Московский физико-технический институт (государственный университет)
[2]Закрытое акционерное общество "ОКБ САПР"
[3]Национальный исследовательский ядерный университет «МИФИ»

Проблема защиты от кибератак является сегодня очень актуальной [1]. В частности, большую проблему представляют уязвимости нулевого дня [2]. С момента обнаружения такой уязвимости до момента, когда будут приняты меры по её устранению, риск взлома информационной системы повышается.

Для повышения защищённости могут использоваться такие методы, как тестирование на проникновение (пентестинг), внедрение принципов разработки безопасного программного обеспечения, своевременное обновление программного обеспечения. На конкретной системе возможна регулярная проверка открытых портов, запущенных процессов, списка пользователей, поиск руткитов специальными средствами и так далее. Такие меры могут помочь предотвратить вторжение, но, конечно, не являются стопроцентной гарантией защиты.

Что же делать, если предотвратить атаку всё-таки не удалось? В этом случае важно иметь как можно более полное представление о том, каким образом она была произведена, какое место в системе оказалось “слабым звеном” и кто именно её осуществил. Основной инструмент здесь – анализ журналов работы операционной системы и прикладного

программного обеспечения. Необходимость регистрации происходящих событий предписывается и нормативными документами [3–5]. Злоумышленник, не желая быть обнаруженным, может замести за собой следы, удалив или модифицировав эту информацию. Таким образом, приходим к необходимости защищать и сами журналы.

Предложим решение этой задачи с использованием резидентного компонента безопасности (РКБ) [6], вынесенного за пределы защищаемой системы. Будем использовать usb-накопитель с флеш-памятью, доступ к которой ограничивается специальным микроконтроллером, осуществляющим процедуры идентификации/аутентификации и производящим операции чтения и записи согласно с политикой безопасности. Устройство со схожей функциональностью существует – продукт “ПАЖ” компании ОКБ САПР [7]. Его можно использовать как базу для нового решения. Предоставим возможность записи информации в режиме append-only, таким образом удалить или модифицировать ранее записанные данные будет невозможно. Будем переносить журналы системы с определённой регулярностью на такое устройство, тогда задача их защиты сведётся к задаче защиты этого устройства, решать которую значительно проще. Отметим, что аналогичное решение было предложено ранее для решения другой задачи – хранения и передачи журналов средств доверенной загрузки [8, 9] .В том случае мы имели дело с логами, собираемыми в единое хранилище с большого количества устройств под управлением специализированной ОС, а устройство на базе ПАЖ играло роль среды передачи данных.

Для управления устройством ПАЖ разработана библиотека на языке С, с использованием которой написана программа, осуществляющая перенос журналов. Можно настроить регулярный запуск такой программы (например, с помощью cron в семействе ОС Linux). Пользователь ЭВМ, к которой подключается ПАЖ, имеет возможность сформировать список файлов, являющихся источниками логов (например, /var/log/syslog, /var/log/auth.log). При запуске программа переносит свежие (то есть те, которые были добавлены после последнего старта утилиты) записи из заданных источников на ПАЖ и обновляет дату последнего экспорта для каждого их них.

Отметим некоторые недостатки этого решения. Злоумышленник, получив необходимые права на защищаемой ЭВМ, сам может использовать программу переноса журналов и, таким образом, может заполнить память устройства мусорной или недостоверной информацией. Тем не менее возможность изменить записи, относящиеся ко времени до момента проникновения (точнее, до момента осуществления последнего перед проникновением экспорта журналов), у него отсутствует. При анализе журналов можно выявить этот момент и не считать записи, сделанные после него, корректными. Для этого нужно иметь на вооружении специальные аналитические алгоритмы. Ещё одна проблема заключается в необходимости физического доступа к ПАЖ для получения журналов с него в случае компрометации системы. Также нужно каким-то образом решать проблему заполнения памяти устройства.

Подведём итоги.

1. Предложен подход по повышению защищенности ЭВМ за счет обеспечения контроля целостности журналов с помощью специализированного ПАК.
2. Выбрана подходящая платформа и предложено решение на её основе
3. Предложена схема общего способа встраивания ПАК в состав систем.
4. Разработано ПО для ОС Linux, осуществляющее запись на ПАК.
5. Разработана схема встраивания в ОС Linux.
6. Выявлен ряд недостатков.

В дальнейшем планируется реализация переноса журналов с помощью специального драйвера ПАЖа, позволяющего осуществлять операцию записи на него. Также возможна реализация переноса журналов и для других операционных систем (в частности, для семейства Windows). Особое внимание будет посвящено анализу и устранению выявленных недостатков.

Литература

1. Kaspersky Security Bulletin 2016. Прогнозы на 2017 год: конец «Индикаторов заражения» [Электронный ресурс] URL: https://securelist.ru/files/2016/11/KSB_Predictions_2017_RUS.pdf (дата обращения 21.10.2017).
2. Отчёт. Угрозы и тенденции в области информационной безопасности 2016–2017 гг.
3. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [Электронный ресурс]. URL: https://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения 14.10.2017).
4. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/567 (дата обращения 24.03.2017).
5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/561 (дата обращения 24.03.2017).
6. *Конявский В.А*. Методы и аппаратные средства защиты информационных технологий электронного документооборота: диссертация доктора технических наук. М., 2005. 360 с.
7. Специальный съемный носитель информации: патент на полезную модель № 94751. 27.05.2010, бюл. № 15.
8. *Андреев В.М., Давыдов А.Н.* Безопасное хранение журналов работы СЗИ // Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. Минск: РИВШ, 2015. С. 49–52.
9. *Эпиктетов Д.А., Алтухов А.А.* Специальный съемный носитель как среда передачи журналов средств доверенной загрузки // Вопросы защиты информации, 2017. №3. С. 29–33.

УДК 004.056.5

Разработка системы защиты исполняемого кода с использованием технологии Intel SGX

А.М. Гладков, Р.К. Заводских, И.А. Левицкий

Московский физико-технический институт (государственный университет)

Введение

В настоящем проекте рассматривается задача защиты программного обеспечения, заключающаяся в сохранении в секрете исполняемого кода приложения. Целью является обеспечить доступ к пользованию приложением только полномочным пользователям и построить систему, противостоящую различным атакам. Более того, главной особенностью этой системы является то, что даже при получении полных прав доступа к компьютеру, на котором выполняется приложение, злоумышленник не имеет возможности запустить приложение без надлежащей аутентификации или получить его ассемблерный код.

Программным приложениям зачастую приходится работать с конфиденциальной информацией: с паролями, номерами счетов, финансовыми данными. Доступ к этим данным должен быть только у полномочных получателей. Эти секретные данные не должны быть непреднамеренно раскрыты другим пользователям или приложениям. Применение политики безопасности для этих данных на компьютере является задачей операционной системы. В приложениях также часто используются дополнительные защитные меры, чтобы предотвратить доступ третьим лицам к данным, даже если злоумышленнику удалось получить доступ к ОС или к пользовательскому оборудованию.

Если говорить о защите исполняемого кода, на сегодняшний день есть определённый спектр методов защиты, направленных на усложнение реверс-инжиниринга готового продукта. Основной проблемой является то, что конечный продукт может запускаться в среде, в которой присутствует более привилегированный процесс, способный прочитать виртуальную память нужной программы. Частично эта проблема решается удалением у защищаемого участка виртуальной памяти флага на чтение, и в таком случае gdb не сможет в дальнейшем прочитать её. Но эта мера не способна защитить ни от

обычного дампа исполняемого файла, ни от ситуации, когда сама операционная система является скомпрометированной, то есть имеющей возможность читать адресное пространство секретного исполняемого кода.

Описание технологии Intel SGX

В целях возможности создания программ, обеспечивающих высокоуровневую защиту секретных данных, корпорацией Intel была разработана технология Intel Software Guard Extensions, или Intel SGX. Intel SGX представляет собой набор инструкций ЦП, предоставляющих возможность приложению создавать анклавы – области в виртуальном адресном пространстве, защищенные от чтения и записи извне этой области, в том числе другими процессами и ядру ОС.

Этапы создания анклава следующие: внутри будущего анклава выделяется участок памяти, в него загружается код программы, и в заключение происходит инициализация анклава. После последнего действия возможность получить извне доступ к памяти анклава напрямую пропадает. Теперь, по замыслу создателей технологии, при помощи специальных функций-мостов в анклав можно загружать данные, которым необходимо обеспечить защиту.

Постановка и решение задачи

Проблема, решаемая нами в данной работе, состоит в том, что технология Intel SGX подразумевает защиту данных, но не исполняемого кода. По предположению, что память анклава закрыта от чтения и записи из недоверенных участков после инициализации, конкретные исполняемые анклавом инструкции тоже засекречены. Но до инициализации код анклава помещается в память ещё в открытом виде, и его можно беспрепятственно прочитать. Так как целью является сохранение исполняемого кода в секрете, необходимо разработать алгоритм, предотвращающий описанный сценарий.

Для решения предлагается следующая клиент-серверная архитектура. Имеется сервер разработчика ПО; в обязанности сервера входит шифрование секретного кода и передача его клиентской части. Клиент запускает загрузчик приложения - часть программы, отвечающую за авторизацию пользователя на сервере и дальнейшего получения прав на запуск программы. В случае успешной авторизации создается анклав и сервер строит с загрузчиком закрытый канал связи. По каналу сервер посылает зашифрованный код, загрузчик передает код в анклав, где происходит его расшифровка. После этого управление передается расшифрованному коду.

Литература

1. *John M., Benjamin O.* Intel Software Guard Extensions Tutorial Series // Intel Software Developer Zone, 2016.
2. *Matthew H*. Intel® SGX for Dummies (Intel® SGX Design Objectives) // Intel Software Developer Zone, 2015.
3. *Ittai A.* [*et al.*]. Innovative Technology for CPU Based Attestation and Sealing // Intel Software Developer Zone, 2013.
4. Software Guard Extensions Programming Reference // Intel Software Developer Zone, 2014.

УДК 004.94

Исследование применения кодовых методов к задаче стеганографии на базе файловой системы

Г.А. Мельников[1], Э.А. Казиахмедов[1], К.С. Киреев[1], В.С. Потапова[2,3]

[1]Московский физико-технический институт (государственный университет)
[2]Сколковский институт науки и технологий
[3]Институт проблем передачи информации им. А.А. Харкевича РАН

Стеганография ставит перед собой цель скрывать и передавать сообщения таким образом, чтобы не было известно о факте передачи. Иными словами, в объект (контейнер) сообщение встраивается так, что модифицированный объект практически неотличим от

оригинала. В данной работе в качестве контейнеров рассматривались цифровые изображения. Необходимо было гарантировать корректное извлечение сообщения и вместе с тем в исходном изображении делать как можно меньше изменений, сохраняя всю значащую информацию об оригинале [1].

Известны методы стегоанализа, которые могут определить наличие сообщения в изображении, если оно встраивалось непосредственно в цветовой канал пикселя. Это, как правило, статистические методы, основанные на предположениях о распределении значений наименее значимых битов пикселей (LSB) [2]. В нашем случае схема использует JPEG-изображения, и сообщение встраивается в частотную область. Кроме того известно, что использование кодов Хэмминга позволяет делать меньшее количество изменений в контейнере при встраивании сообщений, чем обычное встраивание изменением наименее значимых битов [3], [4]. Все это, в свою очередь, уменьшает вероятность обнаружения информации. Помимо этого, отличительной особенностью данной работы от существующих решений является возможность разворачивания полноценной файловой системы на базе данного цифрового формата. Полезная информация распределяется по всем графическим файлам, тем самым существенно усложняя задачу статистического анализа. Использование файловой системы предоставляет простой интерфейс взаимодействия с конечным пользователем.

Приведем пример работы схемы на этапе непосредственного встраивания. Допустим, что в контейнер $x=(1001000)$ встраивается сообщение $m=(110)$. Для этого мы считаем синдром контейнера $s = Hx^T$, где H – матрица Хэмминга (размера 3 × 7):

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad (1)$$

$$H \cdot x^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \quad (2)$$

В нашем примере $s=(101)$. Далее мы вычисляем $s+m$ в поле F_{2^3}, (получаем $r=(011)$) и меняем в контейнере соотвествующий бит:

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}. \quad (3)$$

В рассматриваемом примере это 3-й бит, и модифицированный контейнер имеет вид $x'=(1011000)$. Таким образом, мы встроили три бита, изменив всего один символ в контейнере. Извлечение же сообщения состоит в вычислении синдрома модифицированного контейнера:

$$H \cdot x'^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = m^T. \quad (4)$$

Итак, перейдем к описанию схемы. Итоговая последовательность действий имеет следующий вид:

6. для блоков пикселей вычисляются матрицы коэффициентов дискретного косинусного преобразования (DCT), далее происходит квантование коэффициентов (эти шаги повторяют JPEG-сжатие). Значения полученных DCT-коэффициентов могут отличаться для разных реализаций данного преобразования. Поэтому для решения задачи стеганографии важно использовать тот же алгоритм, что использовался для генерации JPEG-изображения. В нашем случае – это реализация, предоставляемая библиотекой libjpeg (данная библиотека используется для создания скриншотов и т. д.);
7. для встраивания полезной информации выбираются DCT-коэффициенты, больше некоторого ненулевого числа, т.к. изменение нулевых коэффициентов приведет к увеличению размера исходного изображения. Запись в данные коэффициенты происходит в порядке, заданном псевдослучайной последовательностью, которая генерируется по заданному ключу (для извлечения информации необходим тот же ключ);
8. сообщение встраивается с помощью кода Хэмминга в наименее значащие биты коэффициентов. Как сказано в предыдущем пункте, последние биты DCT-коэффициентов выстраиваются в порядке некоторой псевдослучайной последовательности. В памяти данные биты хранятся линейно, т.е. каждый байт массива хранит 8 полученных значащих бит последовательности. Каждые 2^k–1 бит последовательности — это контейнер (см. схему работы кодов Хэмминга выше), в который будет встраиваться k бит полезной информации (сообщение *m* из примера). Параметр кода k можно задать при компиляции программы.
9. после встраивания продолжается JPEG-сжатие, а именно сжатие Хаффмана.

Кроме того, нужно отметить, что в ходе этой процедуры изображение теряет так называемые метаданные (markers). Так что необходимо специально извлекать их перед началом процедуры встраивания и после накладывать на модифицированное изображение. Тесты показывают, что это не мешает последующему извлечению сообщения.

Работа Потаповой В.С. выполнена при финансовой поддержке РФФИ (проект 16-01- 00716).

Литература

1. *Fabien A., Petitcolas P.* Information Hiding Techniques for Steganography and Digital Watermarking London: Artech House, 2000. 220 p.
2. *Arooj Nissar, A.H. Mir* Classification of steganalysis techniques: A study // Digital Signal Processing, Volume 20, Issue 6, 2010. P. 1758–1770.
3. *Ron Crandall* Some Notes on Steganography // Steganography Mailing List, 1998. P. 12–18.
4. *F. Galand, G. Kabatiansky* Information hiding by coverings // Proceedings of Information Theory Workshop, 2003. P. 1–5.

УДК 519.725

О применении обобщенных весов Хэмминга к построению новых верхних границ для кодов с локальным восстановлением

С.А. Круглик[1,2,3], К.Н. Назирханова[1,3], А.А. Фролов[2,3]

[1]Московский физико-технический институт (государственный университет)
[2]Сколковский институт науки и технологий
[3]Институт проблем передачи информации им. А. А. Харкевича РАН

Кодами с локальным восстановлением (LRC) называют такие коды над конечным алфавитом, что каждый символ является функцией небольшого числа других символов, называемых восстанавливающими множествами (мощность данных множеств обозначим через *r*) [1]. Данные коды имею важное приложение применительно к системам

распределенного облачного хранения и хорошо исследованы в литературе. Известны хорошие верхние и нижние границы на кодовое расстояние и скорость, ровно, как и конструкции оптимальных кодов для больших алфавитов [2], [3].

Естественным обобщением является рассмотрение случая с несколькими не пересекающимися множествами для каждого кодового символа, называемое кодами с локальным восстановлением и доступностью. Данное свойство позволяет обрабатывать множественные запросы к временно недоступному серверу параллельно и особенно важно в приложении к т.н. «горячим данным», одновременно запрашиваемых множеством пользователей. Данный случай является наименее исследованными в литературе, и мы знаем лишь грубые верхние и нижние границы, а также тривиальные конструкции [4, 5, 6].

В недавней совместной работе Вэбэра и Абдель-Гафара было рассмотрено применение обобщенных весов Хэмминга для улучшения известных границ на кодовое расстояние некоторых разновидностей кодов с локальным восстановлением [7]. В данной работе этот подход применен для улучшения границ на кодовое расстояние кодов с локальным восстановлением и доступностью, полученных в работе [8]. В результате получаем следующую границу на -й $(1 \le \kappa \le k - rt)$ обобщенный вес Хэмминга кода с локальностью r и доступностью t (когда каждый кодовый символ имеет t непересекающихся восстанавливающих множеств):

$$d_\kappa \le \min_{1 \le s \le \lfloor \frac{k-1-\kappa}{r-1} \rfloor} n - k - s + \kappa.$$

Применение оценки на -й обобщенный вес Хэмминга из работы [9] и минимизация по s дает следующую границу на кодовое расстояние кода с локальностью r и доступностью t:

$$d \le \frac{q^\kappa - q^{\kappa - q}}{q^\kappa - 1}(n - k - \lfloor \frac{k-1-\kappa}{r-1} \rfloor + \kappa).$$

Работа Круглика С.А. выполнена при при финансовой поддержке РФФИ (проект 16-01-00716).

Литература

1. *Tamo I. and Barg A.* A family of optimal locally recoverable codes // IEEE Trans. Inf. Theory, 2014. V. 60. N 8. P. 4661–4676.
2. *Tamo I., Barg A. and Frolov A.* Bounds on the parameters of locally recoverable codes // IEEE Trans. Inf. Theory, 2016. V. 62. N 6. P. 3070–3083.
3. *Rawat A. S., Koyluoglu O. O. and Vishwanath S.* Optimal locally repairable codes via rank-metric codes // Proc. IEEE Int. Symp. Inf. Theory (ISIT), 2013. P. 1819–1823.
4. *Tamo I., Barg A.*Bounds on locally recoverable codes with multiple recovering sets // Proc. IEEE Int. Symp. Inf. Theory, Honolulu, HI, USA, Jun./Jul. 2014. P. 691–695.
5. *Huang P., Yaakobi E., Uchikawa H. and Siegel P.H.* Linear locally repairable codes with availability // Proc. IEEE Int. Symp. Inf. Theory, Hong Kong, Jun. 2015. P. 1871–1875.
6. *Kruglik S. and Frolov A.* Bounds and Constructions of Codes with All-Symbol Locality and Availability // Proc. IEEE Int. Symp. Inf. Theory, Aachen, 2017. P. 1023–1027.
7. *Abdel-Ghaffar K.A.S. and Weber J.H.* Bounds for Cooperative Locality Using Generalized Hamming Weights // Proc. IEEE Int. Symp. Inf. Theory, Aachen, 2017. P. 699–103.
8. *Helleseth T., Klove T., and Ytrehus O.* Generalization of the Griesmer bound // Error Control, Cryptography, and Speech Compression. New York, NY, USA: Springer-Verlag, 1994. V. LNCS 829. P. 41–52.

УДК 003.26

Применение технологии цифрового маркирования в потоковом видео, кодированном стандартом H264/AVC в B-кадрах

А. Ю. Городилов

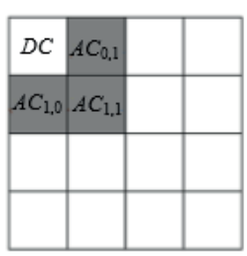
Московский физико-технический институт (государственный университет)
Лаборатория мультимедийных систем и технологий

В настоящее время остро стоит вопрос сохранения авторских прав при распространении контента. Существует множество способов цифрового маркирования неподвижных изображений и потокового видео для дальнейшего установления авторства контента. Необходимым условием использования алгоритмов внедрения цифровых водяных знаков (ЦВЗ) является незаметность и устойчивость к атакам третьих лиц. В данной работе рассматривается метод внедрения цифрового водяного знака в потоковое видео, кодированное стандартом H.264/AVC. Данный стандарт и его продолжение H.265/HEVC являются наиболее популярными кодеками в области высокоэффективного сжатия видеоданных.

В работах [1–3] были рассмотрены методы внедрения ЦВЗ в значения векторов движения, коэффициентов блоков предсказания в режиме INTER.

В данной работе предлагается внедрение ЦВЗ в цветоразностные блоки B кадров. Цифровой водяной знак представляет собой набор бит, или паттерн, распределенный определенным образом по кадру. Внедрение происходит в различные коэффициенты дискретно косинусного преобразования. Рассматривается изменение как DC, так и AC коэффициентов с различной степенью интенсивности. Основной задачей внедрения ЦВЗ является исключить возможность извлечения и устранения его третьими лицами, не обладающими секретной информацией (ключом). В качестве секретной информации используются параметры внедрения бит: положение изменяемых коэффициентов в блоке, положение блоков с изменяемыми коэффициентами в кадре, изменяемые компоненты U или V. Набор этих параметров генерируется криптографически стойким генератором псевдослучайной последовательности чисел (КСГПСПЧ). Изменения коэффициентов в блоке происходит по следующему правилу:

$$\left|AC_{i,j} - AC_{i+1,j}\right| = \begin{cases} -D, & bit = 1, \\ D, & bit = 0, \end{cases}$$



где, i и j – координаты AC коэффициентов в блоке. D – параметр разноса их значений, определяющий стойкость ЦВЗ к атакам сжатия. Либо:

$$DC = \begin{cases} DC - D, & bit = 1, \\ DC + D, & bit = 0. \end{cases}$$

Также в работе представлены результаты измерений SNR полученных изображений с внедренным ЦВЗ в B кадры при различных параметрах. На рис. 1 показана последовательность I-B-P кадров после внедрения ЦВЗ и разница, по сравнению с оригинальным B кадром. Основным критерием оценки метода при внедрении в ЦВЗ является его незаметность на общем фоне изображения. Для этого собираются субъективные оценки искажения видеоданных от нескольких человек, и учитывается объективный параметр PSNR. Также оценивается степень устойчивости ЦВЗ при

различных атаках: масштабирование, обрезание и сжатие видеопоследовательности.

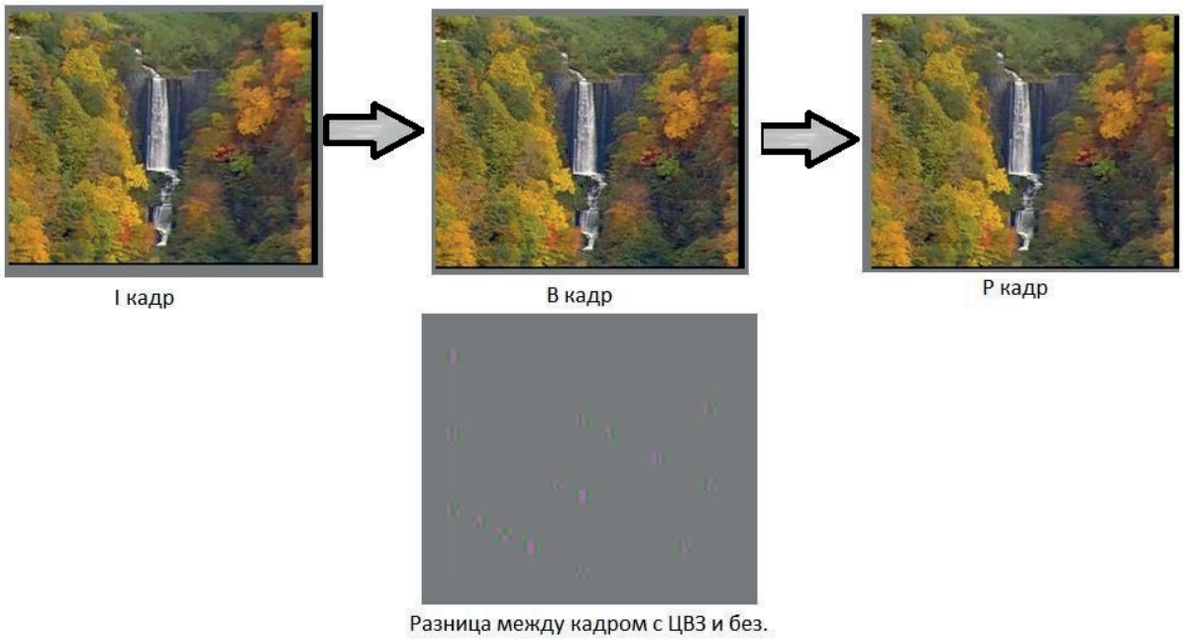


Рис. 1. Внедрение ЦВЗ в B кадр

Литература

1. *Xinghao Jiang, Tanfeng Sun, Yue Zhou, Wan Wang, Yun-Qing Shi.* A Robust H.264/AVC Video Watermarking Scheme with Drift Compensation //The Scientific World Journal. Volume 2014, Article ID 802347.
2. *Thomas Stutz, Florent Autrusseau, Andreas Uhl Inter-Frame* H.264/CAVLC Structure-Preserving Substitution Watermarking// LUNAM Universit´e de Nantes, France. Technical Report 2013-02. April 2013
3. Григорьян А. К., Аветисова Н. Г. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор // Информационно-управляющие системы. № 2, 2010. С. 38.
4. И. Гук. Особенности сжатия видеоданных по рекомендации H.264 // Компоненты и Технологии. №2, 2006.

УДК 004.056.55

Использование модифицированной (U|U+V)-конструкции в криптосистеме McEliece

А.А. Красавин

Московский физико-технический институт (государственный университет)

Криптосистема McEliece может быть описана следующим образом [1].

Для генерации ключа выбирается линейный q-ичный (n, k, d)-код $\boldsymbol{C}$ с порождающей матрицей G, для которого известен эффективный алгоритм декодирования ошибок, весом не более t. Выбираются случайные невырожденные $k \times k$ матрица S и $n \times n$ перестановочная матрица P. В качестве открытого ключа системы публикуется матрица $\bar{G} = SGP$. Закрытым ключом системы являются алгоритм декодирования кода $\boldsymbol{C}$ и матрицы S, и P.

Для шифрования сообщения m, представленного в виде q-ичного вектора длины k выбирается случайный q-ичный вектор e длины n веса не более t. Шифротекст рассчитывается по формуле:

$$c = m\bar{G} + e. \quad (1)$$

Для расшифрования сообщения с пользователь вычисляет $\bar{c} = cP^{-1}$, декодирует $\bar{c}$ алгоритмом декодирования для кода $\boldsymbol{C}$: $\bar{c} \to \{\bar{x}, \bar{e}\}$: $\bar{c} = \bar{x}\bar{G} + \bar{e}$ и получает $m = \bar{x}S^{-1}$.

Оригинальная криптосистема McEliece была построена на кодах Гоппы [1]. В последствии для увеличения скорости работы или уменьшения размеров ключей криптосистемы было предложено использовать другие коды, например коды Рида–Маллера [2], обобщенные коды Рида–Соломона [3], LDPC-коды [4] и другие. Однако для многих из предложенных схем были найдены атаки на структуру матрицы $\bar{G}$, позволяющие вычислить закрытый ключ из открытого. Все эти атаки использовали различные особенности данных кодов. Так, атаки на криптосистему McEliece, построенную на кодах Рида–Маллера [5] или на полярных кодах [6], использовали для атаки поиска слов кода минимального веса.

Для защиты от подобных атак в работах [2], [7] было предложено использовать (U|U+V)-конструкцию и ее модификации. Недостатком предложенных конструкций является значительное увеличение размера ключа.

Предложена модификация (U|U+V)-конструкции, которая позволяет получить меньший размер ключа в криптосистеме McEliece:

Пусть $\boldsymbol{C}$ – (n, k, d) q-ичный код с порождающей матрицей G и эффективным алгоритмом декодирования ошибок веса менее t. Пусть A и K – случайные матрицы размером $k \times L$ и $L \times n$ соответственно.

Код $\overline{\boldsymbol{C}}$, заданный порождающей матрицей $\bar{G} = \binom{G}{K}$, – $(n, k, +L, d_0 \le d)$-код. Показано, что возможно задать K так, что $d_0 \ge d/2$. Этого можно добиться, например, если взять все строки матрицы K случайными векторами веса $d/2$.

Если B – порождающая матрица случайного $(d - d_0 + L + 1, L, d_J = \left\lfloor \frac{d-d_0+1}{2} \right\rfloor)$ кода, то код $\boldsymbol{D}$, заданный порождающей матрицей $J = \begin{pmatrix} G & AB \\ K & B \end{pmatrix}$, может исправить не менее t ошибок по следующему алгоритму декодирования.

Пусть принято сообщение $c = xJ + e, wt(e) \le t$.

1. c представляется в виде: $c = (z^1|z^2)$, длина z^1 равна n;
2. перебираются все вектора e_i – q-ичные последовательности длины L;
3. для каждого e^i вычисляется $v^i = z^1 - e_i K$;
4. v^i декодируется по алгоритму для кода $\boldsymbol{C}$: $v^i = u_i G + \xi^i, wt(\xi^i) \le t$.
5. если вес вектора $\xi = (\xi^i|(z^2 - (u_i A - e_i))B)$ меньше t, то $x = (u_i|e_i), e = \xi$, иначе повторяются п.п.2–5.

Решение всегда существует и единственно, а данный алгоритм декодирования в q^L раз хуже алгоритма декодирования кода $\boldsymbol{C}$.

Способ построения кода $\boldsymbol{D}$ из $\boldsymbol{C}$ назван KA-схемой.

Подкод $\boldsymbol{D_1}$ кода $\boldsymbol{D}$, заданный порождающей матрицей $J_1 = (G + AK \quad AB)$, может исправить не менее *t* ошибок по следующему алгоритму декодирования:

Пусть принято сообщение $c = xJ_1 + e, wt(e) \le t$.

1. c представляется в виде: $c = (z^1|z^2)$, длина z^1 равна n;
2. перебираются все вектора e_i – q-ичные последовательности длины L;
3. для каждого e^i вычисляется $v^i = z^1 - e_i K$;
4. v^i декодируется по алгоритму для кода $\boldsymbol{C}$: $v^i = u_i G + \xi^i, wt(\xi^i) \le t$.
5. если вес вектора $\xi = (\xi^i|(z^2 - u_i A)B)$ меньше t, то $x = u_1, e = \xi$, иначе повторяются пп.2-5.

При использовании кода, построенного при помощи предложенной KA-схемы, в криптосистеме McEliece, структурные атаки на систему будут невозможны без решения сложной задачи – отделения столбцов матриц G от AB и слов кода $\boldsymbol{C}$ от слов $\bar{c} = c + k, c \in \boldsymbol{C}, k \in \boldsymbol{K}$, где $\boldsymbol{K}$ – множество, состоящее из строк матрицы K.

Предложен способ уменьшения размера ключа в криптосистеме McEliece, построенной при помощи KA-схемы, заключающийся в модификации схемы и алгоритмов шифрования и расшифрования следующим образом:

Пусть $\boldsymbol{C}$ – (n, k, d) q-ичный код с порождающей матрицей G и эффективным алгоритмом декодирования ошибок веса менее t. Для генерации ключей выбираются случайные матрицы A и K размером $k \times L$ и $L \times n$ соответственно, случайные невырожденные матрицы S и P, размером $k \times k$ и $n \times n$ соответственно. Выбирается криптографически стойкая хэш-функция $h(\cdot)$.

В качестве открытого ключа публикуется матрица $\bar{G} = S(G + AK)P$ и хэш-функция $h(\cdot)$.

Для шифрования сообщения m, представленного в виде q-ичного вектора длины k выбирается случайный q-ичный вектор e длины n веса не более t. Шифротекст рассчитывается по формуле:

$c = (m\bar{G} + e \mid h(m \mid e))$.

Для расшифрования сообщения c:

1. вычисляется $\bar{c} = cP^{-1} = (c_1|c_2)$, длина c_1 равна n;
2. перебираются все вектора e_i – q-ичные последовательности длины L;
3. для каждого e^i вычисляется $d_i = c_1 - e_i K$;
4. d_i декодируется по алгоритму для кода $\boldsymbol{C}$: $d_i = x_i G + \xi_i, wt(\xi_i) \leq t$.
5. если $c_2 == h(x_i, \xi_i)$, то вычисляется $m = x_i S^{-1}$, иначе повторяются пп.2-5.

Литература

1. *McEliece R.J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report, Jet Propulsion Laboratory, Pasadena. 1978. P. 114–116.
2. *Sidelnikov V.M.* A public-key cryptosytem based on ReedMuller codes // Discrete Math. Appl. 1994, 4(3). P. 191–207
3. *Niederreiter H*. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Problems of Control and Information Theory. 1986. V. 15. N 2. P. 159–166.
4. *Baldi M., Chiaraluce F.* Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes // Proc. IEEE Int. Symposium Inf. Theory – ISIT. 2007. P. 2591–2595.
5. *Minder L., Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // Advances in Cryptology - EUROCRYPT 2007. 2007. V. 4515 of Lecture Notes in Comput. Sci. P. 347–360.
6. *Bardet M., Chaulet J., Dragoi V., Otmani A., Tillich J.P.* Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes. Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. 2016. P. 118–143.
7. *Irene Marquez Corbella, Jean-Pierre Tillich*. Attaining capacity with iterated (U|U + V) codes based on AG codes and Koetter-Vardy soft decoding. ISIT 2017. 2017. P. 6-10.

УДК 004.94

Исследование механизмов построения криптовалют с использованием новых типов доказательств выполнения работы

Г.В. Балицкий[1,2], А.И. Дзись[1,2], Н.М.Козырский[1,3], Г.А.Чирков[1]

[1]Московский физико-технический институт (государственный университет)
[2]Институт проблем передачи информации РАН
[3]Институт радиотехники и электроники РАН

Bitcoin – электронная платежная система, разработанная Сатоси Накамото, и получившая широкую огласку в прессе в 2011 г. До этого года все операции с валютой требовали взаимодействия с доверенными лицами: банками, платежными системами, ЦБ и др. Однако вопрос о благонадежности данных организаций не имеет очевидного ответа. Bitcoin решает данную проблему, используя Blockchain – технологию, реализующую распределенную базу данных, поддержка которой не требует наличия доверенных лиц. Этот фактор привел к взлету популярности и курса валюты в 2013.

В основе блокчейна лежит идея «доказательства выполнения работы» (Proof-of-Work, PoW), изложенная в 1993 году в статье [1]. Концепция PoW такова**:** для доступа к общим ресурсам пользователю необходимо выполнить достаточно сложную задачу, решаемую за приемлемое время, и таким образом ограничить количество доступов

пользователя к данным. Основное требование к задаче состоит в том, что работа, выполняемая пользователем, должна быть гораздо более трудоемкой, чем проверка результата серверной частью.

В протоколе Bitcoin в качестве PoW используется следующая задача: при заданном d найти такое число r, что

$$SHA256(SHA256(r)) < d \quad (1) \qquad (1)$$

где SHA256 – это хеш-функция, полная спецификация которой доступна в статье [2]. Очевидно, подбор r является значительно более ресурсоемкой задачей, чем проверка выражения (1). Главная проблема такого PoW состоит в том, что решение подобной задачи нужно только лишь для доказательства работы. Возникает вопрос: существуют ли такие задачи, которые можно использовать в качестве PoW, и результат которых можно переиспользовать для решения каких-либо сторонних задач?

Первым ответом на поставленный вопрос стала криптовалюта Primecoin, описанная в [3]. Главным ее отличием от криптовалюты Bitcoin стало то, что в ней, в качестве PoW, используется задача нахождения простых чисел особого типа. Таким образом, преимущество Primecoin заключается в том, что результат решения задачи может быть повторно использован в каких-то других целях, отличных от доказательства работы. Такой класс задач, имеющих все вышеназванные свойства PoW, называется полезным доказательством работы (useful Proof of Work, uPow). В 2017 году в статье [4] были предложены несколько различных типов задач, таких как 3SUM, All-Pairs Shortest Path, которые можно использовать в качестве uPoW.

В данной работе была рассмотрена практическая реализация криптовалюты uCoin на основе uPoW. В качестве uPoW был использован метод, описанный в [4], который заключается в использовании высокой вычислительной сложности задачи поиска «k-ортогональных векторов», принадлежащих k разным множествам, и малой сложности проверки результата для выполнения функций PoW. Решение этой задачи имеет практическую ценность. Также был проведен сравнительный анализ uCoin с такими известными криптовалютами как Bitcoin и Primecoin.

Литература

1. *Dwork C., Naor M.* Pricing via processing or combatting junk mail / Ernest F. Brickell, editor // Advances in Cryptology - CRYPTO ’92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992, Proceedings, V. 740 of Lecture Notes in Computer Science, P. 139–147. Springer, 1992.
2. *Gilbert H., Handschuh H.* Security Analysis of SHA-256 and Sisters // Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003. Ottawa, 2003.
3. *King, Sunny* Primecoin: Cryptocurrency with Prime Number Proof-of-Work, 2013.
4. *Ball M., Rosen A., Sabin M., Vasudevan P.N.* Proofs of Useful Work // IACR, 2017.

УДК 004.94

Исследование применения «отслеживаемых» кодов на основе IPP кодов для задачи защиты цифрового контента на примере изображений

А.Г. Бауман[1], К.Н. Назирханова[1,2], Е.А. Сайгина[1], Н.Д. Скуратов[1,2]

[1]Московский физико-технический институт (государственный университет)
2Институт проблем передачи информации им. А.А. Харкевича РАН

Защита цифрового контента является одной из наиболее бурно развивающихся отраслей защиты информации. Интерес в данной области обусловлен необходимостью для правообладателей защитить объекты своего авторского права, размещенные в сети Интернет, от контрафакции. На данный момент существует множество различных способов борьбы с незаконным использованием продуктов, один из которых заключается в создании системы для зарегистрированных пользователей, где цифровой контент хранится в зашифрованном виде.

Схемы, позволяющие отследить «пиратов», были предложены в [1]. Их идея заключается в том, что если коалиция злоумышленников конечного размера создает устройство для неавторизованного пользователя, тогда можно идентифицировать хотя бы одного из ее участников. Для этого дистрибьютор шифрует данные с помощью сессионного ключа k, а всем авторизованным пользователям предоставляет персональные ключи для расшифровки. С целью создания неавторизованных ключей для дешифрования некоторая коалиция злоумышленников создает связку ключей, основанную на их общем знании ключей. Если мы предполагаем, что мощность коалиции не превышает t, то тогда в случае обнаружения неавторизованного ключа, дистрибьютер должен уметь отследить хотя бы одного злоумышленника. Данные схемы могут быть «открытыми» или «секретными». Одним из классов «открытых» схем являются коды со свойством идентифицирования «родителя» или IPP коды (Identifiable Parent Property). Один из частных случаев называется «отслеживаемыми» кодами, описанными в [2, 3] и более детально изучен в [4–6]. Эти коды были применены в данной работе для защиты цифрового контента.

В свою очередь мы разработали программный продукт, способный шифровать изображения и создавать ключи для авторизованных пользователей, основанные на схеме построения «отслеживаемых» кодов. Благодаря свойству данного семейства кодов, при обнаружении нелегальной «связки ключей» правообладатель сможет предотвратить незаконное применение своего продукта.

В результате исследования созданной нами системы мы установили, что при создании авторизованным пользователем незарегистрированного набора ключей всегда есть возможность восстановить основополагающую «связку», тем самым найти злоумышленника и привлечь его к ответственности за несоблюдение лицензионного соглашения.

Литература

1. *Chor B., Fiat A., Naor M*. Tracing traitors // Desmedt Y.G. (ed.) CRYPTO 1994. LNCS, V. 839, P. 257–270. Heidelberg: Springer, 1994.
2. *Egorova E., Kabatiansky G.* Analysis of Two Tracing Traitor Schemes via Coding Theory / Barbero Á., Skachek V., Ytrehus Ø. (eds) // Coding Theory and Applications. ICMCTA 2017. Lecture Notes in Computer Science, V. 10495. Springer, Cham.
3. *Lindkvist T., Lofvenberg J., Svanstrom M.* A class of traceability codes // IEEE Transactions on Information Theory. 2002. V. 48, I. 7.
4. *Barg A., Cohen G., Encheva S., Kabatiansky G., Z´emor G.* A hypergraph approach to the identifying parent property: the case of multiple parents // SIAM J. Discrete Math. 2001. 14(3). 423–431.
5. *Alon N., Cohen G., Krivelevich M., Litsyn S.* Generalized hashing and parent-identifying codes // J. Comb. Theor. Ser. A. 2003. 10(1). 207–215.
6. *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes // IEEE Trans. Inf. Theor. 2001. 47. 1042–1049.

УДК 004.94

Исследование вопросов сохранения конфиденциальности пользовательской информации при работе с базами данных

Б.Н. Широких[1,2], М.А. Паутов[1,2], Л.В. Щелкун[1]

[1]Московский физико-технический институт (государственный университет)
[2]Институт проблем передачи информации им. А.А. Харкевича РАН

С развитием ИТ-индустрии все большее значение принимают задачи защиты информации. Одной из главных парадигм информационной безопасности является сохранение конфиденциальности баз данных, например, при построении рекомендательных систем [1] или в избирательной системе. В данной статье рассматривается одна из возможных прикладных задач в работе с базой данных – задача классификации данных, с требованием сохранения конфиденциальности информации

(анализ данных с дифференциальной приватностью [2]). Соблюдение конфиденциальности подразумевает, что функция, определенная на произвольной выборке из базы данных (рандомизированное вычисление [2]), практически не чувствительна к изменениям в любой отдельно взятой записи, что фактически предотвращает утечку информации при обращении к базе данных. Однако подобные ограничения могут привести к значительным снижениям качества классификации.

Решение поставленной проблемы начинается с построения алгоритма классификации и оценки ошибки в постановке задачи обучения с учителем (рассматривается алгоритм построения решающих деревьев [3, 4] и его вариации). Следующим шагом необходимо минимизировать необратимое снижение точности классификации на зашумленных данных по сравнению с работой над исходной базой данных. Наиболее интересным аспектом является нахождение оптимальной точности, достигаемой алгоритмом при варьировании связанных собой параметров размера выборки данных и уровня шума (трейд-офф между уровнем шума и размером выборки [5]). А также предлагается эффективный подход к последовательным обращениям к базе данных при построении решающих деревьев, ведь количество запросов ограничено параметром бюджета приватности [2].

При формальной постановке математической задачи в работе возникают следующие определения.

Определение 1. Мультимножество – это обобщение понятия множества, допускающее включение одного и того же элемента по нескольку раз.

В нашем случае под исходным множеством понимается набор элементов из базы данных.

Определение 2. Симметрическая разность (двух множеств) – теоретико-множественная операция, результатом которой является новое множество, включающее все элементы исходных множеств, не принадлежащие одновременно им обоим.

Симметрическая разность для двух заданных множеств равная единице далее будет обозначать, что они отличаются ровно на один элемент.

Пусть $M : A \to \mathbb{R}^d$ – функция определенная на мультимножестве A и возвращающая некоторое значение из d-мерного вещественного векторного пространства. Рандомизированность этой функции следует понимать в смысле зависимости от случайной величины.

Определение 3. Будем говорить, что рандомизированная функция M обеспечивает приватность уровня ε, если для любых двух мультимножеств A и B с симметрической разностью $A \Delta B = 1$ верно $\Pr[M(A) \in S] \le \Pr[M(B) \in S] \times e^{\varepsilon}$ для любого возможного $S \subseteq \mathrm{Range}(M)$.

Вероятность отнести значение функции к определенному подмножеству исходов S определена в классической постановке, как отношение всех равновероятных элементарных исходов к числу всех возможных в S, так как количество исходов конечно.

Определение 4. Для функции $f : D \to R^d$, определенной на произвольном множестве D, чувствительность вводится как значение следующего выражения: $S(f) = \max_{A \Delta B = 1} \left\| f(A) - f(B) \right\|_1$.

Построение рандомизированной функции $M(X)$ подразумевает наличие интерфейса с дифференциальной приватностью. Совершая запрос к базе данных, пользователь получает значение функции на подвыборке данных, к которым он обращается. Наиболее простым и распространенным способом является составление функции из двух частей: детерминированной функции $f(X)$, определенной на множестве подвыборок базы данных, и случайной величины (шума), накладываемого поэлементно поверх датасета.

Мы воспользуемся тем же подходом, что и [5], и выберем в качестве шума случайную величину из многомерного распределения Лапласа, зависящую от чувствительности некоторой детерминированной функции и от уровня приватности.

Утверждение. Для фиксированной функции $f : D \to R^d$ выражение $M(X) = f(X) + (Laplace(S(f) / \varepsilon)^d$ обеспечивает приватность уровня ε.

Примером такой детерминированной функции f (одной из реализованных в нашей работе) является правило, которое подмножеству элементов, принятому на вход, ставит в соответствие новый элемент пространства R^d, у которого каждая характеристика (признак) равна сумме соответствующих характеристик аргументов. Нетрудно заметить, что чем больше элементов базы данных будет просуммированно, тем меньше будет относительная дисперсия шума при разбросе, и количество полученных пользователем элементов будет уменьшаться. Соответственно, возникает формальная постановка задачи поиска оптимума для точности классификации между количеством элементов в выборке и уровнем шума.

Базой, на которой строится решающий алгоритм, служит, как было упомянуто ранее, бинарное решающее дерево. Основной идеей для модификации алгоритма является использование заново запрошенных данных на каждом уровне дерева. Так как рандомизированная функция каждый раз возвращает «зашумленные» данные, то для каждой из подвыборок в листьях дерева проводятся статистические оценки точного значения этой функции.

Схематически алгоритм описывается следующим образом.

- Запрашивается выборка.
- Согласно некоторому правилу разбиения выбирается координата пространства признаков, по которой разделение имеет наибольшую точность.
- Строится бинарное дерево решений. Для каждого поддерева:
  - запрашивается подвыборка, оказавшаяся в этом поддереве;
  - производится статистическая оценка подвыборки на основе всех запросов;
  - аналогично находится оптимальное разбиение уже по статистической оценке;
  - если не выполняется некоторый критерий останова, то рекурсивно строятся два поддерева для разделенных точек.

Под точностью в данном алгоритме понимается отношение количества верно классифицированных объектов к количеству всех классифицируемых объектов либо другая определяемая пользователем функция качества $L(Y, Y^*, \varepsilon)$, где Y – предсказанные метки классов, Y^* – действительные метки классов, ε - параметр шума, от которого также может зависеть функция качества.

Критерий останова определяет превышение количества запросов к базе данных (бюджет приватности), достижение высокого значения функцией качества в одном из листов или в одном из листов осталось слишком мало точек.

В качестве бенчмарка для каждого из предложенных алгоритмов устанавливается обычное решающее дерево, но на незашумлённых данных.

Литература

1. *McSherry F., Mironov I.* Differentially private recommender systems: building privacy into the net // Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2009. P. 627–636.
2. *Friedman A., Schuster A*. Data mining with differential privacy // Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2010. P. 493–502.
3. *Quinlan J.R.* Induction of decision trees // Machine learning. 1986. V. 1. N 1. P. 81–106.
4. *Salzberg S.L.* C4. 5: Programs for machine learning by J.Ross Quinlan. Morgan Kaufmann Publishers, inc., 1993 // Machine Learning. 1994. V. 16. N 3. P. 235–240.
5. *Dwork C.* [*et al.*]. Calibrating noise to sensitivity in private data analysis // TCC. 2006. V. 3876. P. 265–284.

УДК: 004.056.52

Разграничение доступа к функциям управления средства виртуализации VMware vSphere

П.М. Журов

ЗАО "ОКБ САПР"

Виртуализация – самый эффективный способ сокращения расходов на ИТ-инфраструктуру с возможностью повышения эффективности и адаптивности для компаний любых размеров.

Но как и любое техническое средство, предназначенное для хранения и обработки информации, виртуальную инфраструктуру необходимо защищать.

На протяжении продолжительного периода времени среди средств виртуализации, представленных на рынке, лидером [1] является продукт компании VMware – vSphere.

Но, даже несмотря на все достоинства данного ПО, в нём есть существенный недостаток с точки зрения безопасности: администратор отвечает как за управление инфраструктурой, так и за разграничение доступа пользователя к её элементам. Это влечет за собой высокую трудоёмкость решения следующей проблемы: если в системе есть несколько сегментов, то критически возрастает вероятность преднамеренной или случайной утечки данных из одного сегмента в другой [2, 3, 4]. Для её решения необходимо программное средство, позволяющее разграничить доступ к элементам инфраструктуры для всех пользователей, включая администратора.

На сегодняшний день на рынке существует всего три продукта с подобным функционалом. Но один из них [5] не имеет сертификата ФСТЭК (а значит, не может применяться в государственных информационных системах), а второй [6] – не работает напрямую с vSphere (использует сторонний клиент), что вынуждает администратора изменить привычный порядок работы.

Более того, в связи с заявлением VMware о том, что в следующей версии продукта [7] будет использоваться новый клиент управления на основе HTML5, что влечет за собой изменение принципа взаимодействия веб-клиента с сервером, из чего можно сделать вывод, что существующие решения нужно дорабатывать, а значит, проблема остается актуальной. Отсюда возникает задача написать программное средство, которое обеспечит разграничение доступа для администраторов ВИ к объектам ВИ и функциям управления за счет перехвата пакетов, передаваемых от веб-клиента в сервис централизованного управления гипервизорами, их анализа и принятия решений на основе заданных в управляющем ПО параметров и при этом будет лишено всех вышеперечисленных недостатков.

Данная задача была разбита на следующие подзадачи.

1. Получить и проанализировать пакеты данных, передаваемых от веб-клиента на сервер управления.
2. Разработать алгоритм принятия решения о запрете или предоставлении доступа субъекта (администратора виртуальной ВИ) к объектам ВИ.
3. Написать программное обеспечение для прокси-сервера, реализующее выбранный алгоритм.

Анализ трафика позволил понять, как новая версия клиента взаимодействует с сервером управления. Было обнаружено, что сам пользователь, объект, с которым он взаимодействует и действие, которое над ним совершает, однозначно идентифицируется с помощью заголовков и содержания запросов. Для обеспечения взаимодействия администратора с сервером напрямую (отсутствие стороннего клиента) было принято решение использовать прозрачный прокси-сервер, который блокирует трафик при попытке совершить действие, запрещенное политикой безопасности. Сам прокси-сервер был реализован с помощью библиотеки mitmproxy для Python. Для задания политик безопасности использовалась база данных, для которой ранее был реализован графический пользовательский интерфейс. Обращаясь к этой базе данных, прокси-сервер пропускает трафик, либо возвращает сообщение об ошибке доступа.

Таким образом, по результатам работы были решены все поставленные задачи, необходимый функционал готов к использованию и соответствует всем требованиям ФСТЭК [2, 3] по обеспечению безопасности информационных систем.

Литература

1. VMware Named a Leader in Gartner Magic Quadrant for Enterprise Mobility Management Suites for Seventh Consecutive Year [Электронный ресурс]. Режим доступа: http://ir.vmware.com/overview/press-releases/press-release-details/2017/VMware-Named-a-Leader-in-Gartner-Magic-Quadrant-for-Enterprise-Mobility-Management-Suites-for-Seventh-Consecutive-Year/default.aspx, свободный.
2. Приказ №17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: утвержден ФСТЭК России 11 февраля 2013 г.
3. Приказ №21. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: утвержден ФСТЭК России 18 февраля 2013 г.
4. *Угаров Д. В., Постоев Д. А.* Проблемы реализации разграничения доступа к функциям управления виртуальных сред // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», М., 2016г., Вып.3, №114. С. 34–35.
5. ESXi Security [Электронный ресурс]. Режим доступа https://www.hytrust.com/solutions/private-cloud-controls/esxi/, свободный.
6. vGate [Электронный ресурс]. Режим доступа https://www.securitycode.ru/products/vgate/, свободный.
7. Goodbye, vSphere Web Client! [Электронный ресурс]. Режим доступа https://blogs.vmware.com/vsphere/2017/08/goodbye-vsphere-web-client.html, свободный.

УДК 519.725

Криптосистема, основанная на новых ранговых кодах

Э.М. Габидулин, Н.З. Хоан

Московский физико-технический институт (государственный университет)

Криптосистемы с открытым ключом, или асимметричные криптосистемы, характеризуются тем, что ключ зашифрования является общедоступным (открытый ключ), а ключ расшифрования является секретным и известен только получателю зашифрованного сообщения. В настоящее время основные варианты асимметричных криптосистем основаны на использовании трудных вычислительных задач, таких как разложение целого числа на множители или задачи дискретного логарифма (см., например, [1]).

Менее популярными являются асимметричные криптосистемы, основанные на линейных кодах. Однако в перспективе они могут вытеснить криптосистемы на других принципах, так как с появлением квантовых компьютеров последние станут не стойкими. Ниже будет описана асимметричная криптосистема на линейных кодах в ранговой метрике.

Пусть $GF(q)$ – базовое конечное поле, а $GF(q^m)$ – его расширение степени m. Пространство векторов $GF(q^m)^m$ длины m снабдим ранговой весовой функцией: ранговый вес вектора $\mathbf{g} = \left(g_1\ g_2 \cdots g_m\right) \in GF(q^m)^m$ равен максимальному числу координат, линейно независимых над базовым полем $GF(q)$. Ранговый линейный (m,k)-код с максимальным ранговым расстоянием (MPP код) определяется с помощью порождающей матрицы:

$$\mathbf{G}_k = \begin{pmatrix} g_1 & g_2 & \cdots & g_m \\ g_1^q & g_2^q & \cdots & g_m^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_m^{q^2} \\ \vdots & \vdots & \cdots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_m^{q^{k-1}} \end{pmatrix} \in GF(q^m)^{k\times m}.$$

Кодовые векторы рангового МРР кода – это $GF(q^{\mathrm{m}})$-линейные комбинации строк этой матрицы. Ранговый вес любого ненулевого вектора не меньше $d_{\mathrm{r}} = m - k + 1$. Мощность кода равна q^{mk} и является максимально возможной.

Первый вариант асимметричной криптосистемы Габидулина–Парамонова–Третьякова (системы ГПТ) предложен в работе [2]. В настоящее время система ГПТ имеет следующий вид.

Открытый ключ – матрица G_{pub} размера $k \times (t + m)$, являющаяся произведением трех матриц.

$$G_{\mathrm{pub}} = S(Y\ G_{\mathrm{k}})P.$$

Здесь матрица $\mathrm{G_k}$ – порождающая матрица МРР-кода, S – невырожденная квадратная матрица порядка k над расширенным полем $GF(q^m)$ (строчный скремблер), P – невырожденная квадратная матрица порядка $(t + m)$ над базовым полем (столбцевой скремблер), Y – матрица размера $k \times t$ со столбцевым рангом t (искажающая матрица).

Секретный ключ – матрицы G_{k}, S, P, Y по отдельности и быстрый алгоритм декодирования.

Зашифрование – информационный вектор m длины k над расширенным полем $GF(q^m)$ преобразуется в шифрованный вектор $\mathbf{c}$ длины $t + m$ по правилу

$$\mathrm{c} = \mathrm{mG_{pub}} + \mathrm{e},$$

где e – вектор искусственной ошибки рангового веса $t_2 < t = (n - k + 1)/2$.

Расшифрование – легальный пользователь с помощью быстрого алгоритма декодирования находит и устраняет заранее неизвестную искусственную ошибку e. Затем из оставшейся части извлекает информационный вектор m.

Этот вариант системы ГПТ оказался уязвимым к структурным атакам, предложенным в работе [3]. Причина состоит в высокой структурированности порождающей матрицы G_{k}. Матриц S, P, Y оказалось недостаточно, чтобы надежно скрыть структуру порождающей матрицы.

В настоящее время найдены новые МРР-коды с частично разрушенной структурой. Один из вариантов предложен в работе [4]. Цель нашей работы состоит в том, чтобы проверить применимость атак работы [3] к новым кодам. Порождающая матрица новых кодов может быть представлена в следующем виде:

$$\tilde{\mathbf{G}}_k = \begin{pmatrix} g_1 + \eta g_1^{q^k} & g_2 + \eta g_2^{q^k} & \cdots & g_m + \eta g_m^{q^k} \\ g_1^q & g_2^q & \cdots & g_m^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_m^{q^2} \\ \vdots & \vdots & \cdots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_m^{q^{k-1}} \end{pmatrix} \in GF(q^m)^{k\times m}.$$

В порождающей матрице «зашумлена» только первая строка. Используем эту матрицу в системе ГПТ. Оказалось, что процедура взлома работает для матрицы $\mathrm{G_k}$, но не работает для матрицы $\tilde{\mathbf{G}}_k$! Это первый результат, показывающий, что криптостойкость системы ГПТ может быть увеличена за счет выбора МРР-кода.

Благодарности. Работа частично финансировалась в рамках гранта РФФИ №15-07-08480-17.

Литература

1. *Владимиров С.М., Габидулин Э.М., Колыбельников А.И., Кшевецкий А.С.* Криптографические методы защиты информации. М.: МФТИ. 2016. 266 с.
2. *Gabidulin E.V., Paramonov A.V., and Tretjakov O.V.* Ideals over a noncommutative rring and their application in cryptology // Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Tecniques, EUROCRYPT'91, P. 482–489, Berlin; Heidelberg: Springer-Verlag, 1991.
3. *Overbeck R.* . Structural attacks for public key cryptosystems based on Gabidulin codes. // J. Cryptology. 2008. 21(2). 280_301.
4. *Sheekey J.* A NEW FAMILY OF LINEAR MAXIMUM RANK DISTANCE CODES // Advances in Mathematics of Communications doi:10.3934/amc.2016019. 2016. V. 10, N. 3. P. 475–488.

УДК 62-50

Декодирование двухкомпонентных подпространственных кодов

Э.М. Габидулин, К.В. Ву

Московский физико-технический институт (государственный университет)

Класс многокомпонентных кодов с нулевым префиксом (МНП-коды) предложен в 2008 г. Э.М. Габидулиным и М. Боссертом [1], [2] на основе SKK-кодов [3].

Рассмотрим задачу декодирования МНП-кодов при передаче сообщений по бинарному симметричному каналу без памяти. Модель системы связи состоит из источника сообщений, кодера для канала, канала связи, декодера и блока, называемого получатель сообщений.

Источник сообщений содержит N различных сообщений, которые могут быть записаны в виде такого же числа двоичных чисел. Эти сообщения выбираются случайно (например, с равной вероятностью $1/N$) и посылаются в систему связи, сначала на вход кодера канала. В нашей модели используется двухкомпонентный МНП код с параметрами длина $n = 8$, размерность $m = 3$, кодовое расстояние $d_{\text{sub}} = 6$. Так как конструкция подпространственного кода включает ранговый код, то сначала построим ранговый код, матрицы которого имеют размер $(m = 3)\ x(n - m = 5)$, ранговое расстояние равно $d_{\text{r}}=3$. Всего 32 матрицы первой компоненты и одна матрица второй компоненты. Первая компонента – это SKK-код с подпространственным расстоянием $d_{\text{sub}} = 2m = 6$.

Матрицы первой компоненты подпространственного кода являются конкатенацией единичной матрицы порядка 3 и матрицы рангового кода. Матрица второй компоненты является конкатенацией полностью нулевой матрицы размера $(m = 3)\ x(n - m = 5)$ и единичной матрицы порядка 3. Всего в этом коде N=33 кодовых слова соответственно числу сообщений источника. Следовательно, каждому сообщению источника соответствует одно из кодовых слов в виде последовательности из 8 двоичных символов – нулей и единиц. Непрерывный поток единичных и нулевых символов поступает в канал связи. Канал считаем двоичным симметричным без памяти. Его моделируем с помощью генератора независимых двоичных символов, где вероятность единичного символа обозначена P_0 . Будем менять это значение от 0.04 до 0.5. Рассмотрим работу декодера. Образуем суммы по модулю 2 полученного сообщения-матрицы поочерёдно с каждым из возможных сообщений, что могут быть на выходе кодера. Подсчитываем число единиц в матрице. Выбираем то из сообщений-матриц, где число единичных позиций в матрице наименьшее. Это сообщение считаем передававшимся. Если есть два или более случаев с одинаковыми значениями числа единиц, то принимаем решение об отказе от декодирования. Вероятность ошибки декодирования растёт одновременно с вероятностью ошибки в канале. Аналогично растёт и вероятность отказа от декодирования. Вероятности оценены относительными значениями соответствующих ситуаций.

Проведено моделирование системы связи при использовании подпространственного двухкомпонентного МНП-кода, бинарного симметричного канала и

декодера, работающего по правилу минимума ошибок. Полученные зависимости вероятностей ошибок декодирования, отказов от декодирования и правильных решений декодера вполне согласуются с теорией: чем лучше канал, тем выше вероятность правильных решений и меньше вероятность ошибок и отказов от декодирования.

Таблица 1.

p_0	0.04	0.08	0.125	0.17	0.21	0.25	0.29	0.33	0.375	0,42	0.46	0.5
$p_{прав}$	0,824	0.694	0.568	0.470	0.385	0.284	0.243	0.182	0.144	0.114	0.071	0.043
$p_{неправ}$	0	0.073	0.149	0.248	0.330	0.365	0.423	0.474	0.536	0.554	0.585	0.611
$p_{отказ}$	0,176	0.233	0.283	0.282	0.285	0.351	0.334	0.344	0.32	0.332	0.344	0.346

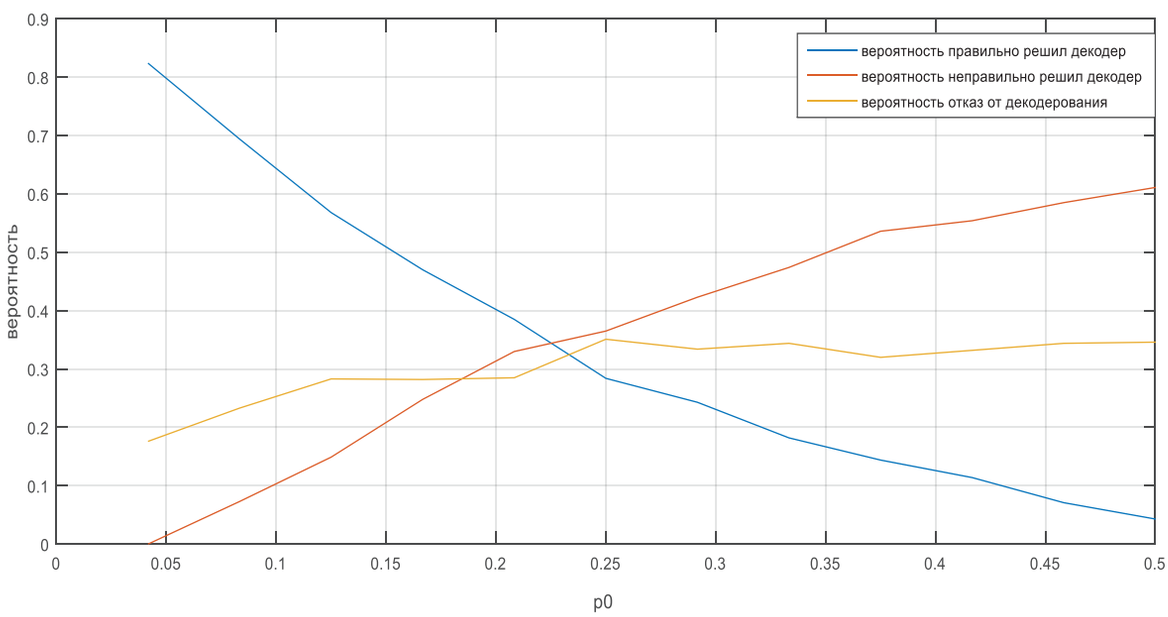


Рис. 1.Зависимости $P_{\text{прав}}$, $P_{\text{неправ}}$, $P_{\text{отказ}}$ от p_0

Литература

1. *Gabidulin E.M., Bossert M.* Codes for Network Coding // Proc. 2008 IEEE Int. Sympos.on Information Theory (ISIT'2008). Toronto, Canada. July 6–11. 2008. P. 867–870.
2. *Габидулин Э.М., Боссерт М.* Алгебраические коды для сетевого кодирования // Пробл. передачи информ. 2009. Т. 45. № 4. С. 54–68.
3. *K¨otter R., Kschischang F.R.* Coding for Errors and Erasures in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. № 8. P. 3579–3591.

УДК 004

Нахождение ошибок использования памяти после освобождения в бинарном коде

А.К. Асланян, В.Г. Варданян

Институт системного программирования РАН

Обнаружение ошибок в программном обеспечении является важной задачей для повышения безопасности и надежности. Это можно сделать в любое время в течение жизненного цикла программного обеспечения. В идеале все ошибки должны обнаруживаться на этапе тестирования до развертывания программного обеспечения. Тем

не менее тестирование программного обеспечения не всегда позволяет найти все возможные ошибки. Более того, когда для написания программ используются небезопасные для памяти языки, такие как C / C ++, эти ошибки могут привести к нарушениям безопасности. Несмотря на это, эти языки программирования по-прежнему популярны из-за высокой производительности. C / C ++ используются для разработки операционных систем, баз данных, сетевых протоколов, криптографических библиотек, ракетных систем, простых систем управления и т. д.

Использование памяти после освобождения – это класс ошибок памяти, которые возникают, когда программа продолжает использовать указатель после его освобождения. Существует ряд [1–7] исследований, в которых особое внимание уделяется обнаружению дефектов использование памяти после освобождения. В общем случае они могут быть обнаружены как при статическом, так и в динамическом анализе. Методы статического анализа часто основаны на процессе дисассемблирования бинарного файла. Методы динамического анализа пытаются отслеживать выполнение программы и искать потенциальные дефекты. Решения, основанные на динамическом анализе для обнаружения дефектов использования памяти после освобождения, обычно потребляют высокую производительность и могут пропускать множество ошибок, поскольку они способны исследовать только небольшую часть пространства выполнения программы.

Разработанная платформа способна анализировать бинарные файлы нескольких архитектур (x86, x86-64, arm, MIPS, POWER-PC) и основана на статическом анализе программ. Мы вводим новый подход для обнаружения дефектов использования памяти после освобождения, который основан на графовом представлении программы. Инструмент состоит из двух основных компонентов: генерации графов зависимости системы и анализа полученных графов. Граф зависимости системы объединяет граф вызовов, межпроцедурные данные, граф потока управления и граф потока данных. Генерация графов зависимости системы реализована с использованием платформ Ida Pro [8] и Binnavi [9]. Основой для генерации графов зависимости системы является REIL [10] представление. На втором этапе основной алгоритм анализирует полученные графы для обнаружения ошибок использования памяти после освобождения. Рисунок 1 представляет основную архитектуру предлагаемого инструмента.

Предлагаемый инструмент тестирован на известных тестовых наборах, таких как Juliet [11]. Результаты показывают, что мы можем найти все ошибки использования памяти после освобождения, представленные на этих тестах. Инструмент также тестировался на десятки реальных программ, которые содержат ошибки. В табл. 1 представлен список успешно обнаруженных ошибок. Все тесты производились на системе с 20 физическими процессорами intel xeon 2.3 ГГц.

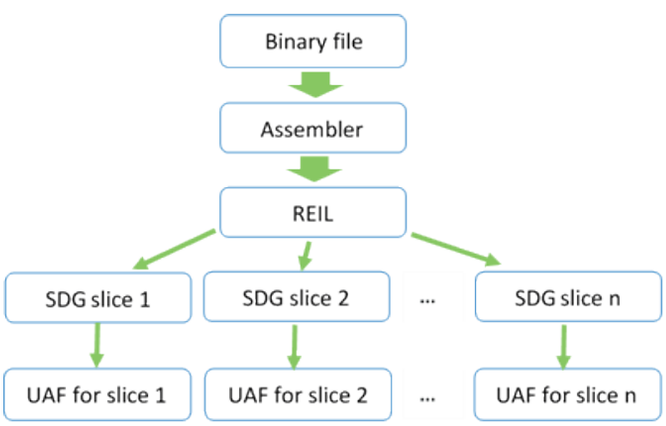


Рис.1. Архитектура инструмента

Таблица.1

Результаты

Имя проекта	Версия	Размер проекта	Время анализа	Неверные срабатывания
Jasper	1.900.1	1 МБ	166 с.	0%
giflib	5.1.2	50 КБ	10 с.	0%
libtiff	4.0.3	1 МБ	100 с.	33%
openslp	1.2.1	700 КБ	40 с.	50%
libssh	0.5.2	700 КБ	99 с.	21%

Литература

1. *Cuoq P*., *Kirchner F*., *Kosmatov N*., *Prevosto V*., *Signoles J*. and *Yakobowski B*., Frama-C—a software analysis perspective. // SEFM. 2012. P. 233–247.
2. *Xu W*., *DuVarney D. C*. and *Sekar R*. An efficient and backwards-compatible transformation to ensure memory safety of C programs. // ACM SIGSOFT Software Engineering Notes. 2004. V. 29. P. 117–126.
3. *Caballero J*., *Grieco G*., *Marron M*. and *Nappa A*. Undangle: early detection of dangling pointers in use-after-free and double-free vulnerabilities. // Proceedings of the 2012 International Symposium on Software Testing and Analysis. 2012. P. 133–143.
4. *Lee B*., *Song C*., *Jang Y*. and *Wang T*. Preventing Use-after-free with Dangling Pointers Nullification. // NDSS Symposium. 2015.
5. *Feist J*., *Mounier L.* and *Potet M.L*. Statically detecting use after free on binary code. // Journal of Computer Virology and Hacking Techniques. 2014. V. 10. N. 3. P. 211–217.
6. *Cesare S*. Detecting bugs using decompilation and data flow analysis. // Black Hat USA. 2013.
7. *Dewey D*., *Reaves B*. and *Traynor P*. Uncovering Use-After-Free Conditions in Compiled Code. // 10th International Conference on Availability, Reliability and Security. 2015.
8. https://www.hex-rays.com/products/ida
9. https://www.zynamics.com/binnavi.html
10. https://www.zynamics.com/binnavi/manual/html/reil_language.htm
11. https://samate.nist.gov/SRD/testsuite.php

УДК 519.727

Декодирование компоненты многокомпонентного кода

И.Ю. Сысоев

Московский физико-технический институт (государственный университет)

Многокомпонентные коды используются при передаче данных в случайном сетевом кодировании [1]. Лифтинговая конструкция используется для восстановления информации о преобразовании строк матрицы в процессе передачи [2]. В данной работе рассмотрен алгоритм декодирования компоненты многокомпонентного кода. Он развивает идею декодирования компоненты [3]. При декодировании кодовое слово представляется в виде матрицы, разделённой на части. Каждая часть состоит из δ столбцов, причём её можно представить в виде столбца матриц размером $\delta \times \delta$. Общее количество частей равняется $r+1$. Сначала методом преобразования Гаусса (складывание строк между собой, их перестановка) значимый элемент первой части приводится к диагональному виду:

$$\begin{Vmatrix} Y_{11} & * \\ Y_{21} & * \\ Y_{31} & * \\ Y_{r1} & * \end{Vmatrix} \to \begin{Vmatrix} D_1 & * \\ \mathrm{O}_\delta & * \\ \vdots & * \\ \mathrm{O}_\delta & * \end{Vmatrix}. \quad (1)$$

В выражении (1) D_1 соответствует позиции значимого элемента. В общем случае значимый элемент соответствует элементу, индекс которого равняется номеру части. Далее определяется ранг значимого элемента $Rk(D_1)$. Если $Rk(D_1) < \frac{1}{2}$, то декодер принимает решение о том, что значимая позиция при кодировании равнялась нулевой матрице $\Xi_1 = \begin{vmatrix} \mathrm{O} \\ \mathrm{O} \\ \dots \\ \mathrm{O} \end{vmatrix}$. Следовательно, передавалась последняя компонента наименьшей мощности с номером $r+1$. Если $Rk(D_1) = \frac{1}{2}$, то принимается решение об отказе от декодирования. Если $Rk(D_1) > \frac{1}{2}$, то декодер принимает решение о том, что при передаче значимая часть равнялась $\Xi_1 = \begin{vmatrix} I \\ \mathrm{O} \\ \dots \\ \mathrm{O} \end{vmatrix}$, и переходит к декодированию значимого элемента второй части. Нулевые элементы на диагонали значимого элемента первой части будут считаться стираниями при декодировании кода компоненты. Матрица будет приведена к виду

$$\begin{Vmatrix} I & M_1 & * \\ \mathrm{O} & D_2 & * \\ \mathrm{O} & \mathrm{O} & * \\ \dots & \dots & \dots \\ \mathrm{O} & \mathrm{O} & * \end{Vmatrix}. \quad (2)$$

При декодировании значимого элемента второй части D_2 также будет применяться метод Гаусса приведения элемента к диагональному виду с тем отличием, что строчки, содержащие M_1, при этой операции задействованы не будут. После приведения к диагональному виду D_2 декодер должен выполнить расчёт $Rk(D_2)$. Если $Rk(D_2) < \frac{1}{2}$, то декодер принимает решение о том, что вторая часть после кодирования равнялась $\Xi_2 = \begin{vmatrix} M_1 \\ \mathrm{O} \\ \dots \\ \mathrm{O} \end{vmatrix}$. Следовательно, отправленный кодовый вектор относится к компоненте r. Если $Rk(D_2) = \frac{1}{2}$, то принимается решение об отказе от декодирования. Если $Rk(D_2) > \frac{1}{2}$, то

декодер считает, что отправленная часть равнялась $\Xi_2 = \begin{vmatrix} \mathrm{O} \\ I \\ \mathrm{O} \\ \dots \\ \mathrm{O} \end{vmatrix}$. При таком решении методом Гаусса должно быть выполнено следующее преобразование матрицы:

$$\left\| \begin{matrix} I & M_1 & * \\ \mathrm{O} & D_2 & * \\ \mathrm{O} & \mathrm{O} & * \\ \dots & \dots & \dots \\ \mathrm{O} & \mathrm{O} & * \end{matrix} \right\| \to \left\| \begin{matrix} I & \mathrm{O} & * \\ \mathrm{O} & D_2 & * \\ \mathrm{O} & \mathrm{O} & * \\ \dots & \dots & \dots \\ \mathrm{O} & \mathrm{O} & * \end{matrix} \right\|. \qquad (3)$$

Строчки, содержащие нулевые диагональные элементы из D_2, переходят в категорию строк, у которых возникли ошибки стирания.

Аналогичным образом на шаге s (всего r шагов при декодировании компоненты) принимается решение о том либо отнести принятую матрицу к компоненте $r+1-s$, либо решить, что она относится к одной из компонент набора с индексами $(1,2,\dots,r-s)$, либо принять решение об отказе от декодирования.

В результате декодирования будет получен номер компоненты и индексы строк, в которых произошли стирания.

Если ранг ошибки при передаче исходной матрицы не превышает $\frac{\delta}{2}$, то в каждой значимой части ранг ошибки также не будет превышать $\frac{\delta}{2}$, что позволит без ошибок декодировать полученную матрицу описанным алгоритмом.

Литература

1. *Габидулин Э.М., Пилипчук Н.И., Боссерт М.* Декодирование случайных сетевых кодов // Проблемы передачи информации. 2010. Т. 46. № 4. С. 33–55.
2. *Silva D., Kschischang F.* Using Rank-Metric Codes for Error Correction in Random Network Coding // Proc. ISIT-2007. 2007. P. 796–800.
3. *Gabidulin E.M.*, *Pilipchuk N.I., Sysoev IY.* Decoding New Multicomponent Codes // Proc. of XV International Symposium “Problems of Redundancy in Information and Control Systems” Redundancy-2016. 2016. P. 53–57.

Научное издание

Труды
60-й Всероссийской научной конференции МФТИ

Радиотехника и компьютерные технологии

20-26 ноября 2017 года

Составители:
М.В. Милов, С.О. Русскин

Редакторы:
В.А. Дружинина, И.А. Волкова, О.П. Котова, Н.Е. Кобзева

Корректоры:
И.А. Волкова, О.П. Котова, Н.Е. Кобзева

Набор и вёрстка:
М.А. Чайковский

Подписано в печать 12.12.2017. Фомат 60 × 84 $^{1}/_{8}$.
Усл. печ. л. 24,25. Тираж 50 экз. Заказ № 608
Федеральное государственное автономное образовательное
учреждение высшего образования «Московский физико-технический институт
(государственный университет)»
141707, Московская обл., г. Долгопрудный, Институтский пер., 9
Тел. (495)408-58-22

"Полиграфия "ПРОДВИЖЕНИЕ"
123592, г. Москва, ул. Кулакова дом 20, стр. 1Б
E-mail: info@prodv.pro
Тел. (495) 988-93-68

ISBN 978-5-7417-0648-0