Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

МАТЕРИАЛЫ 53-Й НАУЧНОЙ КОНФЕРЕНЦИИ АСПИРАНТОВ, МАГИСТРАНТОВ И СТУДЕНТОВ

(Минск, 2–6 мая 2017 года)

Минск, БГУИР
2017

Телекоммуникационные системы и сети: материалы 53-й научной конференции аспирантов, магистрантов и студентов (Минск, 2–6 мая 2017 г.). – Минск: БГУИР, 2017. – 107 с.

В сборник включены лучшие доклады, которые были представлены на 53-й научной конференции аспирантов, магистрантов и студентов БГУИР, отобранные по следующим направлениям: метрология и стандартизация; телекоммуникационные системы; сети и устройства телекоммуникаций; защита информации.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

СОДЕРЖАНИЕ

РОЛЬ МИКРОЭЛЕКТРОНИКИ В СИСТЕМАХ ПЕРЕДАЧИ, ОБРАБОТКИ И ХРАНЕНИЯ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Воробьев И.Ю., Асомадинов И.О.

Печень Т.М.– ассистент

На сегодняшний день сложно представить мир без электронных устройств. Прослеживая историю электротехники можно увидеть её эволюцию и развитие - электронные устройства становилась все более сложнее и совершеннее. С течением времени появилась необходимость передачи и обработки сигнала, для более быстрой и точной работы. Также, помимо передачи и обработки появилась потребность в компоновке и сборе важной информации. Эти задачи и привели ученых к созданию электроники.

С каждым годом, электроника бурно развивается, она переживает процесс миниатюризации - уменьшение ее физических размеров, при этом вычислительная мощность и скорость обработки увеличивается в несколько сотен раз. Сейчас все более широко развивается нано-электроника. С ее помощью можно почти без потерь обработать и передать большое количество информации за малый промежуток времени.

Для раскрытия данной темы мы затронем следующие темы:

Микроэлектроника — это подраздел электроники, связанный с изучением и производством электронных компонентов с геометрическими размерами характерных элементов порядка нескольких микрометров и меньше. Основные ветви, связанные с микроэлектроникой:

1) Обработка сигнала средствами микроэлектроники.
2) Передача информации средствами микроэлектроники.
3) Хранение информации средствами микроэлектроники.

I. **Обработка сигнала**— область радиотехники, в которой осуществляется восстановление, разделение информационных потоков, подавление шумов, сжатие данных, фильтрация, усиление сигналов. Существует множество направлений обработки сигналов, зависящие от их природы. Для аналоговых сигналов обработка может включать усиление и фильтрацию, модуляцию и демодуляцию. Для цифровых сигналов также осуществляется сжатие, обнаружение и исправление ошибок.

- Аналоговая обработка сигналов — для неоцифрованных сигналов, таких как радио-, телефонные или телевизионные сигналы.
- Цифровая обработка сигналов — для оцифрованных сигналов. Обработка осуществляется с помощью цифровых схем, в том числе с помощью программных решений.
- Статистическая обработка сигналов — включает анализ и получение информации из сигналов, основываясь на их статистических свойствах.

На разных этапах процессов получения и обработки информации как материальное представление сигналов в устройствах регистрации и обработки, так и формы их математического описания при анализе данных, могут изменяться путем соответствующих операций преобразования типа сигналов.

Операция дискретизации (discretization) осуществляет преобразование аналоговых сигналов (функций), непрерывных по аргументу, в функции мгновенных значений сигналов по дискретному аргументу.

Операция квантования или аналого-цифрового преобразования (АЦП; английский термин Analog-to-Digital Converter, ADC) заключается в преобразовании дискретного сигнала $s(t_n)$ в цифровой сигнал $s(n) = s_n \approx s(t_n)$, n = 0, 1, 2,.., N, как правило, кодированный в двоичной системе счисления.

Операция цифро-аналогового преобразования (ЦАП; Digital-to-Analog Converter, DAC) обратна операции квантования, при этом на выходе регистрируется либо дискретно-аналоговый сигнал $s(t_n)$, который имеет ступенчатую форму, либо непосредственно аналоговый сигнал s(t), который восстанавливается из $s(t_n)$, например, путем сглаживания.

Перед тем как сигнал отправить на какое-то расстояние, его нужно преобразовать. Необходимо отправить аналоговый сигнал на какой-то приемник. Для этого аналоговый сигнал нужно перевести в цифровой. В этом случае используют аналого-цифровой преобразователь (АЦП). На рис.1. показаны возможности основных архитектур АЦП в зависимости от разрешения и частоты дискретизации.

Как правило, АЦП — электронное устройство, преобразующее напряжение в двоичный цифровой код. Разрешение АЦП — минимальное изменение величины аналогового сигнала, которое может быть преобразовано данным АЦП — связано с его разрядностью. В случае единичного измерения без учёта шумов разрешение напрямую определяется *разрядностью* АЦП.

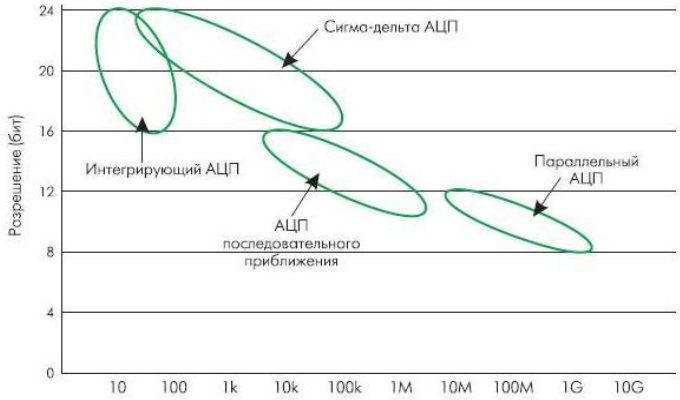


Рисунок 1 – основная архитектура АЦП

Разрядность АЦП характеризует количество дискретных значений, которые преобразователь может выдать на выходе. В двоичных АЦП измеряется в битах, в троичных АЦП измеряется в тритах. Например, двоичный 8-разрядный АЦП способен выдать 256 дискретных значений (0…255), поскольку 2^8=256 троичный 8-разрядный АЦП способен выдать 6561 дискретное значение, поскольку 3^8=6651.

II. **Передача сигнала**— физический перенос данных в виде сигналов от точки к точке или от точки к нескольким точкам средствами электросвязи по каналу передачи данных, как правило, для последующей обработки средствами вычислительной техники.
Примерами подобных каналов могут служить медные провода, ВОЛС, беспроводные каналы передачи данных или запоминающее устройство. Передаваемые данные могут быть цифровыми сообщениями, идущими из источника данных. Это может быть и аналоговый сигнал — телефонный звонок или видеосигнал, оцифрованный в битовый поток, используя импульсно-кодирующую модуляцию (PCM) или более расширенные схемы кодирования источника (аналого-цифровое преобразование и сжатие данных).

III. **Запоминающее устройство** (ЗУ) — устройство, предназначенное для записи и хранения данных. В основе работы запоминающего устройства может лежать любой физический эффект, обеспечивающий приведение системы к двум или более устойчивым состояниям. Устройство, реализующее компьютерную память. К основным параметрам цифровых ЗУ относятся информационная ёмкость (битов, тритов и т. д.), потребляемая мощность, время хранения информации, быстродействие.
Самое большое распространение цифровые запоминающие устройства приобрели в компьютерах (компьютерная память). Кроме того, они применяются в устройствах автоматики и телемеханики, в приборах для проведения экспериментов, в бытовых устройствах (телефонах, фотоаппаратах, холодильниках, стиральных машинах и т. д.), в пластиковых карточках, замках.

Усовершенствование микроэлектроники – залог качественно обработанный информации.

Список использованных источников:

1) Большая советская энциклопедия. 3-е изд. 1969—1978 гг.
2) S. Norsworthy, R. Schreier, G. Temes. Delta-Sigma Data Converters.
3) Behzad Razavi. Principles of Data Conversion System Design.
4) Ханзел Г. Е. Справочник по расчету фильтров. США, 1969.

ОПТИЧЕСКИЕ ВОЛОКНА В СИСТЕМАХ ТЕЛЕКОММУНИКАЦИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сугако А. В., Юган А. К.

Печень Т.М. – ассистент

С самого начала человечеству требовались средства связи для передачи информации на внушительные расстояния. Люди всеми возможными способами стремились создать пути передачи информации с наибольшей скоростью, лучшей защищённостью и качеством целостности информации. В наше время технологии развиваются с невероятно быстро и новые устройства требуют новые проводники информации, более быстрые, с большим возможным расстоянием передачи без отражателей и усилителей, с наименьшим количеством приборов для передачи, с простой установкой и принципом работы. И в 1950-х годах такой способ передачи был найден: передача информации со скоростью, сравнимой со скоростью света, с наибольшим диапазоном частот и лучшей помехозащищенностью - это оптическое волокно.

Оптическое волокно - нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

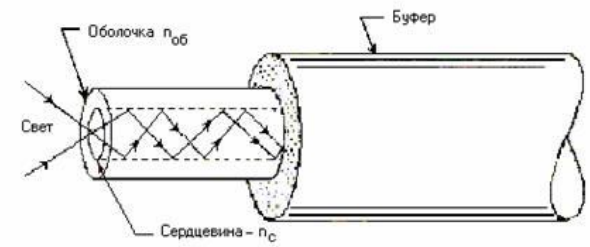


Рисунок 1 Конструкция простейшего оптического волокна

Оптическое волокно в простейшем случае состоит из сердцевины и оболочки, как показано на рисунке 1. Они имеют разные показатели преломления. Сердцевина при этом используется как собственно среда передачи, а оболочка используется для создания границы раздела между ней и сердцевиной. Эта граница формирует физический канал волноводного типа – световод, по которому и распространяется световой луч – переносчик передаваемого информационного сигнала.

Оптические волокна бывают одномодовые (распространяется только одна мода) и многомодовые (распространение нескольких или многих мод).

Параметрами оптического волокна являются: числовая апертура, которая связана с максимальным углом ввода излучения из свободного пространства, относительная разность показателей преломления и нормированная частота.

Волокно характеризуется двумя важнейшими характеристиками: затуханием и дисперсией.

На затухание света в волокне влияют такие факторы, как собственные потери (потери на поглощение и рассеивание) и кабельные потери. Общее затухание определяется суммой этих потерь. Существуют окна прозрачности (ОП) кварцевого оптического волокна, в которых свет распространяется вдоль волокна с малым затуханием, показанные на рисунке 2.

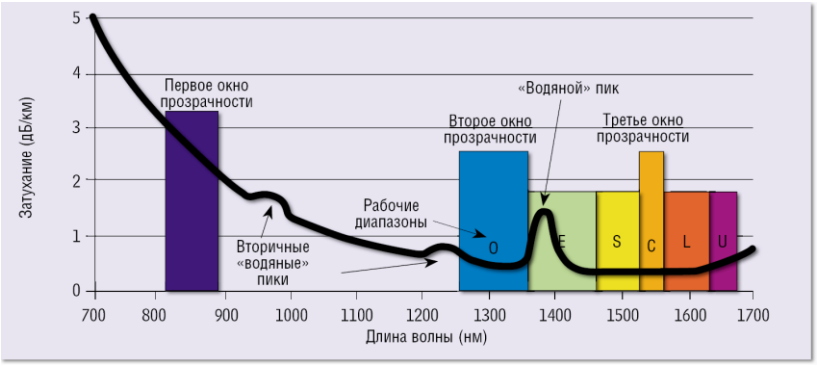


Рисунок 2 Окна прозрачности (ОП)

Дисперсия - это расплывание светового импульса по мере его движения по оптическому волокну. Она может быть нескольких видов: модовая, поляризационная и хроматическая, которая разделяется на материальную, волноводную и профильную. Результирующая дисперсия включает в себя все виды дисперсии и ограничивает максимальную скорость передачи информации по линиям связи.

Основными преимуществами оптоволокна являются:

- Широкополосность оптических сигналов, обусловленная очень высокой частотой несущей.
- Очень малое затухание светового сигнала в волокне, что позволяет строить волоконно-оптические линии связи длиной до 100 км и более без регенерации сигналов;
- Устойчивость к электромагнитным помехам со стороны окружающих медных кабельных систем, электрического оборудования и погодных условий;
- Защита от несанкционированного доступа;
- Электробезопасность;
- Долговечность.

К недостаткам можно отнести:

- Относительно высокая стоимость элементов оптического кабеля;
- Относительно высокая стоимость сварки оптического волокна;
- Дисперсия

В настоящее время активно тестируются новые способы передачи сигнала, а также материалы, с помощью которых можно повысить полосу пропускания практически на порядок. Кроме того оптоволокно все активнее внедряется в высокотехнологичные и инновационные области промышленности. Связь с датчиками на опасных производствах и атомных станциях уже давно выполняется исключительно с применением оптоволокна. Теперь к этому добавляется использование оптоволокна в космической, авиационной и, конечно же, в военной промышленности. Применение оптоволокна дает столько преимуществ, что на второй план уходит основной его недостаток – дороговизна. Именно поэтому оптоволокно признано материалом 21 века.

Список использованных источников:

1. "Файбер Оптик Пассив Системс" (ФОПС)
Режим доступа: http://www.fopc.ru.- Дата доступа: 25.11.2016.
2. Ландсберг Г.С. Оптика. Изд. 5-е.- М.:Наука,1976.
3. Лазерный Портал
Режим доступа: http://laser-portal.ru, Дата доступа: 22.11.2016.
4. Слепов Н.Н. Современные технологии цифровых оптоволоконных сетей связи.- Москва :Радио и связь,2000.

ФИЗИЧЕСКИЕ ОСНОВЫ ЦВЕТНОГО ТЕЛЕВИДЕНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Захарченя А.С., Серченя А.А.

Печень Т.М. – ассистент

Телевидение – это наиболее уникальный и оригинальный способ вещания, сочетающий в себе возможности визуального и аудиального вещания. Можно выделить вещательное телевидение, т.е. ориентированное на массового зрителя, и прикладное, более узкоспециализированное. Цель данного доклада – рассмотреть физические основы цветного телевидения, разобрать, как же передается цвет и чем он характеризуется.

Зрительную информацию о внешнем мире мы получаем при помощи зрительного аппарата. Телевидение использует особенности и несовершенств глаза. Одна из них, активно используемая ТВ, отражена в трёхкомпонентной теория восприятия цветов. Согласно этой теории, в глазу имеются три вида рецепторов (колбочек), воспринимающих соответственно красную (длинноволновую), желтую (средневолновую) и голубую (коротковолновую) части видимого спектра. Таким образом, все возможные цвета ЦТ передает при помощи всего трех: красного, зеленого и синего – взятых в определенном соотношении. На основе этого в 1931 всеми странами была принята стандартная колориметрическая система RGB. В ее основе лежит равносторонний треугольник, вершины которого соответственно характеризуют спектральные цвета. Экспериментально установлено, что количественно и качественно световой поток может быть определен следующей формулой:

$$F' = r'R + g'G + b'B = mF$$

где F' - заданный или искомый световой поток; r', g', b' - количество или модули красного, зеленого, синего цветов.

Воспроизведение каждого цвета при установленных основных параметрах однозначное. Работают в этой системе, используя координаты цветности, сумма которых равна 1 и которые не зависят от яркости цвета и определяют его цветность. Преимущество данной системы в возможности экспериментально вычислить ее параметры, а недостаток – в сложности вычислений, возникающей из-за наличия отрицательных координат для большой группы реальных цветов, а синтезировать такие цвета невозможно. Этот недостаток отсутствует в стандартной трихроматической системе XYZ. Однако эта система имеет чисто расчетный характер, т.к. ее основные цвета X, Y и Z нереальны, синтезировать их не представляется возможным [1].

Цвет можно охарактеризовать количественно и качественно. Количественной характеристикой является яркость. Яркость, воспринимаемая глазом, не идентична яркости объект и связь между ними устанавливает с помощью закона Вебера-Фехнера. К качественным характеристикам относятся цветовой тон и насыщенность. Цветовой тон позволяет осознать, какой именно цвет мы видим, а насыщенность – это степень отличия данного цвета от белого (измеряется в %).

Задача ТВ сводится к передаче изображения, точнее, сигналов, однозначно его характеризующих. Изображение полностью характеризуется сигналами основных цветов (СОЦ) и сигналом яркости (СЯ). Передавать (СЯ) и 2 сигнала основных цветов (третий легко находится, т.к. эти сигналы линейно-зависимы) неэкономно по отношению к полосе передаваемых частот, и к тому же все эти три сигнала несут информацию о яркости. При передачи по каналу трех сигналов (яркости и двух цветных, т.к. цветность – величина двумерная, для ее представления достаточно иметь два сигнала; выбирают обычно красный и синий), они будут искажаться и в итоге сигнал яркости будет претерпевать тройной искажение. При передаче их по каналу на все три сигнала будут влиять помехи, и приемник примет весьма искаженный СЯ, что негативно скажется на изображении. Во избежание этого, а также в силу того, что полосу частот надо экономить, было решено передавать сигнал яркости и два цветоразностных сигнала. Из трех ЦРС передают U_{R-Y} и U_{B-Y} для обеспечения большей помехоустойчивости. Теперь при влиянии искажений на передаваемые сигналы СЯ подвергается искажениям лишь единожды, что положительно влияет на яркость изображения. Учитывая пониженную разрешающую способность зрения к цветовым переходам, можно без ущерба для качества передаваемого изображения сократить с помощью ФНЧ полосу частот ЦРС в 2…4 раза: до 1,5…3 МГц в ТСЧ (было 4,2…6 МГц) и до 7,5…30 МГц в ТВЧ (было 30…60 МГц) [2].

Системы цветного телевидения отличаются по способу передачи этих сигналов. Среди систем ЦвТ можно выделить композитные и компонентные. В настоящее время композитные (аналоговые, совместимые с черно-белым ТВ) системы уже изжили себя и доживают свой век в кабельном телевидении; происходит переход на компонентные (цифровые) системы.

Среди композитных систем выделяют SECAM, PAL и NTSC. В основу формирования сигнала цветности в системе SECAM положен следующий принцип: два цветоразностных сигнала U_{R-Y} и U_{B-Y} передаются последовательно через строку с использованием частотной модуляции. Благодаря последовательной передаче цветоразностных сигналов полностью устранены перекрестные искажения между ними, а применение частотной модуляции позволило снизить чувствительность сигнала цветности к дифференциальным искажениям. В системе NTSC сигнал цветности (который образуют два ЦРС) передается при помощи квадратурной модуляции. Преимущество этой системы в том, что она позволяет

уплотнить передаваемую информацию и получить высокую цветовую четкость при относительно узкополосном канале передачи. И в системе PAL также используется метод квадратурной модуляции, но особенность формирования сигнала цветности в том, что используется АМ с подавлением несущей (балансной) модуляции поднесущей частоты цветоразностными сигналами [3].

В компонентных системах все три сигнала передаются отдельно. Используют или три канала, или какое-либо уплотнение (например, по частоте).

Постепенно аналоговые системы телевещания уходят в прошлое, но на смену им приходят новые аналого-цифровые (PALplus, MAC) и цифровые (ATSC, DVB, ISDB) системы. Это во многом стало возможным благодаря развитию других отраслей электроники: разработке и внедрению оптоволокна и т.д. По причине развития разных типов сетей стало возможным улучшение качества изображения, уменьшение фоновых помех и искажений, а также мы получили возможность использовать Internet-телевидение.

Список использованных источников:

1. Джакония В.Е. Телевидение / В.Е. Джакония. – «Горячая линия – Телеком», 2002. – 640 с.

2. Капуро, П.А. Методы формирования и контроля ТВ сигналов и изображений: пособие / П.А. Капуро [и др.]. – Минск: БГУИР, 2016. – 100 с.: ил.

3. Капуро П.А. ЭУМКД «Телевизионные системы» / П.А. Капуро, А.П. Ткаченко. – Минск: БГУИР, 2008.

МЕТОДЫ ОБРАБОТКИ РАДИОЛОКАЦИОННЫХ СИГНАЛОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Юган А. К, Синевич А. В., Пискижев И. В.

Печень Т.М. – ассистент

В настоящее время человечеству необходимо оборудование для навигации морских и воздушных судов, для прогнозирования погодных условий и научных исследований. Так в 1905 году Кристиан Хюльсмайер запатентовал первый радар. Радар - это устройство для обнаружения и определения местонахождения объектов в пространстве по отраженным от них радиоволнам. Принцип работы радаров один и тот же, но у каждого из них есть своя отличительная особенность относительно обработки сигналов. Принципиально алгоритм состоит в следующем:

- Передатчик радара выдает короткие мощные СВЧ импульсы энергии;
- Переключатель (мультиплексор) попеременно переключает антенну между передатчиком и приемником так, чтобы использовалась только одна необходимая антенна;
- Антенна передает сигналы передатчика в пространство с требуемым распределением и эффективностью. Этот процесс применяется аналогичным образом при приеме;
- Передаваемые импульсы излучаются в пространство посредством антенны в виде электромагнитной волны, которая проходит по прямой линии с постоянной скоростью и будет затем отражаться от цели;
- Антенна принимает обратные рассеянные сигналы (так называемые эхо-сигналы);
- При приеме мультиплексор подает слабые эхо-сигналы на вход приемника;
- Сверхчувствительный приемник усиливает и демодулирует принятые СВЧ сигналы и выдает видеосигналы на выход;
- Индикатор представляет наблюдателю непрерывную графическую картину положения целей относительного радара

Существуют следующие методы обработки радиолокационных сигналов:

1) *Первичная обработка георадарных сигналов*.

Он основан на образовании сверхширокополосного импульса, имеющего от одного до нескольких колебаний тока. За основу алгоритма обнаружения сверхширокополосных георадарных сигналов и определения их характеристик предлагается использовать преобразование Гильберта. Преобразование Гильберта от действительной функции x(t) заключается в вычислении некоторой дополнительной функции y(t), у которой все спектральные компоненты имеют такой же модуль, но повернуты по фазе на 90 градусов, т.е. преобразование реализует функцию идеального фазовращателя.

2) *Обработка сигналов на встречных курсах*.

Рассматривается режим, когда полезная цель движется навстречу носителю РЛС. Этот режим называется сближением с целью в передней полусфере или режимом встречных курсов.

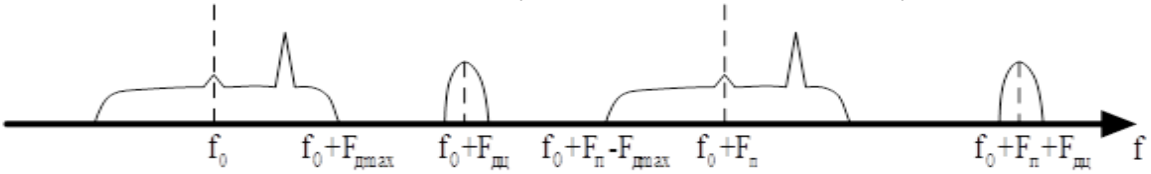


Рисунок 1 – Спектр соседних гармоник при отражении от земли и полезной цели

В этом методе необходимо выбирать частоту повторения излучения импульса такой, при которой спектр отражённых сигналов от цели находился в зоне, свободной от пассивных помех. В момент излучения импульса приёмник закрывается, что приводит к многократному его закрыванию в пределах, на которых обнаруживаются цели. При обнаружении цели за время наблюдения необходимо использовать несколько частот повторения, смена которых производится через определённый временной интервал.

3) *Обработка сигналов в импульсно-доплеровских РЛС.*

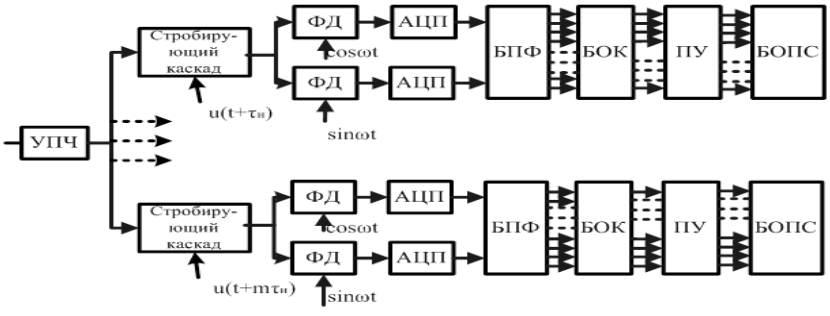


Рисунок 2 – Согласованный фильтр обработки

Здесь обнаружение сигналов от целей ведется на фоне шума приёмника. Отражённый сигнал от цели представляет пачку радиоимпульсов с неизвестной доплеровской частотой, которая подвергается когерентной обработке.

В этом случае в каждом стробируемом канале, ставят доплеровский фильтр, который и осуществляет обработку сигнала. Такой фильтр представлен на рисунке 2.

4) *Обработка сигналов на догонных курсах.*

Режим, когда полезная цель движется в одном направлении с носителем РЛС. Это наиболее сложный режим, потому что отраженные от цели сигналы могут попадать в область доплеровских частот мешающих отражений и обнаружение происходит на фоне пассивной помехи. Здесь можно использовать два режима: ВПЧ (скорость цели много больше скорости носителя), в иных случаях – СПЧ (обнаружение производится на фоне мешающих отражений от земной поверхности). Наиболее приемлемым является выбор частоты повторений, когда спектры отражений от подстилающей поверхности соседних гармоник соприкасаются (рис. 3).

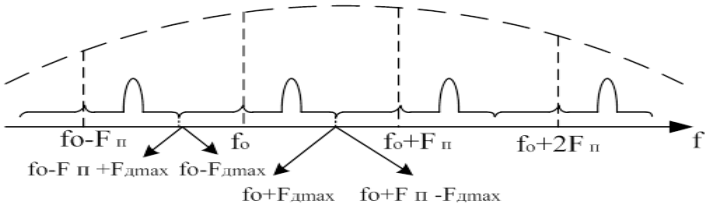


Рисунок 3 – Спектры отражений

5) Базовый алгоритм фильтрации квазинепрерывного сигнала

Этот метод основывается на алгоритме корреляционно-фильтровой обработки.

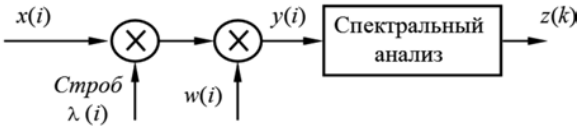


Рис. 4. Блок-схема алгоритма оптимальной фильтрации для одного канала дальности

На рис. 4 представлена схема фильтрации, где первый перемножитель выполняет операцию демодуляции сигнала, второй вводит весовую функцию для снижения боковых лепестков спектра. Для КН сигнала демодуляция для фиксированной дальности сводится к стробированию принятого сигнала пачкой импульсов, идентичной излученной, но сдвинутой на заданную дальность Весовые функции, как правило, синтезируются, исходя из уровня получаемых боковых лепестков спектра гармонического сигнала. Используют весовые функции малой степени и ступенчатые.

Выбор того или иного алгоритма основан на анализе статистических характеристик ошибок измерения координат и гипотез о возможной траектории движения объекта. Обработка принимаемых радиолокационных сигналов на фоне помех, как известно, сводится к вычислению достаточных статистик или практически реализуемых их приближений, т. е. к выполнению определенных математических операций над принимаемой смесью полезных сигналов и помех. Методы вычислений могут быть аналоговые и цифровые. К устройствам обработки радиолокационных сигналов предъявляют все возрастающие и одновременно противоречивые требования, а именно: расширение динамического диапазона входных сигналов; обеспечение обработки широкополосных, протяженных по времени сигналов; повышение точности, надежности; стандартизация; микроминиатюризация; упрощение эксплуатации; снижение стоимости.

Наибольшее значение в настоящее время приобрели цифровые методы обработки. Развиваются также новые методы аналоговой обработки: акустические, акустооптические, спиновые и др.

Список использованных источников:

1. Статья: Копейкин В.В. - Первичная обработка георадарных сигналов.

2. Горелик Г.С. Колебания и волны. – М.: ГИФМЛ, 1959. – 572 с.

3. Финк Л.М. Сигналы, помехи, ошибки. – М.: Радио и связь, 1984. – 256 с.

4. Бобров Д.Ю., Доброжанский А.П., Зайцев Г.В., Ма- ликов Ю.В., Цыпин И.Б., Цифровая обработка сигналов в многофункциональных РЛС. часть 2 – М., 2002, № 1, С. 28-39.

5. Зайцев Г.В. Класс весовых функций малого поряд- ка для спектрального анализа, оптимальных по минимакс-ному критерию. – Радиотехника, № 3, 2011, С. 21-32. 7.

6. Зайцев Г.В. Класс весовых функций для спект- рального анализа с высокой скоростью спада лепестков спектра и минимальным уровнем максимального боково- го лепестка. – Радиотехника, № 1, 2012, С. 55-65.

ЦЕНТРАЛИЗОВАННЫЕ ПРОГРАММНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЬЮ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Глушкевич Е.В.

Зеленин А.С. – м.т.н., зам. декана ФТК

В настоящее время системы управления необходимы для анализа состояния работы сети и проходящего по ней трафика на основе определенной системы мониторинга. Мониторинг сети и трафика, позволяющий в любой момент времени получить исчерпывающую информацию о состоянии сетевой инфраструктуры и характера проходящей по ней информации, занимает одно из ключевых мест в эффективном использовании ресурсов организации.

Системы управления сетью – централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью: включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п. Примерами систем управления могут служить популярные системы HP Open View, IBM Net View, Cacti, Zabbix, Nagios.

Система Zabbix создана для мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Это открытое решение распределенного мониторинга корпоративного класса, предоставляющее возможность проводить мониторинг многочисленных параметров сети, а также состояния и работоспособности серверов. С помощью Zabbix возможно настроить оповещения практически для любого события. Это дает возможность быстро среагировать на возможные проблемы сервера.

Процесс мониторинга подразумевает опрос данных и их получение. Все отчеты и статистика Zabbix, так же как и параметры настроек, доступны через веб-интерфейс. Веб-интерфейс имеет возможность отслеживания состояния сети и работоспособности серверов. На рисунке 1 представлена структурная схема системы мониторинга Zabbix:

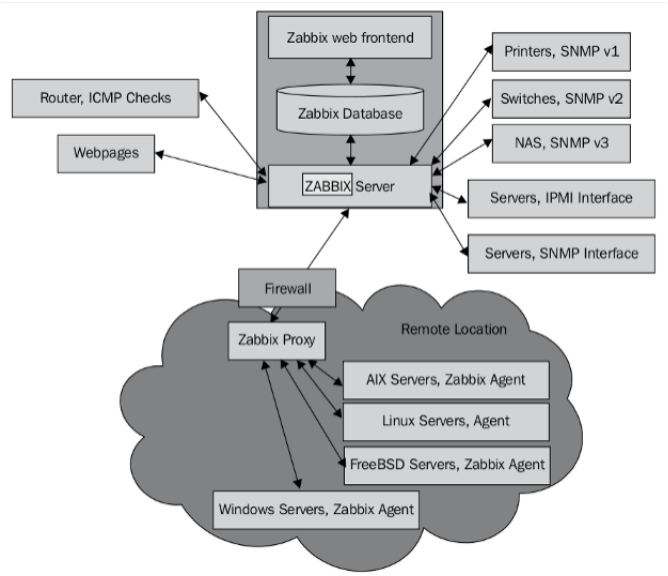


Рис. 1 - Структурная схема системы мониторинга Zabbix

Ядром программного обеспечения является Zabbix сервер, который позволяет удаленно проверять сетевые сервисы и хранить все конфигурационные, статистические и оперативные данные. Сервер является тем субъектом в программном обеспечении Zabbix, который оповестит администраторов в случае возникновения проблем с любым контролируемым оборудованием.

Zabbix прокси предназначен для сбора данных о производительности и доступности от имени Zabbix сервера. Все собранные данные заносятся в буфер на локальном уровне и передаются Zabbix серверу, к которому принадлежит прокси-сервер. Zabbix прокси используется для централизованного удаленного мониторинга сетей, не имеющих локальных администраторов.

Контроль локальных ресурсов и приложений (таких как жесткие диски, память, статистика процессора и т.д.) на сетевых системах осуществляется Zabbix агентом.

Центральный процессор (ЦП) – электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (код программ), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера.

Softirq является механизмом программных прерываний и связан с обработкой аппаратных прерываний ядром операционной системы. Обработчик аппаратного прерывания запрещает прерывания, выполняет необходимые действия и затем разрешает прерывания. Действия, выполняемые обработчиком, должны занимать как можно меньше процессорного времени.

График, представленный на рисунке 2, характеризует процент программных прерываний в определенный момент времени.

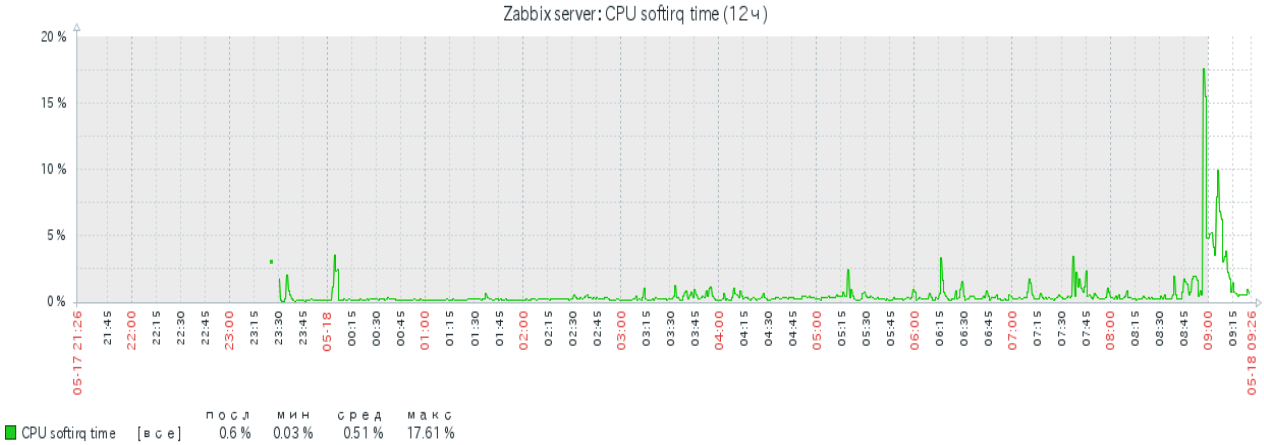


Рис. 2 - Процент программных прерываний в определенный момент времени

В соответствии с графиком большую часть времени количество возникавших на сервере процессов было минимальным – на уровне 0,5…2,5%. И только между 8.56-8.58 замечен резкий рост до 17.61%, что свидетельствует о том, что в это время на сервере было запущено большое количество процессов, не способных выполняться одновременно. По мере их выполнения график постепенно снижался к стандартным значениям.

Показатель interrupts per second (рисунок 3) характеризует количество прерываний процессора, включая прерывания таймера, в секунду. Если число прерываний превышает 10 000 в секунду, то это свидетельствует либо о проблемах с устройствами (аппаратные прерывания), либо о наличии ошибок в программном обеспечении (в случае программных прерываний).

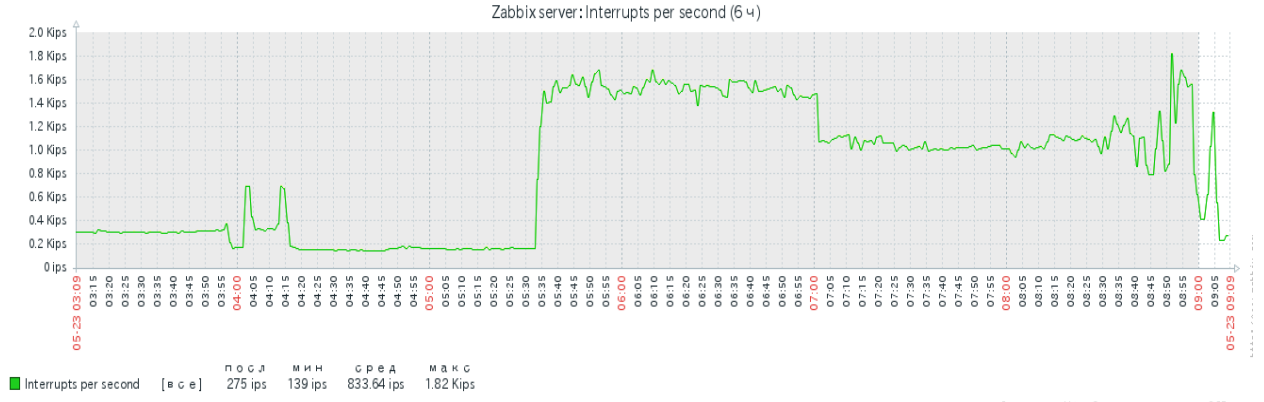


Рис. 3 - Число прерываний в секунду (interrupts per second)

Из полученных данных видно, что максимальное число прерываний находится на уровне 1680sps, следовательно, аппаратных проблем и ошибок ПО в момент исследования не наблюдалось.

Система мониторинга и управления Zabbix значительно упрощает работу системного администратора, дает возможность контролировать внутренние сетевые процессы, а также быстро реагировать на возможные угрозы неисправностей с помощью системы оповещения.

Список использованных источников:

1. Олифер Н. Средства анализа и оптимизации локальных сетей / Н. Олифер, В. Олифер – СПб: ЦИТ, 2000. – 379 с.

2. Олифер Н. Компьютерные сети. Принципы, технологии, протоколы / Н. Олифер, В. Олифер – СПб: Питер, 2015. – 992 с.

3. Руководство по Zabbix [Электронный ресурс]. – Режим доступа : https://www.zabbix.com/ documentation/3.2/ru/ma nual/

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ ЛИНЕЙНОЙ СВЕРТКИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Латушкин К.Ю., Фам М.Т., Шаюнов Е.М., Конюх В. А.
Печень Т.М. – ассистент

Представить современный мир лишенный всякого рода информации так же трудно как и представить его без различных цифровых устройств и приборов. В сочетании эти 2 аспекта жизни человека XXI века представляют собой сложные многоуровневые системы передачи, включающими в свой функционал формирование и обработку различных сигналов. Индустрия связи в республике развивается высокими темпами, недавний переход от работы с аналоговыми сигналами к работе с цифровыми произвел некий прорыв в науке и инженерии страны. ЦОС (Цифровая обработка сигналов) теперь занимает центральное место в сфере телекоммуникаций как в прикладной, так и в научной средах.

Линейная свертка – основная операция ЦОС, особенно в режиме реального времени. Свертка подразумевает не только отображение воздействия системы на передаваемый ей сигнал в рамках его обработки как результат, но и сам процесс, являясь при этом одним из важнейших этапов в формировании сигнала.

Математическим аппаратом линейной свертки является частный случай алгоритмов ДПФ (Дискретное преобразование Фурье) – алгоритмы БПФ (Быстрое преобразование Фурье). Поскольку такие алгоритмы существуют, возникает следующий метод вычисления свертки двух последовательностей:

1) вычисление N-точечного ДПФ для каждой из двух последовательностей;
2) нахождение произведения между полученными ДПФ;
3) восстановление последовательности, полученной в результате взаимодействия двух известных нам последовательностей, по ее ДПФ [1].

Принцип реализации линейной свертки представлен на рисунке 1:

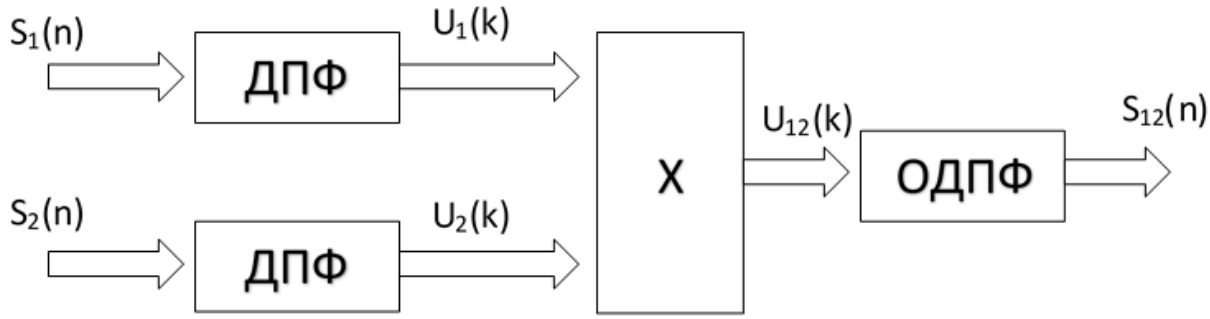


Рис. 1 – Структура линейной свертки

Для свертки характерны такие свойства как:

1. дистрибутивность ($(f_1+f_2)*g = f_1*g + f_2*g$);
2. ассоциативность ($f*(g*h) = (f*g)*h$);
3. коммутативность ($f*g = g*f$).

Алгоритмы БПФ основываются на фундаментальной идее, заключающейся в разбиении вычисления ДПФ N-членной последовательности на ряд достаточно малых ДПФ. В зависимости от способа, которым проводится разбиение, получается тот или иной конкретный алгоритм, однако все они заметно увеличивают скорость преобразований. Исходя из этого свертку можно разделить на следующие подвиды:

1. свертка, формируемая на основе БПФ с прореживанием по времени
2. свертка, формируемая на основе БПФ с прореживанием по частоте

Первый вид (прореживание по времени), обязан своим названием тому, что при организации вычислений последовательность x[n] (традиционно считающаяся зависящей от времени) разбивается на меньшие подпоследовательности. Во втором классе алгоритмов на части разбивается последовательность коэффициентов ДПФ X[к], в связи с чем их называют прореживанием по частоте.

Метод линейной свертки широко применяется в области радиотехники при работе с сигналами во временной области посредством АЦСУ (Адаптирующего цифрового сверточного устройства). АЦСУ используется в комплексах скрытой радиолокации, в радиолокационных системах с разнесенными приемными и передающими позициями, а также в других областях [2].

Достигаемым техническим результатом изобретения является расширение функциональных возможностей за счет адаптации к изменению параметров и вида модуляции сигналов опорного передатчика.

В данной работе были проведены экспериментальные исследования в специализированных программах MathCad, MATLAB и ФАиС (разработана на кафедре СТК под руководством В. А. Овсянникова).

Список использованных источников:

1. Оппенгейм А., Шафер Р. Цифровая обработка сигналов // ЗАО “РИЦ “ТЕХНОСФЕРА””, 2006. – 856с.
2. Устройство для вычисления дискретного косинусного преобразования // www.freepatent.ru

ВИРТУАЛЬНЫЕ ЧАСТЫЕ СЕТИ VPN НА ОСНОВЕ ТЕХНОЛОГИИ MPLS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Скрипелёва А.А.

Саломатин С.Б. – к.т.н.,доцент

На сегодняшний день большинство организаций и предприятий имеют территориально распределенную структуру, вследствие чего возникает необходимость объединения локальных вычислительных сетей территориально распределенных филиалов в одну корпоративную сеть. Кроме того, существуют проблемы защиты информации, аутентификации и авторизации пользователей, предоставления доступа к ресурсам, обеспечение независимости адресных пространств. Эти задачи в настоящее время помогает решить технология виртуальных частных сетей VPN (Virtual Privat Network).

Под термином VPN понимают круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети.

Построение виртуальной частной сети учреждения, например, для обеспечения документооборота устанавливает следующие задачи: обеспечение защиты соединения, требуемого качества обслуживания, низкую стоимость и расширяемость инфраструктуры. Для решения поставленных задач построения VPN используют технологию MPLS (MultiProtocol Label Switching).

Цель создания VPN на основе технологии MPLS для обеспечения документооборота предприятия — моделирование системы массового обслуживания с входящим самоподобным потоком, которая предоставляет необходимую пропускную способность канала передачи, а так же размер выходного буфера, в соответствии с интенсивностью поступающей нагрузки, требуемым задержкам и вероятностью потерь пакетов.

Защита соединения в сетях MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов. BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться. Членство в VPN зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика. Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям MPLS-VPN очень высокий уровень защищенности.

Для обеспечения дополнительной защиты соединения со стороны клиента могут устанавливаться межсетевые экраны (например, Cisco ASA).

На рисунке 1 приведен пример VPN-сети, создаваемой провайдером.

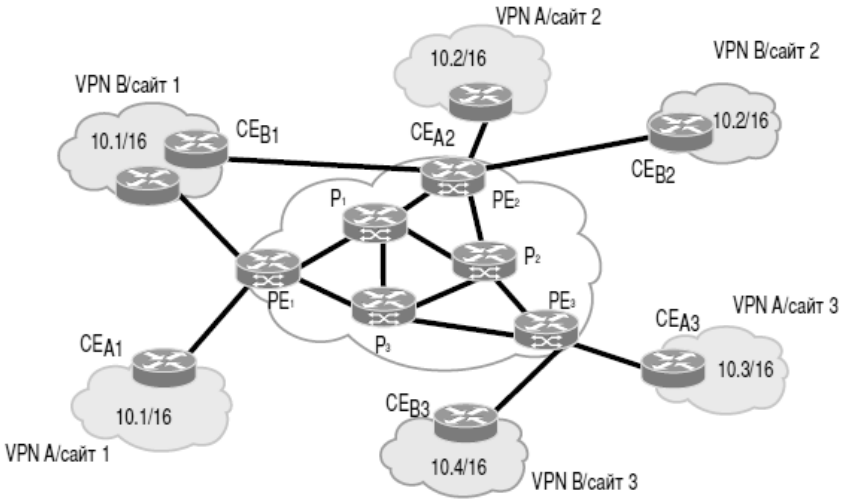


Рис. 1 - Виртуальная частная сеть MPLS

Информационные потоки в пакетной транспортной сети проявляют свойства самоподобия. Задачей выбора параметров магистрального канала является расчет необходимой пропускной способности канала

передачи, а так же размера выходного буфера.

Работу магистрального канала с выходным буфером можно описать моделью систем массового обслуживания с входящим самоподобным потоком и детерминированным временем обслуживания: $f_{BM}/D/1$ (f_{BM} – фрактальное броуновское движение, являющееся самоподобным процессом; D – детерминированный процесс обслуживания; 1 – одно устройство обслуживания, в нашем случае - канал передачи с буфером).

Данная система - $f_{BM}/D/1$ имеет аналитическое решение в виде формулы Норроса:

$$x = \frac{p^{1/(2(1-H))}}{(1-p)^{H/(1-H)}}$$, где p = λ/μ – коэффициент использования ресурса сети; λ – интенсивность поступающей нагрузки; μ – интенсивность обслуживания нагрузки, а в нашем случае и есть искомая пропускная способность; H – параметр Херста, для самоподобных процессов H = 0,9; x – необходимый объем выходного буфера.

$$T = \frac{1}{\lambda}\left[(y * \left(\frac{1}{c} + \frac{y}{c} * \frac{(y*c)^{\frac{2H-1}{2(1-H)}}}{(c-y)^{\frac{H}{1-H}}}\right)\right]$$, где T – задержка пакета, складывающаяся из времени нахождения пакета в очереди и времени передачи пакета по каналу связи.

Таким образом, исходя из параметра входящего информационного потока, мы можем выбрать такую пропускную способность канала, при которой рассчитанный размер буфера будет обеспечивать требуемые задержки пакетов в канале связи.

Для осуществления документооборота учреждения рассчитаем параметр информационного потока передачи данных:

$$\lambda_{DATA} = \frac{y_{DATA}}{n}$$, где n – длина пакета (примем n = 1500 байт = 12000 бит).

При самоподобном входящем потоке резкое возрастание задержек пакетов происходит уже при ρ = 0,6. Рассчитаем необходимый размер буфера и задержку пакета для ρ Є [0,6:1), с шагом 0,1, результаты приведем в таблицу:

y, Мб/с	λ, пак/с	c, Мб/с	μ, пак/с	p	x, пак	T, с
774,9	58002	1160,04	96670	0,6	297	0,031264
774,9	58002	994,32	82860	0,7	8539	3,112616
774,9	58002	870,036	72503	0,8	640001	3850,691
774,9	58002	782,052	65171	0,89	236818632	3,64662E+13

По полученным значениям построим график зависимости задержки от величины пропускной способности канала при фиксированной нагрузке y, Мб/с:

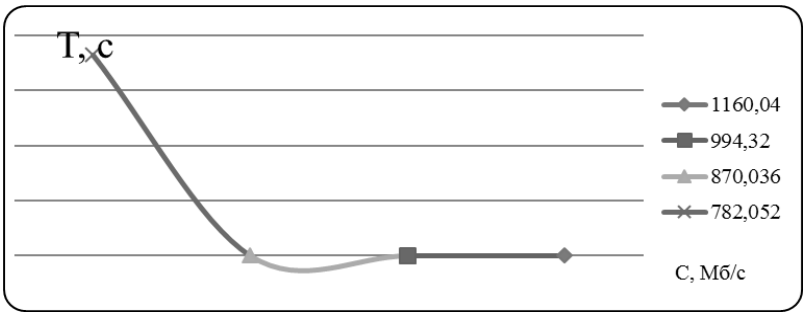


Рис. 2 - График зависимости задержки на передачу от пропускной способности канала

Как видно из таблицы необходимое значение пропускной способности лежит в пределах c = 994,32-1160,04 Мб/с.

Рассчитаем параметры задержки и необходимый размер буфера для ρ Є [0,6:0,7], с шагом 0,01 аналогичным образом и получим, что необходимо выделить для передачи данных полосу пропускания со скоростью не менее 1141,032 Мб/с.

Данная модель VPN MPLS предоставляет необходимую полосу пропускания, позволяет избежать перегрузок канала, роста задержки передачи пакетов и потерь в соответствии с качеством обслуживания QoS.

Список использованных источников:

1. Cisco Systems, Построение виртуальных частных сетей (VPN) на базе технологии MPLS
2. Бехингер М. Безопасность MPLS VPN. – Индианаполис: Cisco Press, 2005. – 312с.
3. Гейн Л. Основы MPLS. – Индианаполис: Cisco Press, 2007. – 651 с.

АЛГОРИТМ СЖАТИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ КОДИРОВАНИЯ ДЛИН СЕРИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Панас В.А.

Цветков В.Ю. – д.т.н.,доцент

В настоящее время задача разработки и исследования новых методов сжатия данных является актуальной научной и прикладной задачей. Особенно актуальной она становится в условиях ограниченности временных и вычислительных ресурсов. В таких условиях является целесообразным использования алгоритмов сжатия на основе кодирования длин серий RLE.

RLE (кодирование длин серий) – алгоритм сжатия данных, заменяющий повторяющиеся символы (серии) на один символ и число его повторов. Серией называется последовательность, состоящая из нескольких одинаковых символов. При кодировании (упаковке, сжатии) строка одинаковых символов, составляющих серию, заменяется строкой, содержащей сам повторяющийся символ и количество его повторов[1].

Классическая реализация алгоритма RLE является малоэффективной при кодировании сжатых данных в двоичном виде[2]. Этот факт является предпосылкой к поиску путей улучшения алгоритма кодирования длин серий. Предлагается модификация классического алгоритма RLE, основанная на разложении полутоновых изображений на битовые плоскости и выборе оптимальной битовой длины блока данных.

Структурная схема модифицированного алгоритма RLE представлена на рисунке 1:

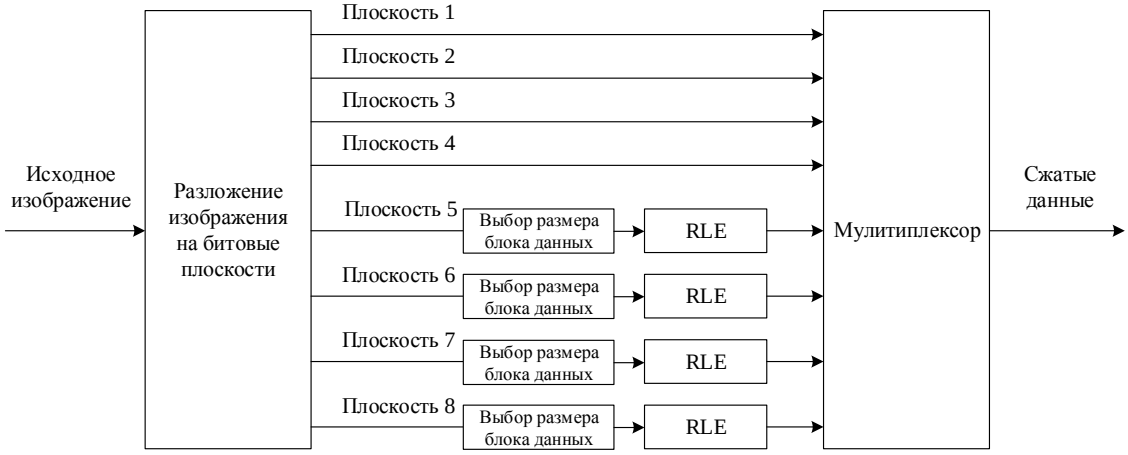


Рис. 1 – Структурная схема алгоритма сжатия на основе кодирования длин серий

На первом этапе алгоритма происходит разложение исходного полутонового изображения на битовые плоскости. Это позволяет сократить диапазон значений пикселей и увеличить число серий из повторяющихся пикселей. На втором этапе происходит выбор оптимальной битовой длины блока данных для каждой плоскости. Таким образом предотвращается нерациональное использование старших битовых разрядов блока данных, имеющее место в классическом алгоритме. После этого следует этап кодирования длин серий, после чего все закодированные данные объединяются с помощью мультиплексирования.

Кроме того, из рисунка 1 видно, что к младшим битовым плоскостям не применяется процедура сжатия. Это обусловлено тем, что младшие плоскости представлены в виде шумов, а семантическая информация появляется на старших битовых плоскостях. Количество сжимаемых плоскостей варьируется для каждого изображения.

Разработанный алгоритм обеспечивает более высокую степень сжатия, чем классический алгоритм RLE и практически не уступает ему во времени выполнения. Схема сжатия нового алгоритма изменяется в зависимости от характера изображения. Это позволяет получать для каждого изображения оптимальные коэффициенты сжатия.

В дальнейшей работе планируется дальнейшая модификация предлагаемого алгоритма.

Список использованных источников:

1. Сэломон, М. Сжатие данных, изображений и звука / М. Сэломон. – М. : Техносфера, 2004. – 368 с.

2. Аль-Бахдили, Х. К. Сжатие полутоновых изображений без потерь на основе кодирования длин серий / Аль-Бахдили Х. К [и др.] // Доклады БГУИР. – 2016. – №2. – С. 63–69.

АНАЛИЗ МЕТОДОВ ВЫДЕЛЕНИЯ ГРАНИЦ НА ИЗОБРАЖЕНИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Буко Я.Ф., Чернушевич П.В.

Макейчик Е.Г. – ст. преподаватель

Выделение границ (выделение краев) — термин в теории обработки изображения и компьютерного зрения, частично из области поиска объектов и выделения объектов, основывается на алгоритмах, которые выделяют точки цифрового изображения, в которых резко изменяется яркость или есть другие виды неоднородностей [1]

В настоящее время, детектирование границ используется для таких целей, как распознавание текста, идентификации и параметризации объектов и др. Для получения границ изображения существует большое количество различных методов: методы Робертса [2], Прюитта [3], Собеля [4], Лапласа [5]. Все эти методы основываются на преобразовании изображения с помощью скользящей маски, которая соответствует группе пикселей используемого изображения.

Один из исторически первых методов выделения границ был метод Робертса, использующий маски 2×2:

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \text{ и } \begin{bmatrix}0 & +1\\ -1 & 0\end{bmatrix}$$

Реализация масок размерами 2×2 не очень удобна, т.к. у них нет четко выраженного центрального элемента, что существенно отражается на результате выполнения фильтрации. Но этот «минус» порождает очень полезное свойство данного алгоритма – высокую скорость обработки изображения.

Оператор Прюитта вычисляется с использованием масок размерами 3×3:

$$\begin{bmatrix}-1 & 0 & 1\\ -1 & 0 & 1\\ -1 & 0 & 1\end{bmatrix} \text{ и } \begin{bmatrix}-1 & -1 & -1\\ 0 & 0 & 0\\ 1 & 1 & 1\end{bmatrix}$$

Оператор Собеля тоже использует область изображения 3x3:

$$\begin{bmatrix}-1 & 0 & 1\\ -2 & 0 & 2\\ -1 & 0 & 1\end{bmatrix} \text{ и } \begin{bmatrix}-1 & -2 & -1\\ 0 & 0 & 0\\ 1 & 2 & 1\end{bmatrix}$$

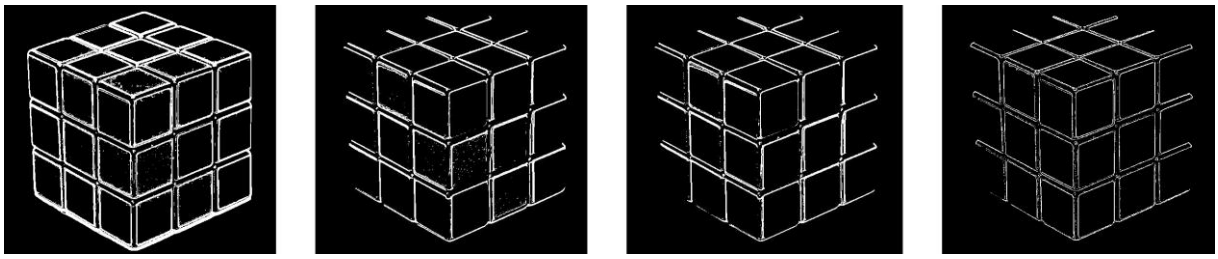
Он довольно похож на оператор Прюитта, а видоизменение заключается в использовании весового коэффициента 2 для средних элементов. Это увеличенное значение используется для уменьшения эффекта сглаживания за счет придания большего веса средним точкам. При наличии центрального элемента и малой ресурсоемкости этому оператору, как и оператор Прюитта, свойственна высокая чувствительность к шумам и ориентации границ областей, а также возможность появления разрывов в контуре.

Оператор Лапласа использует маску размера 3×3:

$$\begin{bmatrix}0 & 1 & 0\\ 1 & -1 & 1\\ 0 & 1 & 0\end{bmatrix}$$

Основным недостатком лапласиана является очень высокая чувствительность к шумам. Кроме того возможны появления разрывов в контуре, а также их удвоение. К достоинствам его можно отнести то, что он нечувствителен к ориентации границ областей, и малую ресурсоемкость.

Описанные методы реализованы в среде разработки MATLAB. Результаты обработки изображения описанными операторами представлены на рисунке 1.



а) б) в) г)

Рисунок 1 – Результаты обработки изображения операторами: а) Робертса; б) Прюитта; в) Собеля; г) Лапласа

Из рисунка 1 видно, что метод Робертса показывает наилучшие результаты.

Список использованных источников:

1. Джесси Рассел, Рональд Кон. Выделение границ.

2. Roberts, L. Machine Perception of 3D Solids / L. Roberts // Optical and Electro-optical Information Processing, – 1965, – Vol. 1, – P. 159–197.

3. Samuel J. Dwyer III. A personalized view of the history of PACS in the USA. In: *Proceedings of the SPIE*, «Medical Imaging 2000: PACS Design and Evaluation: Engineering and Clinical Issues», edited by G. James Blaine and Eliot L. Siegel. 2000;3980:2-9.

4. Duda R., Hart P. Pattern Classification and Scene Analysis. — John Wiley and Sons, 1973. — P. 271—272.

5. Chen, J. S. Fast convolution with Laplacian-of-Gaussian masks [Text] / J. S. Chen, A. Huertas, G. Medioni // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1987. – Vol. 9, Issue 4. – P. 584–590. doi: 10.1109/tpami.1987.4767946

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ПО ВИДЕОНАБЛЮДЕНИЮ НА БАЗЕ ОБОРУДОВАНИЯ D-LINK

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Овчинникова Е.А.
Цветков В.Ю. – д.т.н., профессор

Современная система видеонаблюдения представляет собой программный комплекс, состоящий из видеокамер, мониторов, регистраторов и программного обеспечения. Благодаря распространению высокоскоростного интернета и возможностей мобильной связи функциональные возможности систем видеонаблюдения значительно расширились. Помимо выполнения традиционных охранных функций, системы видеонаблюдения широко используются для наблюдения за различными объектами в режиме реального времени с фиксацией происходящего на накопители информации.

Обеспечение безопасности и видеоконтроля в аэропортах, на улицах городов, стадионах, в метрополитене и прочих объектах - это лишь малая часть области применения систем видеонаблюдения. Поэтому современным специалистам в области инфокоммуникаций и тем, кто только собирается им стать, стоит обратить внимание на данный сектор развития сетевых технологий.

На кафедре Систем Телекоммуникаций БГУИРа планируется разработка ряда лабораторных работ, в ходе выполнения которых студентами данного ВУЗа будут изучены основы функционирования и настройки различного оборудования видеонаблюдения. Планируется, что студентам будет предложена возможность выполнения лабораторных работ как непосредственно в учебных лабораториях БГУИРа, так и при помощи метода дистанционного доступа к имеющемуся оборудованию.

Системы видеонаблюдения делятся на 2 вида: проводные и беспроводные. Персональный выбор того или иного вида зависит от особенностей объекта видеонаблюдения, используемого оборудования, финансовых возможностей и предпочтений пользователей. Основной элемент систем видеонаблюдения - это видеокамера. В зависимости от типа используемых видеокамер все системы видеонаблюдения классифицируют на цифровые и аналоговые видеосистемы. Отличительной чертой аналоговых систем является их простота и относительно невысокая стоимость оборудования. Но при планировании устройства систем видеонаблюдения необходимо осознавать, что аналоговое оборудование уже морально устарело и по многим своим функциональным качеством уступает приборам, работающим на цифровых технологиях, таким как, к примеру, IP-камеры.

IP-камера - это цифровое устройство, предназначенное для осуществления видеосъемки, оцифровки и сжатия видеоизображения. Обработанное видеоизображение IP-камера передает, используя протокол IP (Internet Protocol - протокол межсетевого обмена).

Рынок видеонаблюдения активно развивается. Ведущие производители активно внедряют в свои продукты новый функционал, тем самым показывая весомые отличия между оборудованием различных компаний.
Основными производителями оборудования для видеонаблюдения на сегодняшний день можно назвать такие компании, как HikVision, Samsung, Sony, Panasonic, MicroDigital и D-Link.

Компания D-Link - мировой производитель сетевого и телекоммуникационного оборудования. D-Link предлагает широкий набор решений для домашних пользователей, корпоративного сегмента и провайдеров интернет-услуг. 127 региональных офисов компании D-Link осуществляют продажу и поддержку оборудования на территории более чем 100 стран мира.

Компания предлагает широкий ассортимент оборудования для организации системы видеонаблюдения:

- Камеры:
  - ✓ Фиксированные камеры (для помещений и для наружного наблюдения),
  - ✓ Антивандальные
  - ✓ Поворотные;
  - ✓ Купольные и др.
- Коммутаторы
- Точки доступа
- PoE-инжекторы
- Модемы и др.

Важной составляющей качественной системы видеонаблюдения является не только аппаратная, но и программная часть. Программное обеспечение должно давать возможность просматривать, записывать, обрабатывать и хранить изображение с IP-камер, сортировать записи по любому заданному параметру,

поворачивать видеорегистраторы в требуемую сторону, укрупнять изображение, повышать четкость, отправлять тревожные сообщения на e-mail или сервер и др.

Компания D-Link предоставляет программное обеспечение D-ViewCam DCS-100. Это универсальная система видеонаблюдения, предоставляющая возможность централизованного управления и отображения информации в реальном времени с 32 сетевых камер. Режим карты позволяет создавать карты на основе размещения и положения камер. Все подключенные камеры для удобства просмотра отображаются в древовидном списке устройств. Дополнительные функции, такие как автоматическое патрулирование, поворот, увеличение и фокусировка, обеспечивают оптимальное управление системой видеонаблюдения.

Таким образом, можно с уверенностью сказать, что среди основных производителей систем видеонаблюдения компания D-Link является одним из наиболее благоприятных вариантов для сотрудничества. Оборудование, предоставленное данной компанией, является недорогим, качественным и надежным решением для построения курса лабораторных работ.

Список использованных источников:

1. http://www.dlink.by/by/products/
2. http://systemmanager.by/ur/ip-video/
3. http://nabludau.ru/postroenie-ip-videonablyudeniya-na-predpriyatii-ili-v-torgovom-zale/
4. http://www.dlink.ru/by/products/1433/1820.html

ВЫДЕЛЕНИЕ ПРЯМЫХ ЛИНИЙ НА ИЗОБРАЖЕНИИ БЛА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Крамков Д.А.

Шевчук О.Г. – ассистент каф. СиУТ

Существует огромное количество разных алгоритмов для поиска прямых линий на изображении. Каждый из них по своему хорош. В данной работе использовался метод Line Segment Detector (LSD). К примеру, по сравнение с методом Хафа метод LSD имеет ряд преимуществ, а именно скорость нахождения линий, точность нахождения и др.

Цель работы – Исследования метод Line Segment Detector на изображениях БЛА.

ЛСД предназначен для обнаружения локально прямых контуров на изображениях. Это то, что называется сегментами линии. Контуры это зоны изображения, где уровень яркости изменяется достаточно быстро – от темного до светлого или наоборот. Поэтому основе данного алгоритма лежит вычисление градиента (рисунок 1) каждого пикселя изображения с маской размерностью 2×2 пикселей (рисунок 2) , их объединении в линейные сегменты и последующем уточнении.

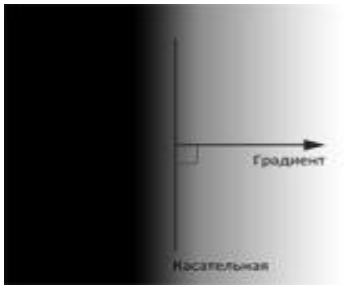


Рис. 1 – Градиент

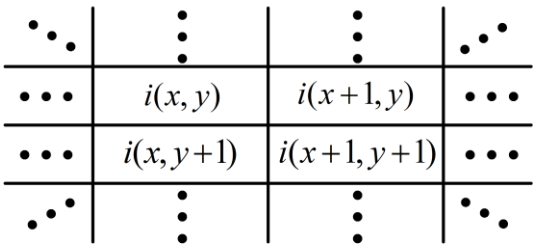


Рис. 2 – Вычисление градиента маской 2 × 2 пикселей

Таким образом, градиент и линии уровня изображения являются ключевыми понятиями. Алгоритм начинается с вычисления угла линии-уровня в каждом пикселе для создания поля. Затем это поле квантуется на связанные области пикселей, которые совместно используют одну и ту же линию-уровня. Квантованные линейные элементы считаются схожими, если $\Delta\theta_i \le \mu$ при $\mu = \frac{\alpha \cdot q}{i \cdot (|\varepsilon_x| + 1)}$, где ε_x – допустимое отклонение, а α – минимальное число пикселей между двумя квантованными направленными элементами. Эти связанные области называются областями поддержки линии.

Каждая область поддержки линии «набор пикселей» является кандидатом на сегмент линии. Соответствующий прямоугольник должен быть связан с ним. Основная инерционная ось области поддержки линии используется в качестве основного направления прямоугольника. Каждый прямоугольник подвергается процедуре проверки. Пиксели в прямоугольнике, угол линии-уровня которых соответствует углу прямоугольника называются выровненными точками. Общее количество пикселей в прямоугольнике подсчитываются и используются для проверки правильности прямоугольника как обнаруженного сегмента линии.

Для тестирования алгоритма LSD исходное изображение получено с помощью БЛА было повёрнуто на 45 градусов по часовой и против часовой стрелки. Так же изображение подверглось увеличению и уменьшению яркости на 30 процентов. Результаты работы алгоритма изображены на рисунке 3.

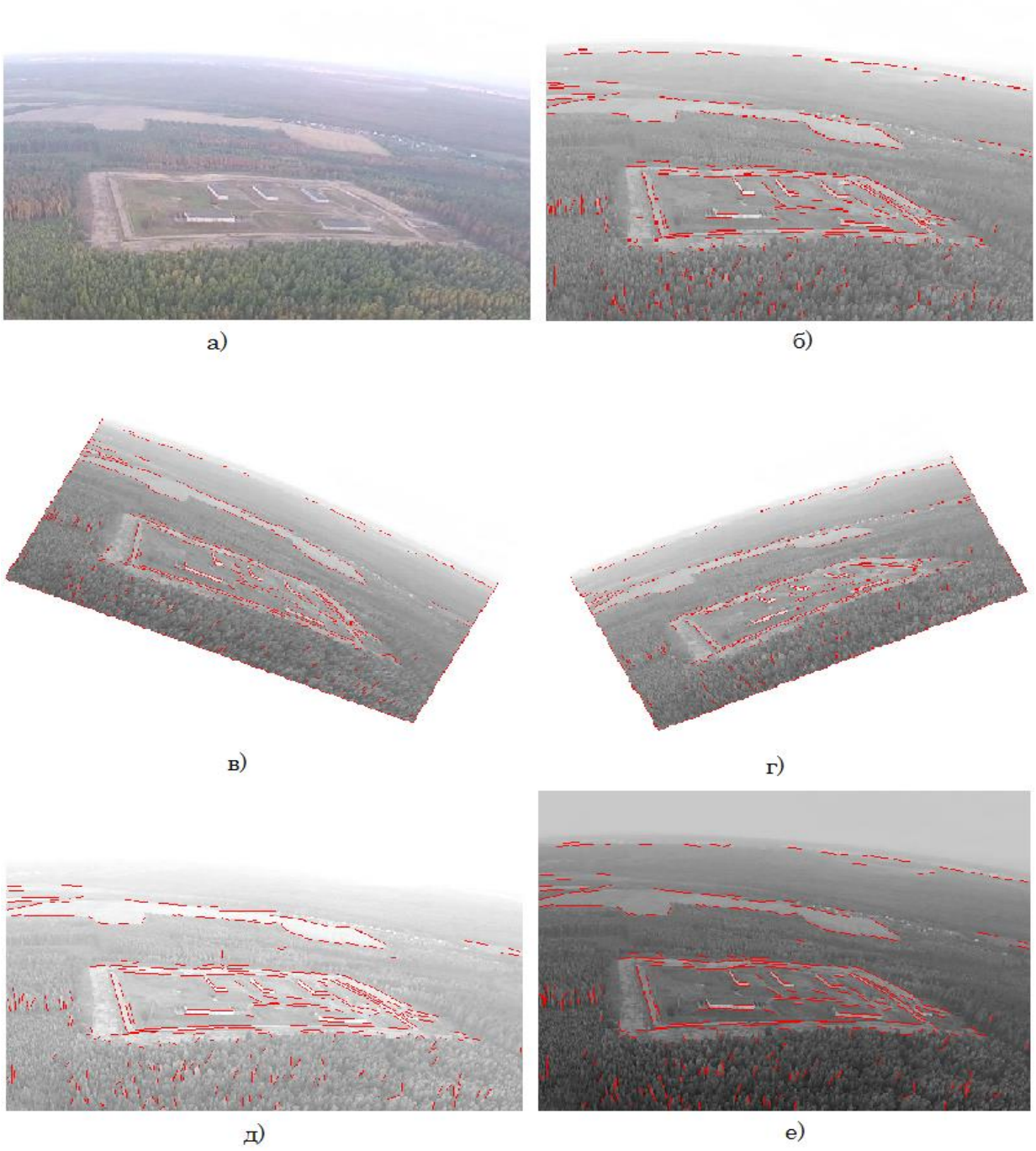


Рис. 3 – Результаты метода Line Segment Detector: а) исходное изображение б) обработка исходного изображения в) при повороте на 45 градусов г) при повороте на -45 градусов д) при увеличении яркости е) при уменьшении яркости

Из рисунка 3 видно, что количество линий, найденное на изображения БЛА с использованием метода LSD, практически не изменяется при повороте и изменении его яркости.

Список использованных источников:
1. http://docs.opencv.org/3.0-beta/modules/line_descriptor/doc/LSDDetector.html
2. http://cvrs.whu.edu.cn/projects/cannyLines/

СЕГМЕНТАЦИЯ МЕТОДОМ ВОДОРАЗДЕЛА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тынкович Т.П., Милютин А. Я.
Шевчук О.Г. – ассистент каф. СиУТ

Довольно часто при анализе изображений возникает задача разделения пикселей изображений на группы по некоторым признакам. Такой процесс разбиения на группы называется сегментацией. Существует большое множество методов сегментации изображения. Часто для решения задачи связанной с соприкасающимися предметами на изображении используется так называемый метод маркерного водораздела. [1] Предлагается рассматривать изображение как некоторую карту местности, где значения яркостей представляют собой значения высот относительно некоторого уровня. Если эту местность заполнять водой, тогда образуются бассейны. При дальнейшем заполнении водой, эти бассейны объединяются. Места объединения этих бассейнов отмечаются как линии водораздела.

Метод маркерного водораздела является одним из наиболее эффективных методов сегментации изображений. При реализации этого метода выполняются следующие основные процедуры:

1) Вычисляется функция сегментации. Она касается изображений, где объекты размещены в темных областях и являются трудно различимыми.
2) Вычисление маркеров переднего плана изображений. Они вычисляются на основании анализа связности пикселей каждого объекта.
3) Вычисление фоновых маркеров. Они представляют собой пиксели, которые не являются частями объектов.
4) Модификация функции сегментации на основании значений расположения маркеров фона и маркеров переднего плана.
5) Вычисления на основании модифицированной функции сегментации.

Для начала, преобразуем наше изображение используя градацию серого (см. рис.1).

Рис. 1 - Grayscale

Для вычисления значения градиента используется оператор Собеля. [2] Градиент имеет большие значения на границах объектов и небольшие (в большинстве случаев) вне границ объектов.

Таким образом, вычислив значения градиента, можно приступить к сегментации изображений с помощью рассматриваемого метода маркерного водораздела.

Для маркировки объектов переднего плана могут использоваться различные процедуры. Мы будем использовать морфологические технологии, которые называются "раскрытие через восстановление" и "закрытие через восстановление". Эти операции позволяют анализировать внутреннюю область объектов изображения. После процедуры маркировки, мы непосредственно выполняем операцию сегментации на основе водораздела. [3] Далее, отобразим на исходном изображении наложенные маркеры переднего плана, маркеры фона и границы сегментированных объектов (см. рис. 2).

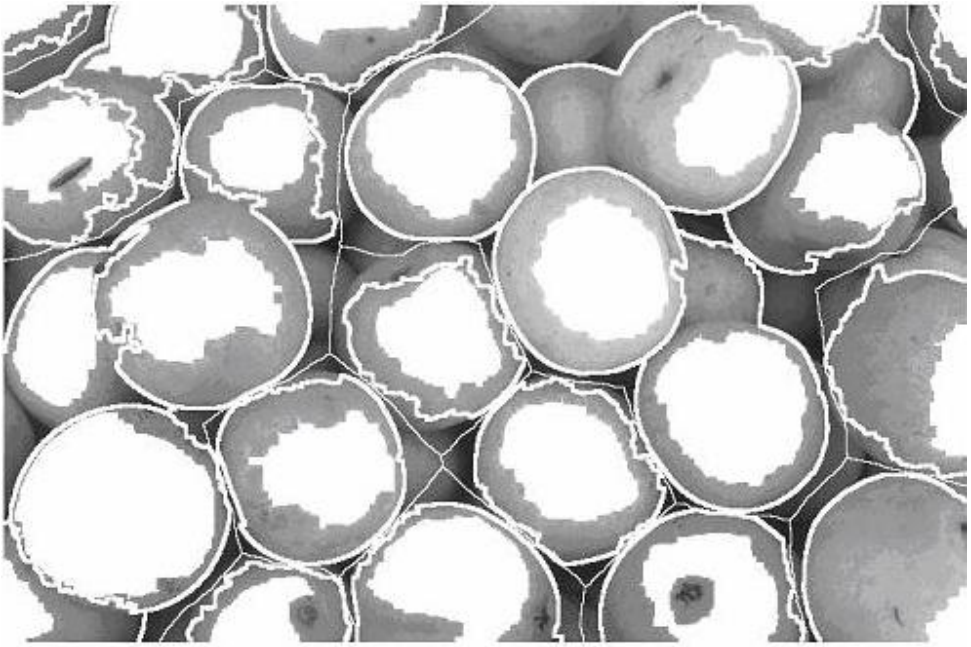


Рис.2 – Маркеры и границы объектов, наложенные на исходное изображение

В результате такого отображения можно визуально анализировать месторасположение маркеров переднего плана и фона.

Список использованных источников:

1 Robert Laganière, OpenCV *2 Computer Vision Application Programming Cookbook*. – 131с.
2. Adrian Kaehler, Gary Bradski, *Learning OpenCV*. – 204с.
3. Adrian Kaehler, Gary Bradski, *Learning OpenCV*. – 402с.

АНАЛИЗ АЛГОРИТМОВ СОВМЕЩЕНИЯ ИЗОБРАЖЕНИЙ, ОСНОВАННЫХ НА ВЫДЕЛЕНИИ ГРАНИЦ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Горбуков А.Д.

Костусев А.В. – аспирант каф. СиУТ

Проблема совмещения изображений заключается в установлении соответствия между точками двух или более изображений. Данная проблема является фундаментальной проблемой компьютерного зрения, поскольку необходимость совмещения изображений возникает при решении таких задач, как выявление изменений в серии изображений, анализ движения, объединение информации от различных сенсоров, стереозрение, текстурный анализ и компенсация движения камеры. Подобные проблемы, в свою очередь, возникают в биомедицинских приложениях, при решении задач фотограмметрии и в зрении роботов, при дистанционном сборе данных, поэтому практическая полезность автоматического совмещения изображений несомненна.

В данной работе рассмотрены различные методы совмещения изображения для компенсации движения камеры, используемые для дальнейшего построения гиперспектральных изображений земной поверхности.

В качестве основного эталонного алгоритма был выбран поиск минимальной разности пересекающейся области, путем полного перебора. Однако данное утверждение требует дальнейшей проверки, так как комплексная оценка результатов может быть проведена только после получения самих гиперспектральных изображений.

Получаемые с камеры изображения, как можно увидеть на рисунке 1, имеют особую специфику в следствии технических особенностей оборудования. Поэтому для дальнейшего использования в стабилизационных методах используется только верхние 12 пикселей.

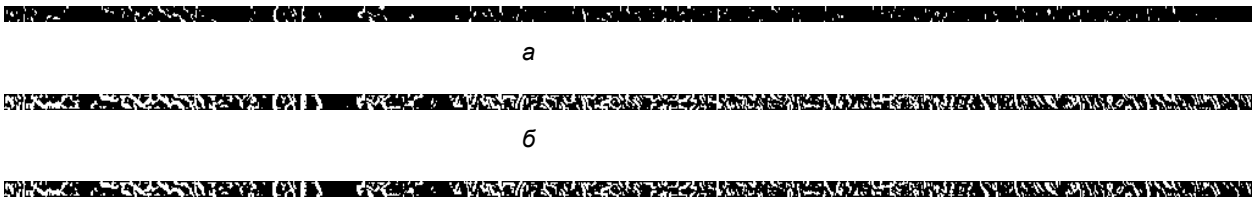
Рис. 1 – Пример исходного изображения

Реализованные алгоритмы можно разделить на две группы:

1. Использующие найденные границы в качестве маски для дальнейшего нахождения пересечения с минимальным средним значением разницы яркости между двумя соседними кадрами;
2. Находят пересечение с максимальным перекрытием найденных границ.

Так же их можно разделить на 3 группы по типу использованного оператора для нахождения границ:

1. Оператор Робертса;
2. Оператор Собеля;
3. Оператор Превитта.



а

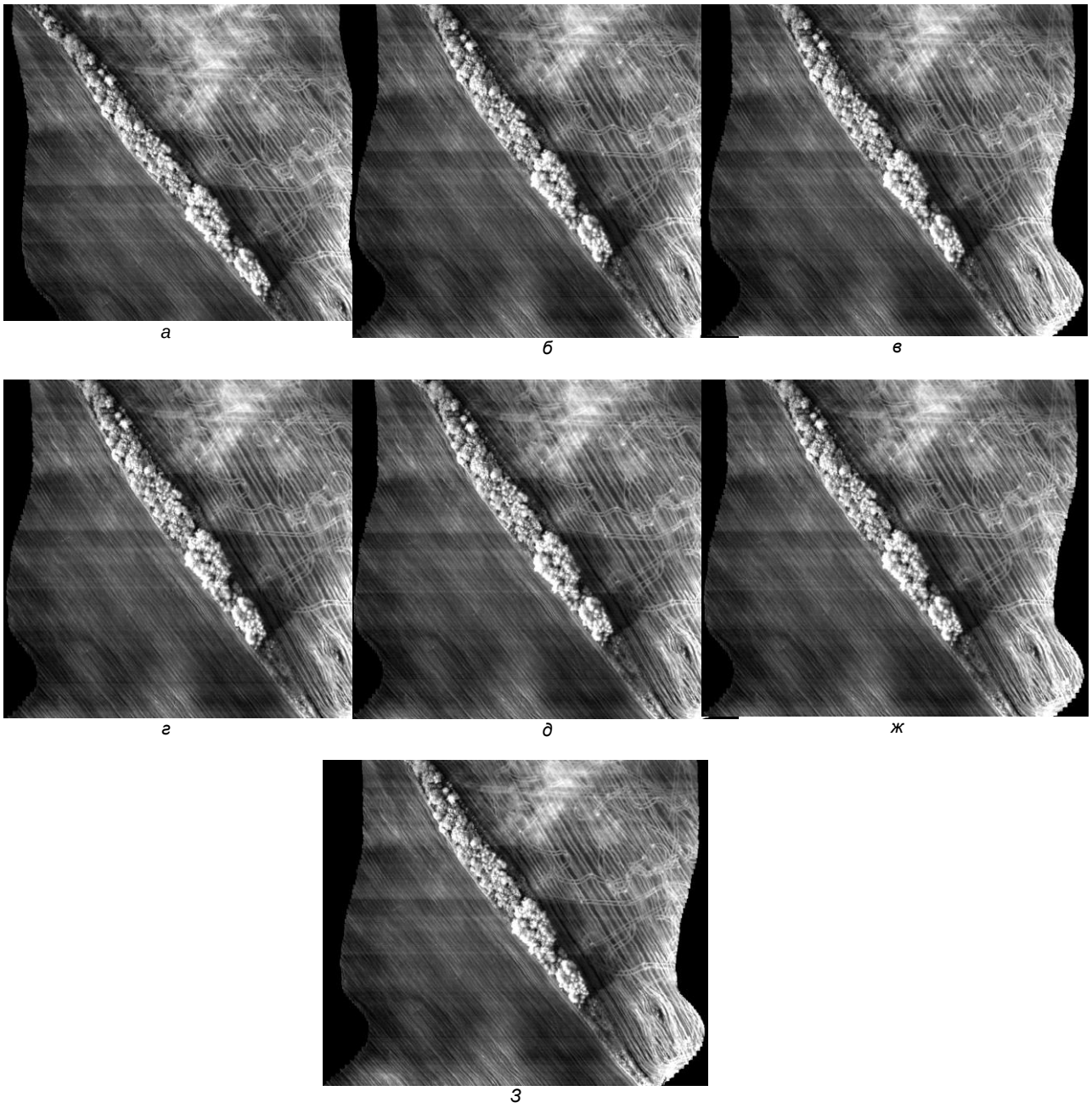
б

в

Рис. 2 – Границы, обнаруженные различными операторами: *а* – оператором Робертса; *б* – оператором Собеля; *в* – оператором Превитта;

Любой из выше перечисленных методов визуально очень хорошо совмещает изображения. Однако имеются некоторые, иногда весьма значительные различия. Оптимизация времени выполнения не проводилась, но методы использующие только границы работают до 10 раз быстрее, хотя и содержат локальные ошибки совмещения.

Все рассмотренные алгоритмы приемлемы по качеству, тем не менее финальная оценка будет получена на основе результатов последующей обработки изображений, а оценка скорости на основе конечной реализации.



а *б* *в*

г *д* *ж*

з

Рис. 3 – Примеры карты, полученной при совмещении изображений: *а* – Робертс маска; *б* – Собель маска; *в* – Прюитт маска; *г* – Робертс только границы; *д* – Собель только границы; *ж* – Преввит только границы; *з* – полный перебор;

Список использованных источников:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений в среде MATLAB / Гонсалес Р., Вудс Р. — Москва: Техносфера, 2012. — 1104с.

2. Duda R., Hart P., Pattern Classification and Scene Analysis / Duda R., Hart P. — John Wiley and Sons,1973. — 271 с.

СОВМЕЩЕНИЕ КАДРОВ ИЗ ВИДЕОПОТОКА С ИСПОЛЬЗОВАНИЕМ МЕТОДА ОПОРНЫХ ТОЧЕК

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Попов М.В., Пчёлкин А.С.

Костусев А. В. – аспирант каф. СиУТ

В настоящее время одной из наиболее сложных и трудоёмких задач является обработка изображений, получаемых с беспилотного летательного аппарата. Существует несколько основных задач обработки изображений, одной из которых является совмещение кадров и составление карты. Так как конструкция камеры не позволяет добиться желаемой стабилизации изображения на больших и средних высотах, возникает необходимость исправления искажений. На сегодняшний день наибольшую эффективность при построении карты предоставляют методы опорных точек: «SURF», «SIFT», «ORB».

Для совмещения изображения возникает необходимость в эффективном сопоставлении выделения точек на паре кадров. Для этих целей каждая интересующая точка вместе с некоторой окрестностью описывается специальным числовым вектором (дескриптором этой точки), после чего между точками с «похожими» дескрипторами устанавливается соответствие.

Хороший дескриптор должен обладать следующими свойствами:

4) Устойчивость.
5) Характерность.

Результат нахождения опорных точек и их дескрипторов с использованием функции «SurfFeatureDetector» представлен на следующих рисунках:

Рис. 1а – Первый кадр

Рис. 1б – Второй кадр

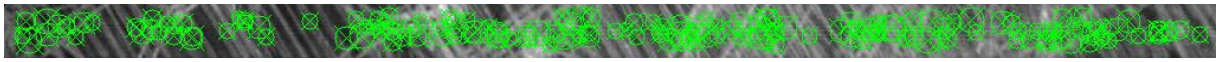


Рис. 1в – Особые точки на первом кадре

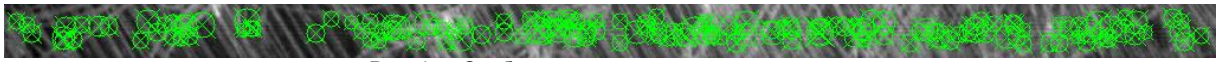


Рис. 1г – Особые точки на втором кадре

На основе полученных дескрипторов строится матрица гомографии, которая характеризует преобразование координат из системы координат одного снимка в систему координат другого снимка. Пример матрицы гомографии представлен на рисунке 2:

```
T1 Img - Keypoint: 158
T1 Img - Descriptors : 158
T2 Img - Keypoints : 153
T2 Img - Descriptors : 153
matching count = 42
 Homography matrix
1.008758 -0.007087 1.928059
0.000335 1.032809 9.872131
0.000008 -0.000042 1.000000
```

Рис. 2 – Матрица гомографии

Построение карты происходит путем наложения следующих кадров со сдвигами, полученными из матрицы гомографии. Результат склеивания двух кадров представлен на рисунке 3:

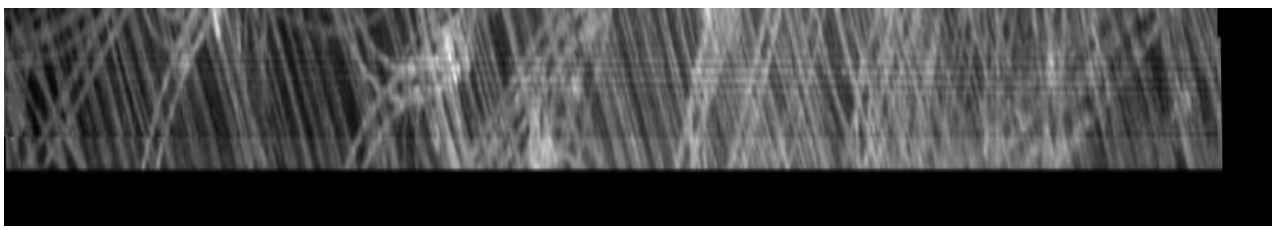


Рис. 3 – Конечный результат склеивания двух кадров (размеры рисунка изменены для большей наглядности)

Таким образом, был реализован метод опорных точек. Данный метод позволяет получить большую эффективность при построении карты, чем иные популярные методы такие как: полный перебор, контурный анализ.

Список использованных источников:

1.Ганина Я.В. Семантическая сегментация изображений на основе метода машинного обучения// Дипломная работа. – Москва,2011-63с.

2. Фурман. Я.А. Введение в контурный анализ; приложения к обработке изображений и сигналов/ Я. А. Фурман, А. К. Кревецкий, А.К. Передреев// Научное издание. – Москва,2003-592с.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ И ПЕРЕДАЧИ СПУТНИКОВЫХ ГИПЕРСПЕКТРАЛЬНЫХ ИЗОБРАЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
Г. Минск, Республика Беларусь
Галкин А. И., Юницкая А. А.

Новицкий В. В. – аспирант каф. СиУТ

Дистанционное зондирование Земли (ДЗЗ) – это одна из наиболее быстро развивающихся областей космической деятельности, использующая передовые научно-технические достижения. Космические аппараты дистанционного зондирования Земли используются для изучения природных ресурсов Земли и решения задач метеорологии.

Одним из наиболее часто используемых методов является спектральный анализ. Спектральный анализ – физический метод определения состава вещества, основанный на получении и исследовании его спектров. Материалы имеют спектры поглощения, которые определяются их химическим составом.

Различия между материалами поверхности или состоянием материалов описываются с помощью значений спектрального коэффициента отражения и объясняются электронными резонансами материалов.

Для получения гиперспектральных данных используются специальные гиперспектральные системы (камеры).

Особенностью гиперспектральных данных является возможность одновременного анализа пространственного распределения и спектральных характеристик наблюдаемых объектов, процессов и явлений. Гиперспектральные данные можно представить как «гиперкуб» - трехмерный массив данных, где каждой точке изображения соответствует спектр, полученный в этой точке снимаемого объекта. При гиперспектральном формировании изображений собирается и обрабатывается информация со всего электромагнитного спектра.

Центральной частью гиперспектральной системы является сенсор, преобразующий оптические яркости земной поверхности в цифровой массив, который формирует гиперкуб.

Гиперспектральная система данных обладает малой шириной спектральных полос и большим количеством регистрируемых каналов. На основе этого, разработаны многочисленные подходы, реализующие анализ тонкой структуры спектров пикселей изображений и их классификацию путем сравнения с эталонными спектральными кривыми (спектральная кривая характеризует связь между значениями коэффициентов отражения и длиной волны).

Особенности гиперспектральных систем:

1. Гиперспектральная система должна иметь сотни спектральных диапазонов;
2. Гиперспектральные системы обычно имеют спектральное разрешение (отношение значения центральной длины волны интервала и ширины интервала) порядка 100;
3. Спектральные диапазоны занимают непрерывную область и регулярно распределены, что позволяет построить непрерывный спектр для каждого пикселя.

Поскольку дистанционная спектрометрия имеет дело со спектрами, которые были получены для смеси самых разных материалов и к тому же искажены при прохождении излучения через атмосферу, связь материала с его спектром не однозначна и может использоваться только как теоретическая основа спектральных дистанционных методов.

Проходя через атмосферу, форма и величина исследуемого спектра отраженного излучения изменяются в соответствии с величинами рассеяния и поглощения существующих в атмосфере газов и твёрдых частиц, что должно учитываться гиперспектральным сенсором. А в определенных условиях эти помехи могут доминировать над спектром исследуемого материала.

Другой важный эффект, который делает обработку гиперспектральных данных неоднозначной, - это смешивание излучения, пришедшего от разных материалов, представленных в области, соответствующей данному пикселю.

Для дистанционной спектрометрии обычно предполагается, что яркости, отвечающие различным материалам, комбинируются линейно.

Получаемые гиперспектральные данные при зондировании необходимы для наблюдения и исследования изменений природной среды и хозяйственной деятельности под воздействием естественных и антропогенных факторов, мониторинга природных ресурсов, инженерной и транспортной инфраструктуры, предупреждения, оценки и минимизации последствий чрезвычайных ситуаций, повышения эффективности управления экономическими процессами и т.д.

Широкому применению гиперспектральных изображений для аэрокосмического мониторинга препятствуют отсутствие достаточного количества спутников и воздушных носителей, оборудованных гиперспектрометрами с требуемыми характеристиками, а также сложности, связанные с обработкой и интерпретацией больших потоков информации, формируемой этими приборами. В связи с этим, для эффективного использования гиперспектральных данных, поступающих при аэрокосмическом мониторинге, требуется разработка и применение эффективных методов, технологий, программных и высокопроизводительных технических средств обработки информации. В последние годы в

области создания и развития средств и технологий дистанционного зондирования Земли наблюдается стремительный прогресс.

При передаче гиперспектральных изображений необходимо эффективно решать следующие проблемы:

1. Объем данных. Гиперспектральные данные трехмерны, причем “спектральный размер” данных часто составляет сотни спектральных компонент. При этом “пространственный размер” этих данных нередко достигает десятков тысяч пикселов.
2. Поток данных. Гиперспектральные данные могут формироваться со скоростью, превышающей возможности канала связи для передачи информации без сжатия.
3. Недостаток ресурсов. Системотехнические характеристики (объем памяти, вычислительная мощность) аппаратуры, которая хранит, передает и принимает данные, ограничены.
4. Канал связи. Цифровой канал связи имеет фиксированную пропускную способность, как правило, недостаточную для передачи несжатых данных.
5. Разрядность. Гиперсепктральные данные часто имеют больший диапазон значений, требующий использования разрядности выше стандартных 8 бит на отсчет.
6. Уникальность данных. Часто повторное получение информации невозможно. Полный список задач, для решения которых она будет использована, неизвестен. Требования к качеству данных очень высокие.
7. Представление данных. “Гиперспектральный куб” в гиперспектральных системах формируется в “повернутом виде”.

Использование компрессии в таких условиях не имеет альтернативы. Перечисленные выше проблемы, возникающие при разработке передачи гиперспектральных данных, порождают следующие требования к методу компрессии в таких системах:

1. Стабилизация скорости формирования потока сжатых данных (управление коэффициентом сжатием).
2. Строгий контроль погрешности.
3. Обработка 16-битных данных.
4. Низкая вычислительная сложность.
5. Низкая структурная сложность.
6. Высокий коэффициент компрессии.

Список использованных источников:

1. Бондур В.Г., Крапивин В.Ф., Савиных В.П. Мониторинг и прогнозирование природных катастроф. М: Научный мир, 2009. 692 с., 22 цв. ил.

2. Козодеров В.В., Кондранин Т.В., Дмитриев Е.В., Казанцев О.Ю., Персеев И.В., Щербаков М.В. Обработка данных гиперспектрального аэрокосмического зондирования // Исследование Земли из космоса, 2012, №5, С.3-11.

3. Райкунов Г.Г., Щербаков В. Л., Турченко С. И., Брусничкина Н. А. Гиперспектральное дистанционное зондирование в геологическом картировании / Под науч. ред. докт. техн. наук, проф. Г.Г. Райкунова. – М.:ФИЗМАТЛИТ, 2014. – 136 с. – ISBN 978-5-9221-1533-9

4. Гашников, М.В. Бортовая обработка гиперспектральных данных в системах дистанционного зондирования Земли на основе иерархической компрессии / М.В. Гашников, Н.И. Глумов // Компьютерная оптика. – 2016. – Т. 40, №4. – С. 541. – DOI: 10.18287/2412-6179-2016-40-4-543-551.

5. Методы и технологии обработки мульти- и гиперспектральных данных дистанционного зондирования Земли высокого разрешения∗ О. И. Потатуркин , С. М. Борзов , А. О. Потатуркин , С. Б. Узилов (2013)

6. Gut N. Hyperspectral imaging // Spectroscopy. 1999. V.14. №3. P. 28-42.

СУПЕР-РАЗРЕШЕНИЕ НА ОСНОВЕ ОБУЧАЮЩЕГОСЯ МНОЖЕСТВА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Никуленко П.М.

Цветков В.Ю. – д.т.н., профессор

В настоящее время все большую необходимость получают алгоритмы повышения разрешения изображений. ОАО "Пеленг" ведёт активную разработку новых способов повышения детализации и четкости спутниковых снимков, так как зачастую необходимую информацию на оригинале распознать невозможно. При этом алгоритмы супер-разрешения позволяют повышать качество изображений, не затрагивая аппаратуру космических аппаратов.

Супер-разрешение – технология, позволяющая повышать разрешающую способность изображений (способность передавать мелкие детали). Алгоритмы супер-разрешения основаны на получении дополнительной информации из каких-либо источников (копии снимков со смещениями и под другим ракурсом, база данных изображений).

Супер-разрешение на основе обучающегося множества имеет преимущество над другими методами в виду того, что не требует модификаций съемочной аппаратуры, так как использует информацию, хранящуюся в базах данных при наземной обработке[1].

Основной принцип предлагаемого алгоритма заключается в нахождении среди изображений базы данных наиболее схожих и подходящих высоких частот для построения повышенного разрешения. Алгоритм можно разделить на следующие шаги:

6) увеличение изображения с помощью бикубической интерполяции;
7) выделение участка 5x5 пикселей и поиск в базе изображений низкого разрешения наиболее похожего участка;
8) нахождение копии участка в базе изображений высокого разрешения;
9) нахождение разности исходного и найденного участка высокой частоты (получение высоких частот аналогично действию фильтра на основе маски нерезкости)[2];
10) наложение с прозрачностью полученной разности на исходный снимок.

Принцип работы алгоритма представлен на рисунке 1:

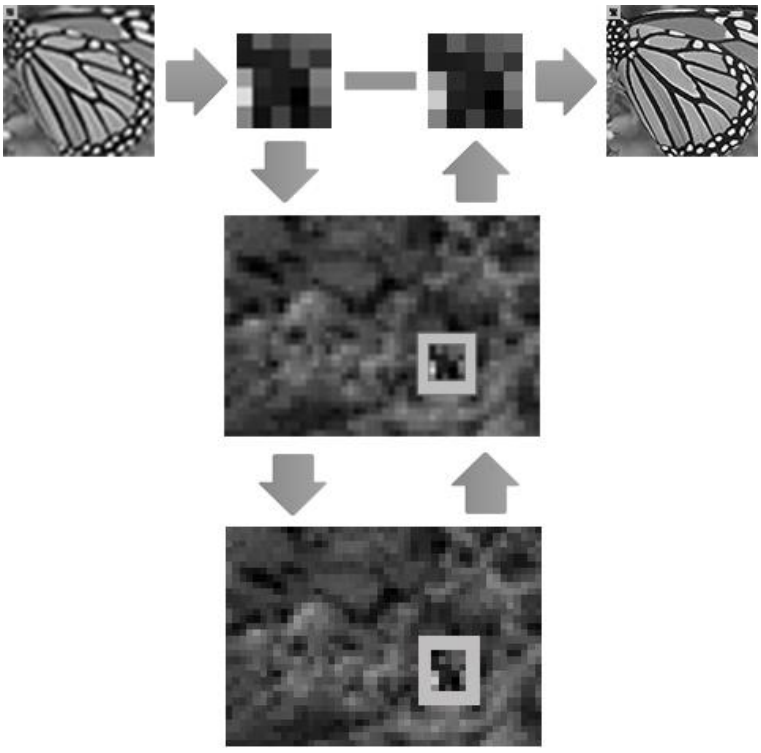


Рис. 1 - Схема работы алгоритма

Исходя из схемы становится понятным, что результат повышения детализации будет зависеть от того, насколько большое количество различных участок в ней будет находиться, при этом даже при небольшой степени сходства четкость изображений будет увеличиваться в виду наложения слоя высоких частот, а возможные ошибки будут корректироваться степенью их прозрачности[3].

Основные результаты обработки представлены на рисунке 2.

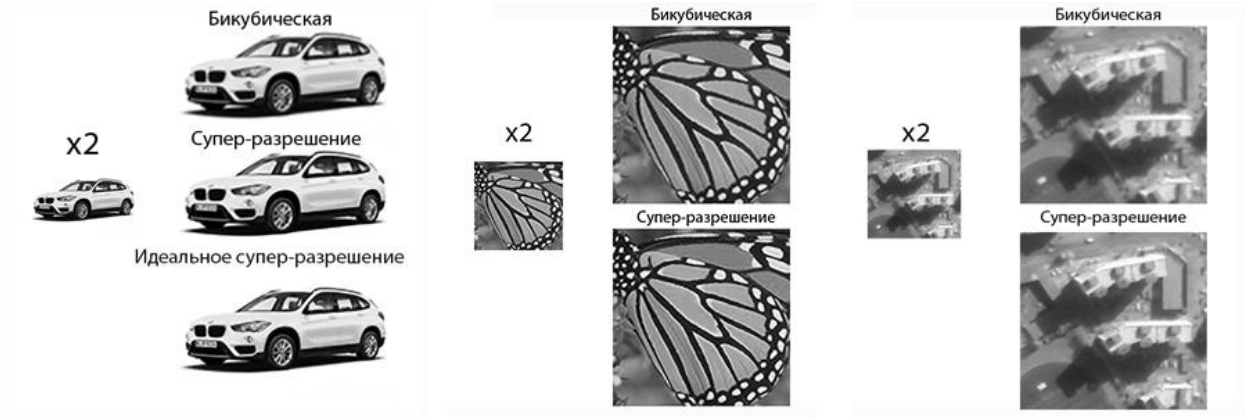


Рис. 2 - Результаты работы алгоритма

Главной проблемой алгоритма является уменьшение ошибок при повышении разрешения, для этого применяется автоматическая коррекция прозрачности накладываемых частот, исходя из степени сходства изучаемых участков. Также существует необходимость развития алгоритма по принципу нейронных сетей, для автоматической выборки из обрабатываемых изображений недостающих в базе высокочастотных участков и последующего накопления их.

Список использованных источников:

1. Michal Irani, Super-resolution from a Single Image
2. Daniel Glasner, Unsharp mask
3. Shai Bagon, Subpixel image processing

SYNTHESIS OF IMAGES BASED ON CELLULAR AUTOMATA

Belarusian State University of Informatics and Radioelectronics

Losyukov L.N, Zhao Qihui

Supervisor – Prof Kanapleka V.K.

A cellular automaton (pl. cellular automata, abbrev. CA) is a discrete model studied in computability theory, mathematics, physics, complexity science, theoretical biology and microstructure modeling. Cellular automata are also called cellular spaces, tessellation automata, homogeneous structures, cellular structures, tessellation structures, and iterative arrays.

A cellular automaton consists of a regular grid of cells, each in one of a finite number of states, such as on and off (in contrast to a coupled map lattice). The grid can be in any finite number of dimensions. For each cell, a set of cells called its neighborhood is defined relative to the specified cell. An initial state (time t = 0) is selected by assigning a state for each cell. A new generation is created (advancing t by 1), according to some fixed rule (generally, a mathematical function) that determines the new state of each cell in terms of the current state of the cell and the states of the cells in its neighborhood. Typically, the rule for updating the state of cells is the same for each cell and does not change over time, and is applied to the whole grid simultaneously, though exceptions are known, such as the stochastic cellular automaton and asynchronous cellular automaton.

Applications

1. Computer processors. Cellular automaton processors are physical implementations of CA concepts, which can process information computationally. Processing elements are arranged in a regular grid of identical cells. The grid is usually a square tiling, or tessellation, of two or three dimensions; other tilings are possible, but not yet used. Cell states are determined only by interactions with adjacent neighbor cells. No means exists to communicate directly with cells farther away. One such cellular automaton processor array configuration is the systolic array. Cell interaction can be via electric charge, magnetism, vibration (phonons at quantum scales), or any other physically useful means. This can be done in several ways so no wires are needed between any elements. This is very unlike processors used in most computers today, von Neumann designs, which are divided into sections with elements that can communicate with distant elements over wires.

2. Cryptography. Rule 30 was originally suggested as a possible block cipher for use in cryptography. Two dimensional cellular automata are used for random number generation. Cellular automata have been proposed for public key cryptography. The one-way function is the evolution of a finite CA whose inverse is believed to be hard to find. Given the rule, anyone can easily calculate future states, but it appears to be very difficult to calculate previous states.

3. Error correction coding. CA have been applied to design error correction codes in a paper by D. Roy Chowdhury, S. Basu, I. Sen Gupta, and P. Pal Chaudhuri. The paper defines a new scheme of building single bit error correction and double bit error detection (SEC-DED) codes using CA, and also reports a fast hardware decoder for the code.

Description of the mathematical model

The cellular automata is a mathematical model of time - space discrete and state - discrete. The general cellular automaton is a quaternion A=(D, S, N, F). D represents the dimension of A, S is a finite state set. N is a primitive vector of n different elements of z^d, $N=(x_1, x_2, \ldots, x_n)$. F is the local programming of the state function of the cellular automata CA_n. The cells are arranged in a finite (infinite) d-dimensional array, and the position is indexed by z^d.

D is the dimension of the cellular automaton. Cellular automata have one-dimensional, two-dimensional, three-dimensional and multidimensional models. One-dimensional cellular automata model is to divide the lines into equal parts, each of which represents a cell; The two-dimensional cellular automata model divides the plane into many square, triangular or hexagonal meshes, which represent the corresponding cells; The three-dimensional cellular automata model divides the space into many three-dimensional grids. With the increase in the number of bits, the phenomenon of cellular automata will be more complicated.

S is a finite state set, The cellular automata characterizes the main features of the simulated system with a finite number of states. When using cell automata to simulate any system, the main features of the real system, the law is extracted, the time is divided into a series of discrete moments, the space according to different dimensions to choose different rules of the grid or grid, In the case of a simple system, the cell automaton can take 0 or 1 for each grid's state value. That is, only a finite state set, S= { 0,1 } , The complex state of the state can take the state set of multiple values k, S= { 0,1…,k } . In the generation of the cell automata pattern, the pattern main feature is a color, and the number of colors of the generated pattern is represented by the number of states.

N is a primitive vector of n different elements of Z^d. The updating of a cell state value of a cellular automaton is determined by itself and its surrounding n cell states, called n-neighborhood cellular automata. In general, the position C_{ij} of the neighborhood of the two - dimensional cellular automata is satisfied: $\{ C_{ij}:|u-i| <= r;|1-j| <= r \}$. R is the neighborhood radius. I, j for the cell line, column position, U, l is the position of the neighborhood up and down.

F gives a local rule for a cell to derive a new state based on the state of its nearest neighbor. The update rules depend on the qualitative understanding of the system's macro-processes and real physical mechanisms, linear rules, and non-linear rules.

Assuming that at time t, the configuration of one-dimensional cellular automata is $a^{(t)}$, then at time t+1, the configuration of cellular automata is $a^{(t+1)}$, then

$$A_i^{(t+1)}=f(a_{i-r}^{(t)}, \dots , a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}, \dots , a_{i+r}^{(t)})$$

among them, the mapping f is a local mapping or local rule of the previously mentioned cellular automata. Independent of i and t. R is the neighborhood radius or spatial scale of the one-dimensional cellular automata. So it can be expressed as a general mathematical form:

$$a_i^{(t+i)} = \int [\sum_{j=-r}^{j=r} \text{aj} \quad \text{ai} + \text{j}^{(t)}$$

One-dimensional cellular automata can be determined only in the simplest case by the cell state on the left and right adjacent lattice points. Often assumed to be consistent with Boolean dynamics, f is determined by the modulo-2 addition value of the two cell states of a_{i-1} and a_{i+1}, at this time, weight $\alpha_j=1$. So at the time t+1, The state of cell a_i is

$$A_i^{(t+)} = f(a_{i-1}^{(t)} , a_{i+1}^{(t)}) = a_{i+1}^{(t)} \eth a_{i+1}^{(t)}$$

In contrast to one-dimensional cellular automata, the configuration of two-dimensional cellular automata is more complex.

Suppose that at time t, the configuration of the two-dimensional cellular automata is $a^{(t)}$, the number of states is k, and the neighborhood radius is r. Then the configuration of the cell automaton at time t + 1 is $a^{(t+1)}$, where the cell state value at position $a_{i,j}^{(t+1)}$ is:

$$A_{i,j}^{(t+1)} = f(a_{i-r,j}^{(t)} , \dots , a_{i-1,j}^{(t)} , a_{i+1,j}^{(t)} , \dots ,a_{i+t,j}^{(t)} , a_{i,j}^{(t)} , a_{i,j-r}^{(t)}, \dots , a_{i,j-1}^{(t)} , a_{i,j+1}^{(t)} , \dots , a_{i,j+r}^{(t)}) \bmod k$$

List of sources used:

1. S. Amoroso; Y.N. Patt. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures. Journal of Computer and System Sciences. October 1972, 6 (5): 448–464.

2. Joel L. Schiff. Cellular Automata: A Discrete View of the World. Wiley & Sons, Inc. – 2011.

АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ WEB-ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фурсов Ф.О., Шигало И.М.
Шевчук О.Г. – ассистент каф. СиУТ

В настоящее время каждый день появляются новые web-приложения, которые построены на различных платформах и написаны на разнообразных языках программирования. Вместе с этим растут требования, предъявляемые к приложениям и всё большую роль, играет обеспечение качества для каждой из систем. Понимание важности процесса тестирования приводит к возникновению тенденций, направленных на применение промышленных способов проверки качества программного обеспечения. Наиболее важным направлением здесь является внедрение различных систем автоматизированного тестирования. Основная роль в осуществлении качественного процесса тестирования принадлежит способам организации взаимодействия всех участников разработки и выбору правильной методологии.

Автоматизация тестирования – использование программного обеспечения для осуществления или помощи в проведении определенных тестовых процессов, например, управление тестированием, проектирование тестов, выполнение тестов и проверка результатов [1]. Внедрение автоматизированного тестирования изменяет модель индустрии программного обеспечения. Это изменение не только предполагает применение инструментальных средств и выполнение автоматизированного тестирования – оно пронизывает весь жизненный цикл программного обеспечения.

Для эффективной реализации автоматизированного тестирования создаются тестовые фреймворки, представляющие собой наборы библиотек и готовых программных модулей, полностью определяющий внутреннюю структуру разрабатываемого приложения [2]. Фреймворк позволяет автоматизировать рутинные операции, связывать между собой различные части системы и разные приложения. Общая схема взаимодействия фреймворков автоматизированного тестирования с тестируемым ПО представлена на рисунке 1.

Рис. 1 – Схема взаимодействия фреймворков с тестовыми сценариями и тестируемыми системами

Тестовые сценарии – это наборы команд, которые необходимо выполнить для осуществления проверки корректного функционирования программного продукта.

Фреймворк – это средство, посредством которого тестовые сценарии передаются тестируемой системе. Фреймворк должен обладать способностью принимать тестовые скрипты и транслировать команды тестируемому объекту в понятном ему формате.

Тестируемая система – приложение, которое принимает команды, поступившие через интерфейс и исполняют их. В качестве приложения может выступать как веб-страница, так и приложение, предназначенное для какой-либо конкретной операционной системы.

Обычно, автоматизированное тестирование учитывает следующие особенности web-приложений:

– кроссплатформенность, т.е. работа их на таких платформах как Windows, macOS, Android, iOS;

– кроссбраузерность, т.е. работа приложений в различных браузерах (Chrome, Mozilla Firefox, Internet Explorer, Safari, Egde);

– многокомпонентость, т.е. web-приложения состоят из множества компонентов, таких как серверы баз данных, серверы приложений, web-серверы [3].

В целом, можно выделить 3 основных направления автоматизации тестирования web-приложений:

– тестирование на уровне пользовательского интерфейса;

– тестирование на уровне API (application programming interface – программный интерфейс приложения);

– тестирование на уровне баз данных.

Выбор того или иного уровня тестирования зависит от сроков и объемов поставленных задач перед командой разработки, сложности проекта, квалификации специалиста по тестированию.

Список использованных источников:

1. Автоматизированное тестирование программного обеспечения. Внедрение, управление и эксплуатация. // Д. Рэшка, Д. Пол, Э. Дастин М: ЛОРИ, 2003 – 576с.

2. TestNG Beginner's Guide. // Varun Menon –Packt Publishing Ltd, 2013 – 276 с.

3. Куликов, С. С. Тестирование программного обеспечения. Базовый курс : практ. пособие. // С. С. Куликов. — Минск: Четыре четверти, 2015. — 294 с..

СИСТЕМА ДЛЯ РАБОТЫ С УВЕДОМЛЕНИЯМИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Наумов Е.С., Подольский Е.А.
Макейчик Е.Г. – ст. преподаватель

На данный момент небольшие предприятия не испытывают трудностей с оповещением персонала. Однако, с ростом числа сотрудников, возникает необходимость в оптимизации процесса уведомления о предстоящих событиях или раздаче персональных поручений. В связи с высоким уровнем развития информационных технологий и высокой степенью их интеграции во все сферы деятельности, основной выбор в решении вопроса выпадает на программные продукты. Тем не менее пользователи различных компьютеров не могли совместно использовать общие данные. Это значительно снижало выгоду, получаемую от компьютеризации предприятия. Решением этой проблемы стало использование для разрабатываемого приложения архитектуры клиент-сервер.

Компьютеры, входящие в состав информационной системы, не являются равноправными. Некоторые из них владеют ресурсами, другие обращаются к этим ресурсам. В архитектуре клиент-сервер все компьютеры разделены на 2 группы: клиенты и серверы. Компьютер, управляющий ресурсом, называют сервером – это мощный компьютер с большой оперативной памятью и большим количеством дискового пространства. На нем выполняется сложная обработка, требующая больших вычислительных ресурсов. На компьютерах-клиентах выполняются первичная обработка данных при вводе, форматирование данных, а также окончательная обработка данных, извлеченных с сервера.

У архитектуры клиент-сервер существует несколько моделей построения[1]:

а) двухзвенная модель;

б) трехзвенная модель;

в) многозвенная модель.

Основным отличием данных моделей является количество используемых серверов.

Система для работы с уведомлениями разработана на языке программирования Java с использованием двухзвенной модели, где все данные обрабатывает один сервер на котором установлено приложение, а в роли клиента выступает WEB-интерфейс данного приложения, доступ к которому осуществляется с компьютеров пользователей.

Принцип реализации системы для работы с уведомлениями представлен на рисунке 1:

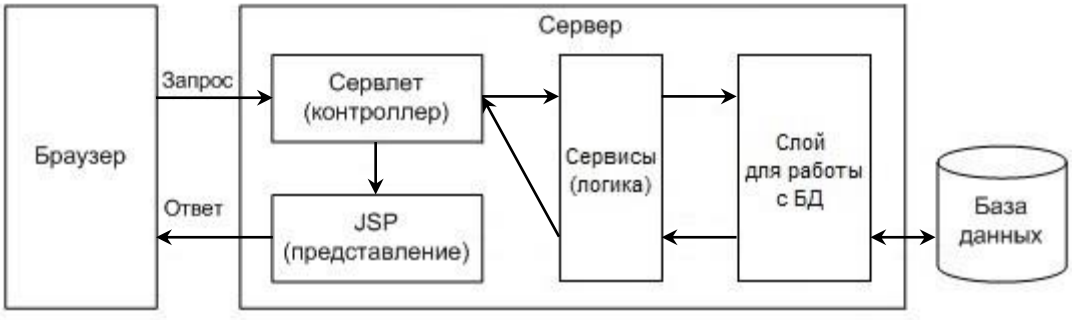


Рис. 1 - Двухзвенная клиент-серверная архитектура

Из рисунка видно, что взаимодействие пользователя с приложением происходит в несколько этапов[2]:

1. Запрос пользователя посылается через WEB-интерфейс контроллеру.

2. Соответствующий класс-контроллер обрабатывает полученный запрос и направляет его в слой сервисов, где содержится вся логика приложения.

3. В слое сервисов соответствующий класс-сервис, в зависимости от запроса, выполняет необходимые операции. Если в процессе выполнения одной из таких операций необходим доступ к базе данных (БД), класс обращается в слой для работы с БД.

4. Класс из слоя взаимодействия с БД, которому был направлен запрос, обращается к базе данных, внося или извлекая необходимую информацию, после чего, получив запрошенные данные, возвращает их в слой сервисов.

5. Класс из слоя сервисов, получив ответ от слоя взаимодействия с БД, передает его контроллеру, из которого был вызван.

6. Контроллер направляет содержимое ответа на соответствующую JSP (Java Server Page) страницу, которая отображается на экране пользователя.

Основным преимуществом системы для работы с уведомлениями является ее способность оптимально организовать рабочий процесс на предприятии. Технические же преимущества основаны на используемой клиент-серверной архитектуре:

1. Централизация данных. Вся обработка данных происходит на сервере, защита которого гораздо выше чем у клиента. Клиент только посылает запросы на извлечение или внесение информации.

2. Технические характеристики. Работа сервера с данными требует высокой вычислительной мощности, однако, так как все вычисления выполняет сервер, системные требования к компьютерам пользователей гораздо ниже.

3. Защита данных. Наличие сервера не только предотвращает доступ к БД со стороны клиента, но и позволяет организовать контроль полномочий, с помощью которого можно разрешить доступ к данным только пользователям с соответствующими правами.

С другой стороны, роль сервера как основной единицы информационной сети также и основной недостаток клиент-серверной архитектуры. Несмотря на крайне низкую вероятность выхода сервера из строя и наличие резервных серверов, его неработоспособность вследствие поломки или недостаточной производительности приводит всю систему к неработоспособному состоянию. К тому же, для поддержки работы сервера требуется отдельно выделенный специалист – системный администратор.

У систем для работы с уведомлениями нет бесплатных аналогов, поэтому каждое предприятие разрабатывает свой продукт с учетом необходимых требований к функционалу. Внедрение таких систем, построенных на основе клиент-серверной архитектуры, успешно решает проблему уведомления сотрудников о различных событиях и поручениях, а также оптимизирует рабочий процесс и взаимодействие между персоналом.

Список использованных источников:

1. Васкевич Д. Стратегии клиент/сервер – Киев : 1997. – 35с.
2. Блинов И.Н., Романчик В.С. Java. Методы программирования – Минск : «Четыре четверти», 2013. – 585с.

ЗНАЧЕНИЕ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ПРЕДПРИЯТИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Романенко О.А, Щитляк А.Н.
Курилович А.В. – ст. преподаватель

В настоящее время локальные сети получили очень широкое распространение. Это обусловлено повсеместной компьютеризацией, которая привела к тому, что появилась необходимость в безопасном и быстром доступе к информации. Средством обеспечения такого доступа стали компьютерные сети. Локальные сети являются важным звеном единой информационно-телекоммуникационной системы предприятий и организаций.

Локальные сети (Local Area Networks, LAN) – это объединение компьютеров, сосредоточенных на небольшой территории, обычно в радиусе не более 1-2 км, хотя в отдельных случаях локальная сеть может иметь и более протяженные размеры, например в несколько десятков километров. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. [1]

Организация локальной сети – основополагающее звено телекоммуникационных систем, так как современные условия работы требуют возможности одновременного доступа нескольких сотрудников к Интернету, различным базам данных. Локальная сеть также необходима для быстрой обработки и печати документов. Это неизбежный процесс, если предприятию необходима оптимизация всех рабочих процессов и увеличение прибыли.

Хорошая организация локальной сети дает возможность предприятию получить в распоряжение скоростной канал передачи и обмена информации. Она объединяет в себе большое количество рабочих узлов-компьютеров, главный сервер и периферийные устройства. Локальная сеть в офисе или группе офисов значительно повышает эффективность и производительность работы предприятия. Она обеспечивает сотрудников непрерывным совместным доступам ко всем ресурсам сети, выходом в Интернет, предоставляет в пользование все периферийные устройства. Сеть дает возможность удобного и оперативного обмена данными между сотрудниками. Таким образом, локальная сеть делает более эффективным электронный документооборот, программа для которого доступна одновременно всем сотрудникам. Грамотная организация сети повышает безопасность корпоративных информационных ресурсов повышенной секретности, делает возможным экономию времени и бюджета для организации новых рабочих мест и модернизации сети, дает возможность одновременно управлять всеми рабочими узлами. [2]

В деловом мире сети передачи данных первоначально использовались для управления финансовой информацией, информацией о заказчике и системой начисления заработной платы. Эти коммерческие сети развивались и делали возможным предоставление различных типов информационных услуг, таких как электронная почта, видео, обмен сообщениями и телефония.

Все шире распространяется использование сетей для эффективного и экономически выгодного обучения персонала. Возможности онлайн-обучения может сократить длительные и дорогостоящие командировки, при этом обеспечивается гарантия того, что все сотрудники должным образом подготовлены к безопасному и эффективному выполнению работы.

В небольших сетях, сетях домашнего офиса возможно организовать общий доступ к ресурсам, таким как принтеры, документы, изображения, музыка между локальными компьютерами.

На предприятиях и в крупных организациях сети могут использоваться в еще более обширном масштабе, чтобы позволить сотрудникам собирать, хранить и получать информацию на сетевых серверах. Кроме того, сети позволяют наладить быструю связь в виде электронной почты, обмена мгновенными сообщениями, а также содействуют совместной работе сотрудников. В дополнение к внутренним организационным преимуществам большинство компаний применяет сети для предоставления продуктов и услуг заказчикам через подключение к Интернету. [3]

Локальные сети и Интернет значительным образом повлияли на общение, обучение, работу и даже развлечения. Существуют сети любого размера, начиная от простых сетей, состоящих из двух компьютеров, до систем, соединяющих миллионы устройств. Современные сети непрерывно совершенствуются для удовлетворения потребностей пользователей.

Список использованных источников:

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы – СПб.: Питер, 2003, 2-е издание – 28 с.

2. Island formoza [Электронный ресурс]. – Режим доступа: http://www.island-formoza.ru/tehnologii/organizacija-lokalnoj-sjeti-prjedprijatija.html

3. Netacad [Электронный ресурс]. – Режим доступа: https://www.netacad.com/

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ПО IP-ТЕЛЕФОНИИ НА БАЗЕ ОБОРУДОВАНИЯ CISCO

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Таран А.В.
Цветков В.Ю. – д.т.н., профессор

В современной жизни IP телефония получила довольно широкое распространение. IP телефония сегодня вытесняет традиционный способ связи, потому что обладает неоспоримыми преимуществами, такими как:

- низкая стоимости звонков;
- возможность звонить в удаленные офисы совершенно бесплатно (оплачивается только интернет трафик);
- гибкое управление звонками.
- создание различных группы пользователей и управление ими, например, установка запрета на звонки по междугородней связи;
- удаленный доступ к телефонной сети (сотрудник может подключиться к корпоративной сети даже из дома);
- мобильность и простота обслуживания (не требуются дополнительные настройки телефона сотрудника в случае смены им рабочего места);
- единая инфраструктура для сети и телефонии.

Вследствие этих преимуществ востребованность специалистов, владеющих основами конфигурирования IP-телефонии, непрерывно растет.

Лабораторные работы на базе оборудования Cisco отлично подойдут для понимания основ конфигурирования.

Компания Cisco на сегодняшний день работает в различных сферах сетевых технологий:

- IP-коммуникации
- Сетевая безопасность
- Беспроводные сети LAN
- Сети хранения (SAN)
- Домашние сети
- Видеосистемы
- Прикладные сетевые услуги

Компания Cisco известна не только своей надежностью и широким функционалом, предоставляемым конечному пользователю, но и обширным выбором оборудования.

Основным оборудованием необходимым для выполнения лабораторных работ являются:

1. серверы;
2. IP-телефоны;
3. VoIP-шлюзы;
4. коммутаторы.

В течение курса обучаемый получает опыт работы с IP-телефонией на базе оборудования от компании Cisco:

- ✓ развертывание корпоративной телефонной связи на базе IP-телефонии оборудования;
- ✓ проектирование и создание на базе IP-телефонии call-центров и контакт-центров с функциями голосовой почты, автосекретаря, персональной маршрутизации звонков, проведения аудиоконференций и др.;
- ✓ проектирование и настройка отказоустойчивой системы IP-телефонии;
- ✓ интеграцию телефонных сетей удаленных офисов в единую телефонную сеть с использованием каналов Интернет.

Прохождение курса лабораторных работ на базе оборудования Cisco предоставляет навыки для развертывания IP-телефонии как в сетях типа SOHO, так и в крупных организациях.

Список использованных источников:
http://www.cisco.com/c/ru_ru/products/index.html
Jonathan Davidson-Voice over IP Fundamentals

ИССЛЕДОВАНИЕ И ОЦЕНКА ХАРАКТЕРИСТИК СИСТЕМЫ БЕСПРОВОДНОГО ДОСТУПА ПЛАТФОРМЫ UWB

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кудлай А.Е.

Хоменок М.Ю. – к.т.н.,доцент

Беспроводные персональные сети медицинского профиля BANET имеют большой потенциал для создания оздоровительных технологий персонального и социального назначения путем сбора эмпирической информации и разработки алгоритмов диагностического назначения на основе облачных технологий.

Сети BANET основываются на обширной области приложений медицинской и потребительской электроники и позволяют производить удаленный мониторинг состояния здоровья/хода лечения пациентов в течение длительного времени без ограничений их нормальной активности, что позволяет получить требуемый объем достоверной статистики.

Ключевые слова: Беспроводные нательные сети, сверхширокополосные сигналы, сетевая архитектура.

Беспроводные нательные сенсорные сети (БНСС) представляют собой сети сенсорных узлов, расположенных либо в непосредственной окрестности тела человека, либо внутри его тела, и взаимодействующих между собой и с центральным координирующим узлом посредством беспроводной связи.

Архитектура БНС состоит из сенсорных узлов, координатора и каналов связи для передачи информации по беспроводной сети, а далее через Интернет/NGN в центры мониторинга, управления и т.п., рис.1.

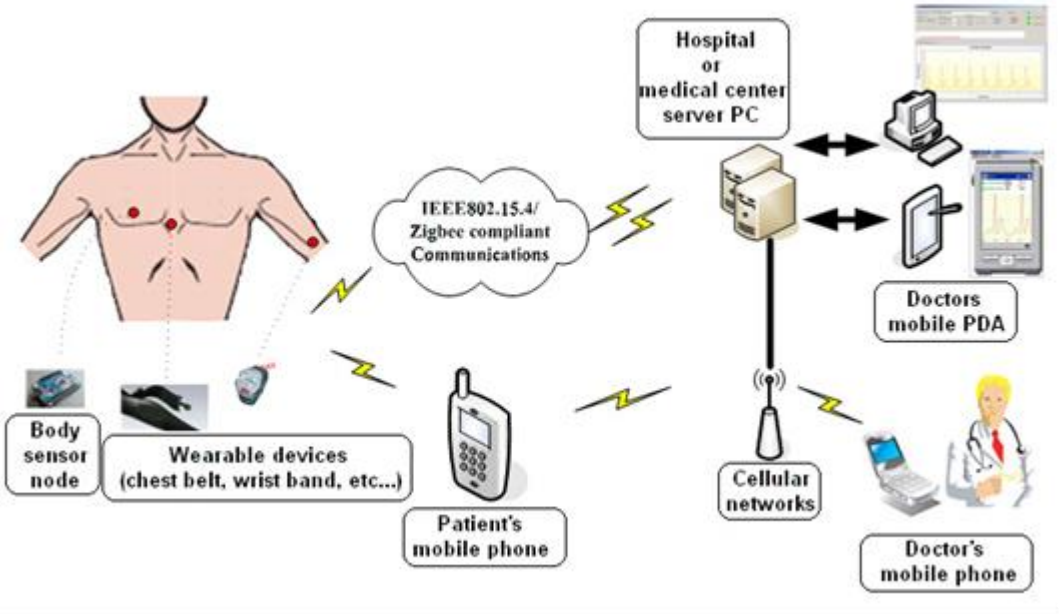


Рисунок 1. Архитектура беспроводной персональной сети медицинского профиля.

Классификация узлов в БНС на основе их роли классифицируется следующим образом:

Координатор – этот узел обеспечивает взаимодействие БНСС со шлюзом к внешнему миру, другой БНС, центру управления и т.п. Все остальные узлы БНСС могут общаться через координатор.

Сенсоры – сенсорные узлы БНС, предназначенные для внутренних или внешних измерений определенных параметров на теле человека.

Для упорядочения развития и применения БНС был создан новый стандарт беспроводной персональной связи IEEE 802.15.6. Стандарт IEEE 802.15.6 определяет три физических уровня – узкополосный (Narrowband – NB), сверхширокополосный (Ultra wideband – UWB) и связь по телу человека (Human Body Communication – HBC). Выбор каждого типа физического уровня зависит от требований к конкретному применению.

Поскольку большинство устройств в больницах работают на частотах гораздо ниже, чем СШП, вероятность возникновения электромагнитных помех, вызванных такими устройствами, минимальна, что гарантирует конечным пользователям безопасность и полезность таких устройств, облегчая СШП приборам путь для выхода на рынок.

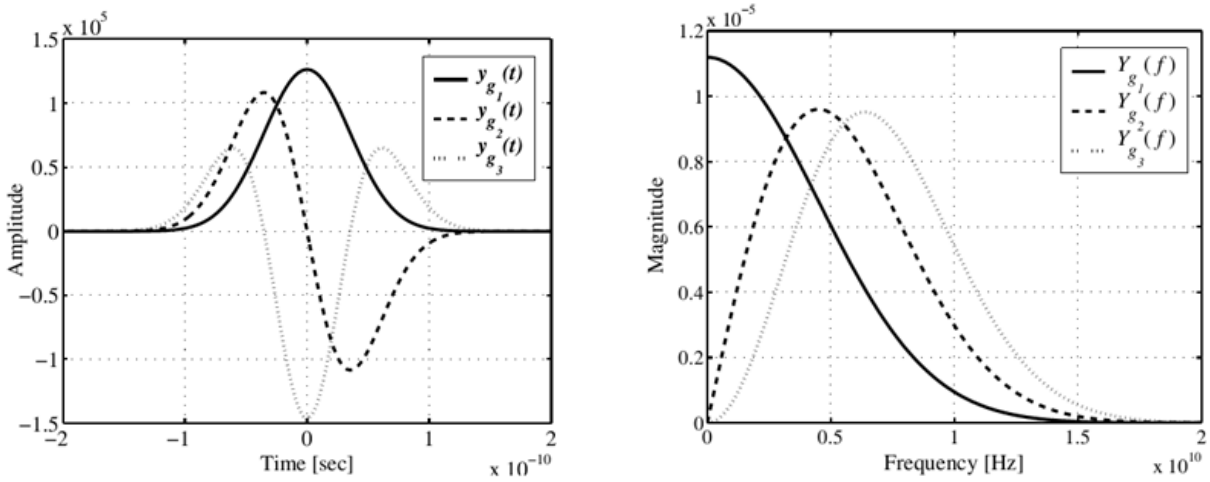
Среди всех СШП устройств, устройства мониторинга жизненно важных функций человека появляются на рынке первыми. Уже в августе 2013 года НИЦ СШП МАИ начинает продажу устройств измерения частоты дыхания и частоты сердечных сокращений (ЧСС), устройства измерение скорости

пульсовой волны (СПВ), а также измерительной платформа для контроля состояния лабораторных животных. Развитие этого сегмента рынка должно развиваться быстрее других глобальных сегментов, нацеленных на продажу приборов мониторинга жизненно важных функций человека. Большой потенциал имеет коммерческое применение СШП технологии в области медицинской визуализации. Это направление включает в себя как телерадиографию, так и построение изображений различных органов. Вскоре возможно появление на рынке СШП 3D-камер, предназначенных для построения движений сердца.

Также возможно использование СШП технологии для других медицинских приложений визуализации, таких как визуализации пульмонологии, акушерских изображений, а также ЛОР изображений. Кроме того, если законодательство не будет ограничивать мощности таких устройств, СШП вскоре может стать одним из наиболее экономически эффективных медицинских технологий.

Несмотря на все преимущества UWB, существует ряд теоретических и практических вопросов, тщательная проработка которых необходима для успешного продвижения данной технологии на рынке беспроводной связи.

Разработка кодов для многостанционного доступа, подавление помех многостанционного доступа (MAI), обнаружение и подавление сосредоточенных помех (NBI), синхронизация приемника по очень узким импульсам, точное моделирование каналов UWB, оценивание задержки и передаточных коэффициентов каналов многолучевого распространения, а также адаптивная схема приемопередатчика – вот лишь некоторые из тех проблем, которые еще требуют серьезных исследований, рис.2.



Математические модели гауссовых моноциклов:

$$Y_{g1}(t) = K_1 e^{-\left(\frac{t}{\tau}\right)^2}, Y_{g2}(t) = K_2 \frac{-2t}{\tau^2} e^{-\left(\frac{t}{\tau}\right)^2}, Y_{g3}(t) = K_3 \frac{-2t}{\tau^2}\left(1 - \frac{2t^2}{\tau^2}\right) e^{-\left(\frac{t}{\tau}\right)^2}$$

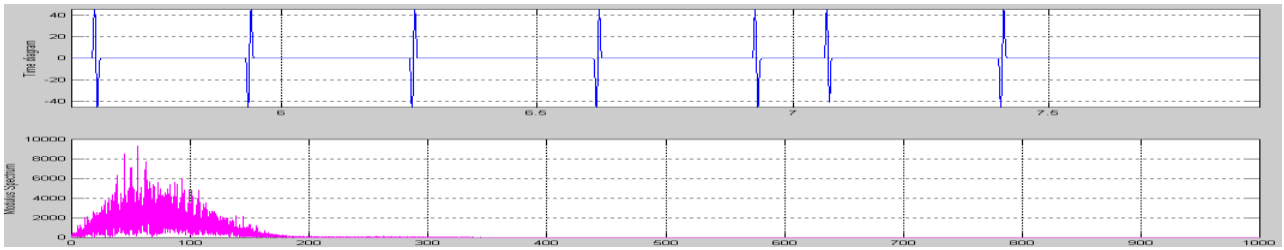


Рис..2 Simulink: Временные и спектральные диаграммы гауссово моноцикла с псевдослучайной перестройкой по времени и балансной модуляцией.

Помимо перечисленных проблем физического уровня, остается открытым и концептуальный вопрос о роли технологии UWB в беспроводных сетях. В то же время остаются актуальными вопросы о роли технологии UWB в организации специализированных беспроводных сетей и сетей датчиков.

Таким образом, обоснование транспортной платформы WLAN сетевых решений BANET с учетом проблем электромагнитного влияния на основе беспроводных сенсорных сетей является перспективным научным и прикладным направлением исследований.

Список использованных источников:

1. Maria-Gabriella Di Benedetto, UWB Communication Systems. A Comprehensive Overview
2. Jamil Y. Khan, Wireless Body Area Networks (WBAN) for Medical Applications
3. Хоменок М.Ю., Щетко И.В. Анализ и оценка основных характеристик технологии сверхширокополосного радиодоступа UWB // Отчет по ГБЦ N 06-2033. 2010 «Разработка методов обработки, передачи и распределения мультимедийной информации».

AD HOC ROUTING PROTOCOLS FOR MOBILE LOCAL AREA NETWORKS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Zaid Ihsan Nuri

Хоменок М.Ю.. – к.т.н.,доцент

Abstract. Mobile ad hoc networks are systems that have ability to self-organize and create temporary networks. Article reflects first step for studying of ad-hoc network protocols to examine several different routing protocols on base of network simulator using performance metrics.

Keywords: Mobile network, Routing protocol, Performance Metrics, Clustering.

The formations of mobile ad-hoc network other words MANET occurs, when the group of wireless mobile nodes dynamically forms a temporary network topology without the use of any existing network infrastructure. The nodes presented in network can move in any direction and acts as a router. However, in the event that it becomes necessary to connect this ad hoc network to another network, for example, such as the same or the Internet, one of these sites in the episodic network may be assigned the rights of a base station or some coordinator of that network. The nodes of the episodic network have a limited transmitter power, because of this they also have limited "radio visibility". Another important property of nodes of such an episodic network, not including reception and transmission, is the ability to retransmit information and route. Therefore, the question arises: how should the work of the episodic network be organized, so that if the nodes are unpredictably moved in the network, it would be possible to guarantee the delivery of information to the desired addressee.

To provide communication in such network, a routing protocol plays a important role to set up optimal route among pair of nodes.

Mobile ad hoc networks use many different routing protocols to route data packets among nodes. Various routing protocols have been developed, and their usage depends on the application and network architecture. As result to survey one can use different classification principals for their taxonomy, figure 1.

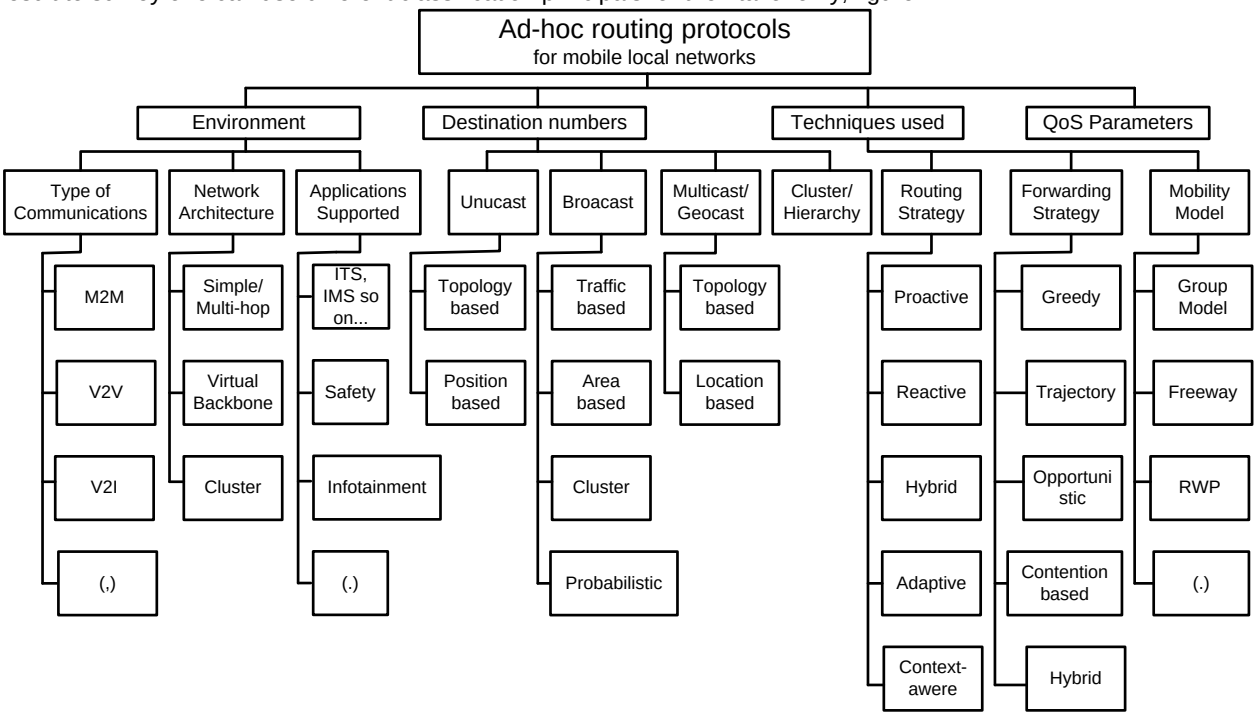


Figure 1. Taxonomy of Ad-hoc routing protocols.

Mobile ad-hoc routing protocols can be categorized into three categories: reactive, proactive, and hybrid. The main characteristic of reactive protocols is that they set up the routes on-demand. When a node wants to start communication with a node to which it does not have any route, the routing protocol will try to establish such a route.

In networks where a proactive routing protocol is used, every node maintains one or more tables that demonstrate the entire topology of the network. There is a need to maintain up-to-date routing information from each node to every other node; thus, the tables are updated regularly. To achieve this, topology information needs to be exchanged between the nodes on a regular basis, leading to high overhead on the network.

For simulation purposes the performance of protocols were evaluated using Average Delay, Control Overhead, Dropping Ratio, Jitter, Normal Overhead, Error Rate, Packet Loss, Latency, Packet Delivery Ratio, and Throughput.

In heterogeneous networks which have a hierarchical structure to opposite homogeneous networks routing protocols have a hybrid principal to realize and routing goes according to a cluster method of communication, figure 2.

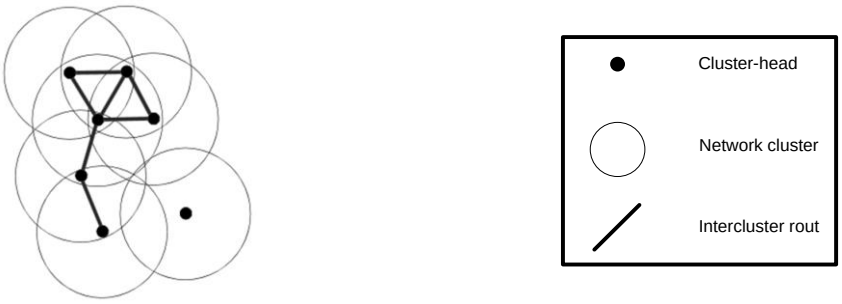


Figure 2. Cluster structure of network

Hybrid protocols combine routing table generation mechanisms inherent in proactive and reactive protocols. In particular, the network allocates a number of subnets within which one of the types of proactive protocols is used, and routing between subnets is performed on the basis of reactive protocols. This approach reduces the size of the routing tables of nodes within the corresponding subnets and reduces the amount of current service information, since the bulk of it circulates within subnets.

The general algorithm of clustering looks like this [1] :

1. Bring the original data to the desired form (data preparation);
2. Choosing a measure of proximity;
3. Choice of algorithm (meta-algorithm) of clustering;
4. Implementation of the algorithm;
5. Presentation of the results;
6. Interpretation of the results.

At the first stage, the data is prepared for clustering. Data for clustering is most often represented in the form of tables, where each column is one of the attributes and a string is a data object.

In the second stage, choose how to characterize the similarity of objects. To this end, various measures of proximity are used, that is, in fact, assessments of the proximity of two objects to each other. Proximity measures are chosen based on the properties of the objects. The proximity measure is selected individually for specific data types. Sometimes it is not possible to find an adequate measure of proximity, and we have to invent it ourselves.

At the third stage, choose the algorithm by which we will build a data model, that is, group objects. The choice of the algorithm is complicated, and it is often necessary to use several algorithms before the desired (interpreted) result is obtained. Sometimes clustering algorithms combine to get a meta-algorithm, the result of doing one when it serves as an intermediate result of the performance of the other.

At the fourth stage, the algorithm is implemented, and its result is the constructed data model, that is, the clustering of objects over clusters.

At the fifth stage, the grouping is attempted to be presented in the most convenient form for interpretation. The algorithms of clustering at the output are given only by groups and objects belonging to them. The presentation of the results of clustering is intended to help to interpret the results of the algorithm most accurately.

Finally, at the last stage of clustering, the results of the execution of the algorithm are interpreted, from which knowledge is obtained, that is, useful rules that can be used in the future to classify new objects as belonging to one group or another -the cluster.

Clustering in mobile ad hoc network can be defined as the virtual partitioning of the dynamic nodes into various groups. A group of nodes identify themselves to be part of a cluster. A special node, designated as cluster-head is responsible for routing, relaying of intercluster traffic, scheduling of intra-cluster traffic and channel assignment for cluster members. The cluster members do not participate in routing. An optional gateway node is also used in some of the clustering schemes, which belongs to more than one cluster, acting as a bridge between cluster heads. Inter-cluster communication is achieved either by cluster-heads or gateways, if present, whereas communication within each cluster is made through direct link. As the complexity and mobility of the network increases, the selection of cluster heads and the management of clusters becomes a challenging task.

The highly dynamic and unstable nature of MANETs makes it difficult for the cluster based routing protocols to divide a mobile network into clusters and determination of cluster heads for each cluster. An optimum cluster-head and gateway selection algorithm is based on maximum resource utilization, fast route discovery, maximum area of coverage and several other factors including stability. In [2] is proposed The Survey of Cluster-based Routing Protocols in Mobile Ad hoc Networks and performed comparative analysis with traditional networks

Cluster Based Location Routing algorithm enables a dynamic, self-starting, and multi-hop routing between nodes. The link will be maintained only if there is at least one header in the intermediate cluster. Since, only the header needs to find the destination path, the routing overhead is less and it is proportional to the number of clusters.

References

1. Methods and means of data analysis. http://bourabai.ru/tpoi/analysis6.htm

2. Survey of Cluster-based Routing Protocols in Mobile Ad hoc Networks. www.ijcte.org/papers/414-G1106.pdf

УПРАВЛЕНИЕ РАДИОРЕСУРСАМИ В СОТОВОЙ СЕТИ 3GPPLTE

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ячменев А.А.

Саломатин С.Б. – к.т.н., доцент

С развитием рынка телекоммуникаций появляется все большее количество пользователей, которым необходимо передавать и принимать высококачественное видеоизображение, поддерживать постоянное высокоскоростное соединение с сетью Интернет, пользоваться разнообразными приложениями, требующих высоких скоростей передачи данных и большую пропускную способность. Постоянная растущая нагрузка на сети операторов подвижной радиосвязи требует регулярной модернизации их сетей. Повсеместное развитие и активное использование современных сетей подвижной радиосвязи четвертого поколения стандарта Long Term Evolution (LTE), пришедшего на смену стандартам третьего поколения, поможет справиться с проблемами, возникшими вследствие постоянно растущей нагрузкой на сети операторов подвижной радиосвязи.

В настоящее время наблюдается быстрый рост количества беспроводных сетей различного типа и назначения, которые вытесняют традиционные кабельные и проводные. Быстрота развертывания и гибкость настройки обеспечивают им конкурентные преимущества. Однако, наличие большого количества таких сетей, работающих поблизости друг от друга и использующих общий частотный диапазон, требует тщательного подхода к управлению их энергетическими ресурсами: мощностью, а также типом излучающей системы. Регулируя уровень излучения и оптимальным образом направляя потоки информации удается обеспечить требуемое качество передачи данных и решить проблему электромагнитной совместимости, означающую в данном случае способность различных компонентов разных сетей одновременно функционировать в реальных условиях эксплуатации, не создавая помех друг другу.

Целью данной статьи является изучение вопросов управления радиоресурсами мобильной сети LTE. Объектом исследований являются системы управления ресурсами сотовых сетей 3GPPLTE.Предметом исследования являются алгоритмы, позволяющие оптимизировать процессы передачи информации в таких сетях, обеспечивая оптимальное их размещение и функционирование. Практическая значимость заключается в выработке методик, алгоритмов управления ресурсами и рекомендаций по оптимизации сотовых сетей 3GPPLTE.

Одной из основных задач сети LTE, как и любой беспроводной системы связи, является обеспечение быстрой и бесперебойной передачи обслуживания от базовых станций к пользовательским терминалам. Обширный спектр предоставляемых пользователям мобильных сетей LTE услуг и при этом ограниченность частотного диапазона ставят перед сотовыми операторами задачу управления ресурсами сети для обеспечения требуемого качества предоставления услуг[1]. В соответствии с рекомендациями консорциума 3GPP, занимающегося стандартизацией сетей LTE, управление радиоресурсами (Radio Resource Management) представляет собой комплексную задачу, включающую управление уровнями радиопомех, управление доступом к радиоресурсам, управление межсотовой интерференцией, управление динамическим распределением радиоресурсов и прочие[2].

Понятие управления радиоресурсами (RRM) включает в себя стратегии и алгоритмы для управления такими параметрами как мощность передачи, распределение пользователей, формирование диаграммы направленности, скорости передачи данных, критерии передачи обслуживания, схема модуляции, схема кодирования ошибок и т. д. Целью управления радиоресурсами является использование ограниченных ресурсов радиочастотного спектра и инфраструктуры радиосети настолько эффективно, насколько это возможно.

В основе современных систем связи четвертого поколения используются такие технологии как система мультиплексирования с ортогональным доступом с частотным разделением каналов (OFDMA, Orthogonal Frequency Division Multiple Access) и метод пространственного кодирования сигнала, при котором передача данных осуществляется с помощью N антенн и их приема M антеннами MIMO (Multiple Input Multiple Output). Множество исследований при создании современных систем связи четвертого поколения ведутся в направлении использования технологии ортогонального доступа с частотным разделением каналов. Технология OFDMA принята в качестве метода доступа для стандарта подвижной радиотелефонной связи LTE, разработанного консорциумом 3GPP (3rd Generation Partnership Project)[3].

На физическом уровне на участке между пользовательским терминалом и базовой станцией в стандарте LTE применяют технологию OFDM (англ. Orthogonal frequency-division multiplexing – мультиплексирование с ортогональным частотным разделением каналов) с модуляцией 4-ФМ, 16-КАМ и 64-КАМ.

Существующий канальный ресурс состоит из *ресурсных блоков (РБ)*, каждый из которых включает 12 расположенных рядом поднесущих, занимающих полосу 180 кГц и одного временного слота (7 или 6 OFDM-символов на интервале 0,5 мс). Каждый OFDM-символ представляет собой *ресурсный элемент (РЭ),* параметрами которого являются 2 значения: {*k*, *l*}, где *k* указывает на номер поднесущей, а *l* – номер символа в ресурсном блоке. Во время передачи по линии «вниз» (от базовой станции к абонентской) в каждом блоке из 12×7 = 84 ресурсных элементов, некоторые из которых применяют для

отправки опорных символов. Выделяемый канальный ресурс определяют количеством ресурсных блоков или групп ресурсных блоков.

Структура ресурсного блока при передаче по линии «вниз» представлена на рисунке 1[2].

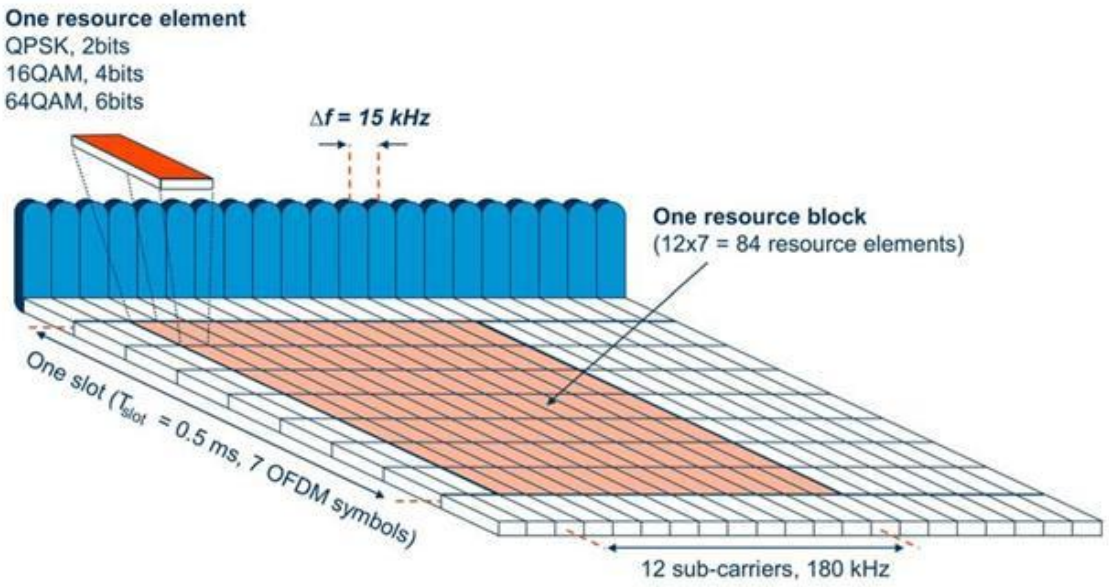


Рисунок 1 – Структура ресурсного блока при передаче по линии «вниз»

Канальный ресурс по линии «вверх» выделяют также ресурсными блоками (12 поднесущих общей полосой 180 кГц в слоте), и субкадрами длительностью 1 мс с 7 или 6 OFDM-символами в каждом слоте. Во время передачи по линии «вверх» применяют измененную технологию OFDM, а фактически производят передачу широкополосного сигнала на одной несущей. Данная технология называется SC-FDMA (Single Carrier-Frequency Division Multiple Access).

На рисунке 2 показано распределение канального ресурса на линии «вверх»[2].

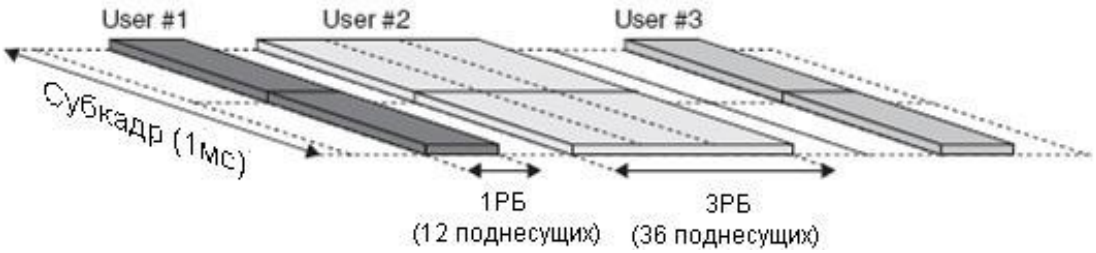


Рисунок 2 –Распределение канального ресурса на линии «вверх»

Управление радиоресурсами подразделяется на статическое и динамическое.

Статическое управление радиоресурсами включает в себя мероприятия по планированию радиосети, например, выбор планов полос распределения частот, построение частотных планов использования радиоканалов, формирование диаграмм направленности антенн и их пространственное разнесение, выбор параметров модуляции и канального кодирования и другие.

Процедуры динамического управления радиоресурсами адаптивно регулируют параметры радиосети к нагрузке трафика, местоположению пользователей, мобильности пользователей, требованиям к качеству обслуживания и т. д.

Таким образом, механизм управления радиоресурсами позволяет эффективно использовать ограниченные ресурсы радиочастотного спектра и инфраструктуру радиосети, обеспечивая качественное обслуживание абонентам.

Список использованных источников:

1. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE. Технологии и архитектура. М.: Эко-Трендз, 2010. 284 с.

2. 3GPP TS 36.300 – Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 12). 2014.

3. Nohrborg M. LTE Overview [Электронный ресурс] – Режим доступа: http://www.3gpp.org/LTE.

ЛАЗЕРНОЕ СКАНИРОВАНИЕ ЗЕМНОЙ ПОВЕРХНОСТИ С ИСПОЛЬЗОВАНИЕМ БЛА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ланденок В.О., Парасочка А.В., Галай Е.А.

Волков К.А. – к.т.н.
Конопелько В.К. – д.т.н., профессор

В настоящее время, воздушное сканирование земной поверхности является одним из самых современных видов съемки, позволяющий получить информацию о местности. В последнее десятилетие данные воздушного лазерного сканирования все чаще начинают применять, как при проектировании, так и при мониторинге различных объектов инфраструктуры и природных процессов. Данный метод находит применение в строительстве, автодорожной отрасли, архитектуре, нефтегазовой отрасли, электроэнергетике и других областях.

Воздушное лазерное сканирование (лидарная аэросъемка) заключается в оптико-механическом сканировании местности лазерным излучением, пульсирующим с высокой частотой (например, 150 кГц), приеме и регистрации отраженного от поверхности объекта сигнала (импульса), определении дальности от точки излучения до точки отражения и вычислении координат точки отражения. Для обеспечения возможности вычисления координат точек лазерных отражений (ТЛО) система воздушного лазерного сканирования (аэросъемочный лидар) имеет в своем составе систему определения положения и ориентации, обеспечивающую на основе ГЛОНАСС и инерциальных измерений определение положения и ориентации сканирующей лазерной системы в момент испускания импульса. Это позволяет получить облако точек лазерных отражений с известными пространственными координатами, обладающее высокой плотностью (несколько точек на $м^2$).

Рис. 1 – Воздушное лазерное сканирование, с использованием систем спутниковой навигации

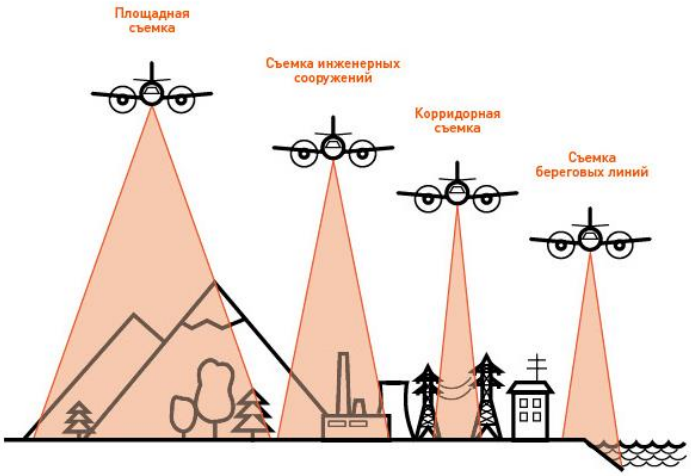


Рис. 2 – Виды воздушного лазерного сканирования

Основные характеристики системы:

1. Система лидар позволяет с воздушного судна измерять расстояния до всех видимых объектов на поверхности земли, полет проходит на высоте 500-1500 м.
2. За одну секунду выполняется порядка 300 тысяч измерений (точек) на поверхности объектов.
3. За один пролёт с борта снимается полоса поверхности земли в 60 градусов.
4. Точность данных, полученных системой лидар, зависит от используемого оборудования и условий полёта и обычно точность составляет 5 – 15 см.
5. Как правило, во время полёта выполняется видеосъёмка и аэрофотосъёмка исследуемой территории земли, что позволяет получить в результате 3D-видео и ортофотопланы.

Преимущества технологии ВЛС:

1. Результатом лазерного сканирования является огромный массив измерений (облако точек), представленный в единой системе координат, который после постобработки преобразуется топографические планы масштаба от 1:1000 и трёхмерные цифровые модели местности.
2. Высокая детальность получаемых материалов.
3. Все данные поступают сразу в цифровом виде.
4. Возможность получения истинного рельефа таких труднодоступных и чересчур обременительных для съемки традиционными методами мест как: тундра, пустыня, заснеженная территория.

Рис. 3 - Облако точек лазерных отражений для застроенной территории

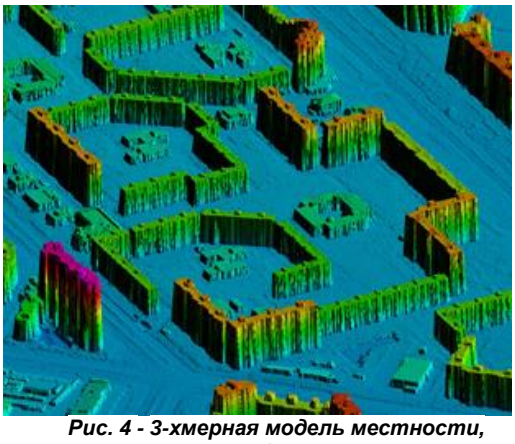


Рис. 4 - 3-хмерная модель местности, построенная по ТЛО, представленная сеткой треугольников

Сферы применения воздушного лазерного сканирования:

1. Топографическая съемка рельефа и создание цифровых моделей рельефа высокой точности и подробности; в решении этой задачи лидарная съемка имеет неоспоримые преимущества, т. к. эта технология обеспечивает высокую точность съемки и плотность точек и позволяет получить координаты точек лазерных отражений даже в залесенной местности под кронами деревьев.
2. Создание сеточных трехмерных моделей местности и объектов местности (моделей поверхности).
3. Создание 3D моделей зданий и сооружений, застроенных территорий.
4. Обследование электротехнических объектов (высоковольтных ЛЭП, подстанций и проч.).
5. Обследование объектов транспортной инфраструктуры.
6. Батиметрическая съемка внутренних водоемов и шельфа.
7. Инвентаризация и мониторинг лесов.
8. Инвентаризация земельно-имущественного комплекса.
9. Мониторинг крупных инженерных объектов, например, открытых разработок полезных ископаемых.

Список использованных источников:

1. Allen, S. Seeing into the Past: Creating a 3D Modehng Pipe¬line for Archaeological Visualization [текст] / S. Allen, P. Feiner, A. Troccoli, H. Bcnko, E. Ishak, B. Smith. - Department of Computer Science, Columbia University. New York, NY, 2004. – англ.

2. Andreas Rietdorf «Automatisierte Auswertung und Kalibrierung von scannenden Messsystemen mit tachzmetrischem Messprinzip» - Munhen 2005.

3. Crassidis, J.L. Sigma-point kalman filtering for integrated gps and inertial navigation [Blech-onic resource] / .I.L. Crassidis. -2005. - 24 p. - англ. Режим доступа *http://www.acsu.buffalo.cdu/ %7ejohnc/gpsins_gnc05.pdf*

4. A new calibration system of a non-metric digital camera [текст] / R. Matsuoka и др.// Procs. 6th Conference on Optical 3-D Measurement Techniques, pp. 130-137. Zurich, Switzerland. Sep¬tember 22-25, 2003.

5. Наземное лазерное сканирование: монография / В.А. Середо-Н19 ВИЧ, А.В. Комиссаров, Д.В. Комиссаров, Т.Л. Широкова. - Новосибирск: СГГА, 2009. - 261 с. ISBN 978-5-87693-336-2.

КОРРЕКЦИЯ ЯРКОСТИ И КОНТРАСТНОСТИ ИЗОБРАЖЕНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лещинский И.В., Дичковский Е.В.
Волков К.А. – к.т.н.
Конопелько В.К. – д.т.н., профессор

Большинство быстрых алгоритмов выделения контуров (Собеля, Робертса, Превитта и др. [1, 3]) основаны на оценке градиента яркости. При этом используется полутоновое изображение, которое может быть получено из цветного посредством извлечения яркостной компоненты. Для моделей цветового пространства YUV (YCbCr), YIQ, HLS, XYZ яркость каждого пикселя доступна непосредственно, тогда как для прочих требуется выполнение соответствующего преобразования.

Наиболее общим способом поиска границ является обработка изображения с помощью скользящей маски (фильтра), которая представляет собой прямоугольную матрицу, содержащую коэффициенты. Поскольку коэффициенты матрицы являются фиксированными, то данные алгоритмы можно отнести к пороговым, т.е. содержащим некоторые предопределенные константные выражения. Практически это обозначает, что принадлежность точки изображения к контуру определяется по критерию абсолютной величины градиента яркости [1, 2]. Однако данный подход не обеспечивает качественного выделения контуров, если изображение имеет различный уровень контраста (разность максимального и минимального значений яркости) на отдельных участках, или низкий уровень контраста в целом. Аналогичная проблема качества выделения контуров возникает, если предполагается использовать их использовать для сшивки пары изображений, имеющих различные яркость и контраст.

Проблема с неравномерностью яркости и контраста на изображении (паре изображений) возникает из-за того, что для представления яркости каждого пикселя технически используется ограниченный целочисленный диапазон (определенной число градаций), т.е. применяется арифметика с переполнением. Если фиксируемое камерой изображение имеет чрезмерный диапазон освещенности, то экспозиция кадра оптимизируется либо для фиксации ярких объектов (что приводит к потере информации о темных участках сцены, которые становятся «черными» – рис. 1а), либо для фиксации темных объектов (что приводит к потере информации о ярких участках сцены, которые становятся «белыми» – рис. 1б) [4]. В случае если экспозиция выбрана неверно, то также возможна ситуация, когда на цифровом изображении используется не весь диапазон возможной яркости пикселей.

а б

Рис. 1 – Влияние выдержки на фотографию при неизменной диафрагме (а – 1,3 с, б – 15 с)

Путем цифровой обработки контраст можно повысить, изменяя яркость каждого элемента изображения и увеличивая диапазон яркостей. Рассмотрим влияние функций преобразования яркости пикселей на яркость и контрастность результата (рис. 2). Если яркость

и контраст не изменяются в процессе преобразования, то функция передает на выход значение своего аргумента (рис. 2а). Яркость для рассматриваемой функции представляет собой сдвиг прямой линии в вертикальном направлении. Яркость изображения увеличивается пропорционально сдвигу прямой графика. Если прямая сдвигается вверх (рис. 2б), яркость изображения увеличивается, а если прямая сдвигается вниз (рис. 2в) – уменьшается. Поскольку используется арифметика с насыщением, то при установке определённой яркости изображения либо оно полностью окажется засвеченным, либо полностью затемнённым.

При использовании преобразования контраста прямая линия меняет свой наклон. При увеличении контраста изображения (рис. 2г) наклон прямой увеличивается, при уменьшении контраста – уменьшается (рис. 2д). При этом сдвиг прямой в горизонтальном направлении означает, что помимо контраста изменяется и яркость изображения. Комбинации наклона и сдвига прямой позволяют одновременно изменять и яркость, и контраст изображения. Например, на рисунке 2е представлен график функции, усиливающей контраст и увеличивающей яркость изображения.

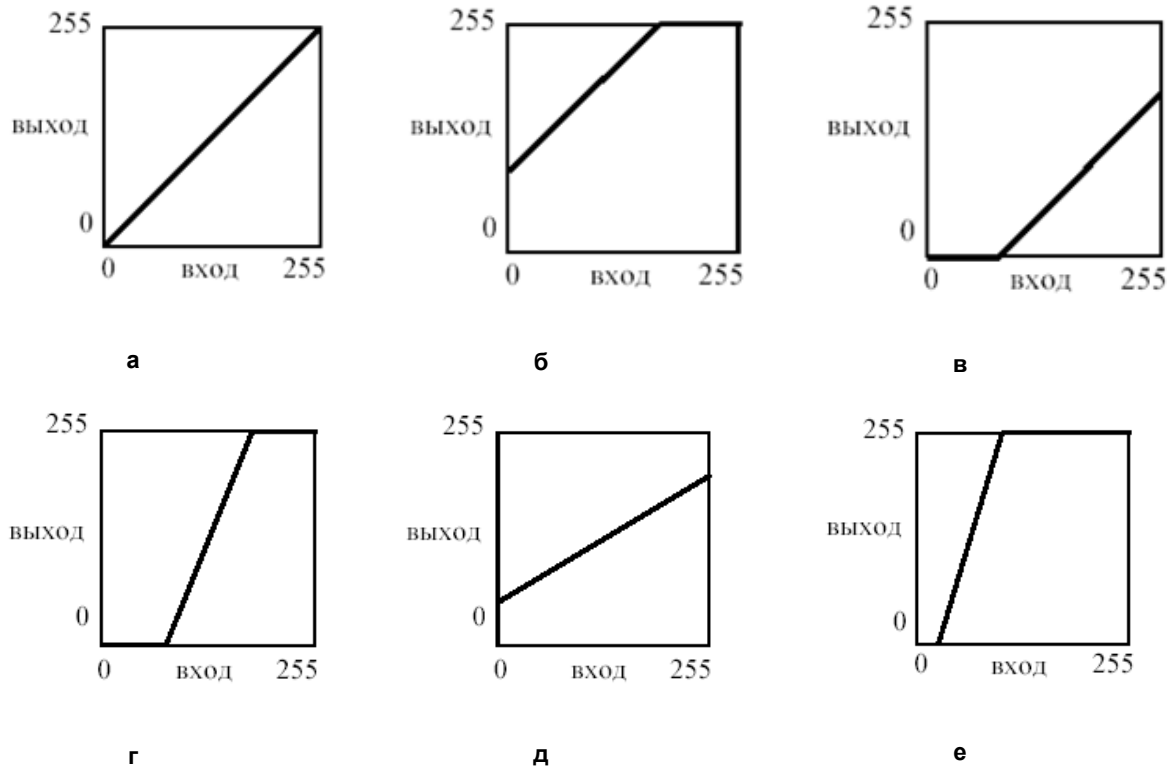


Рис. 2 – Функции преобразования яркости пикселей

Следовательно, для изменения яркости и контрастности изображения достаточно определить функцию преобразования. Для этого разработано несколько методов, большинство из которых основаны на анализе и преобразовании гистограммы яркости изображения. Гистограмма яркости – это график статистического распределения пикселей цифрового изображения с различной яркостью, в котором по горизонтальной оси представлена яркость (далее – в градациях серого в диапазоне 0-255), а по вертикали – относительное число пикселов с конкретным значением яркости. Таким образом, гистограмма соответствует плотности вероятности для яркости пикселей. Если границы гистограммы существенно отличаются от граничных значений яркостного диапазона или имеются ярко выраженные пики, то изображение является недостаточно контрастным.

Список использованных источников:

1. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений – М: Техносфера, 2005. – 1007с.
2. Кудрявцев Л.В. Краткий курс математического анализа – М.: Наука, 1989. – 736с.
3. Анисимов Б.В. Распознавание и цифровая обработка изображений – М.: Высш. школа, 1983. – 295с.
4. Крис Уэстон Экспозиция в цифровой фотосъёмке = Mastering digital exposure and HDR imaging / Т. И. Хлебнова. –М.,: «АРТ-родник», 2008.– С. 18—20. — 192 с.

КАЛИБРОВКА КАМЕРЫ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ OPENCV

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Туча Д.Ю., Ланденок В.О.

Конопелько В.К. – д.т.н., проф.

Современные видеокамеры, имеющие многолинзовые объективы, вносят геометрические искажения в получаемое изображение. Для задач компьютерного зрения наличие искажений нежелательно или недопустимо, поэтому требуется их устранение программным способом. Это достигается путем использования математической модели оптической системы видеокамеры и определенных экспериментально в процессе калибровки ее внутренних и внешних параметров.

Калибровка камеры — это задача получения внутренних и внешних параметров камеры по имеющимся фотографиям или видео, отснятыми ею. Для калибровки видеокамер предлагается использовать реализованные в программной библиотеке OpenCV алгоритмы, учитывающие радиальное и тангенциальное искажение [1].

Радиальное искажение описывается следующей формулой:

$$x_{corrected} = x(1 + k_1 r^2 + k_2 r^4 + k_3 r^6)$$

$$y_{corrected} = y(1 + k_1 r^2 + k_2 r^4 + k_3 r^6)$$

Наличие радиального искажения проявляется в виде «бочки» или эффекта «рыбий глаз».

Тангенциальное искажение происходит потому, что плоскость линзы не идеально параллельно плоскости изображения. Это может быть исправлено с помощью формул:

$$x_{corrected} = x + [2p_1 xy + p_2(r^2 + 2x^2)]$$

$$y_{corrected} = y + [p_1(r^2 + 2y^2) + 2p_2 xy]$$

Позиция каждой точки пикселя с координатами (x, y) в исходном изображении будет скорректирована на новую точку с координатами $(x_{corrected}, y_{corrected})$.

Таким образом, у нас есть пять параметров искажения, которые в OpenCV представлены в виде одной строки матрицы с 5 столбцов:

$$Distortion_{coefficients} = (k_1 \quad k_2 \quad p_1 \quad p_2 \quad k_3)$$

Теперь для блока преобразования мы используем следующую формулу:

$$\begin{bmatrix} x \\ y \\ w \end{bmatrix} = \begin{bmatrix} f_x & 0 & c_x \\ 0 & f_y & c_y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

При этом присутствие w объясняется использованием гомографии системы (и координат $w = Z$). Неизвестные параметры f_x и f_y (фокусные расстояния) и (c_x, c_y), которые являются оптическими центрами. Если для обеих осей общее фокусное расстояние используется с заданным a соотношением сторон (обычно $a = 1$), а затем $f_y = f_x * a$ и в верхней формуле мы будем иметь одно фокусное расстояние f. Матрица, содержащая эти четыре параметра, называется матрицей камеры.

Процесс определения этих двух матриц называется калибровкой. Расчет этих параметров осуществляется с помощью основных геометрических уравнений. Уравнения, используемые в зависимости от выбранных объектов калибрующие [2].

Проведенные натурные эксперименты с широкоугольной камерой для задач стабилизации видео и целеуказания показали эффективность указанных подходов к устранению оптических искажений.

Список использованных источников:
1. Роджерс Д., Адамс Д. Математические основы машинной графики. – М.: Мир, 2001. – 604 с.
2. docs opencv [Электронный ресурс]. – Режим доступа: http://docs.opencv.org.

АЛГОРИТМ ДЕЙКСТРЫ ДЛЯ НАХОЖДЕНИЯ КРАТЧАЙШИХ ПУТЕЙ ВО ВЗВЕШЕННЫХ ГРАФАХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Галай Е.А., Лещинский И.В.

Волков К.А. – к.т.н.

В настоящее время актуальной является задача обеспечения автономного полета беспилотного летательного аппарата (БЛА) с использованием наземных визуальных ориентиров. Для этого требуется осуществлять планирование траектории движения таким образом, чтобы маршрут пролегал через скопления точечных и линейных антропогенных объектов на местности. Это может быть осуществлено с использованием графового представления цифровой карты местности, поиск пути в котором предлагается осуществлять с использованием алгоритма Дейкстры.

Графовое представление цифровой карты местности формируется таким образом, что узлы соответствуют визуальным ориентирам на местности, а дуги – возможным вариантам перемещения БЛА между ними. При этом длина дуг ограничена способностью БЛА автономно перемещаться с использованием бортовой инерциальной системы, так чтобы с учетом возникающей погрешности позиционирования был обеспечен выход в зону видимости наземного ориентира, соответствующему концу дуги. Увеличение количества ориентиров существенно влияет на скорость поиска нужной траектории полета БЛА, в связи с чем предлагается использование алгоритма Дейкстры для быстрого поиска пути во взвешенном графе. Рассматриваемы алгоритм состоит из следующих шагов:

Шаг 1. Всем вершинам, за исключением первой, присваивается вес равный бесконечности, а первой вершине – 0.

Шаг 2. Все вершины не выделены.

Шаг 3. Первая вершина объявляется текущей.

Шаг 4. Вес всех невыделенных вершин пересчитывается по формуле: вес невыделенной вершины есть минимальное число из старого веса данной вершины, суммы веса текущей вершины и веса ребра, соединяющего текущую вершину с невыделенной.

Шаг 5. Среди невыделенных вершин ищется вершина с минимальным весом. Если таковая не найдена, то есть вес всех вершин равен бесконечности, то маршрут не существует. Следовательно, выход. Иначе, текущей становится найденная вершина. Она же выделяется.

Шаг 6. Если текущей вершиной оказывается конечная, то путь найден, и его вес есть вес конечной вершины.

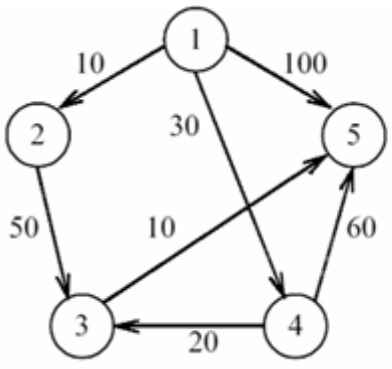
Шаг 7. Переход на шаг 4.

В программной реализации алгоритма Дейкстры построим множество S вершин, для которых кратчайшие пути от начальной вершины уже известны. На каждом шаге к множеству S добавляется та из оставшихся вершин, расстояние до которой от начальной вершины меньше, чем для других оставшихся вершин. При этом будем использовать массив D, в который записываются длины кратчайших путей для каждой вершины. Когда множество S будет содержать все вершины графа, тогда массив D будет содержать длины кратчайших путей от начальной вершины к каждой вершине.

Помимо указанных массивов будем использовать матрицу длин C, где элемент C[i,j] – длина ребра (i,j), если ребра нет, то ее длина полагается равной бесконечности, то есть больше любой фактической длины ребер. Фактически матрица C представляет собой матрицу смежности, в которой все нулевые элементы заменены на бесконечность.

Для определения самого кратчайшего пути введем массив P вершин, где P[v] будет содержать вершину, непосредственно предшествующую вершине v в кратчайшем пути

Псевдокод алгоритма представлен на рисунке 1:



Итерация	*S*	*w*	**D**[2]	**D**[3]	**D**[4]	**D**[5]
начало	{1}	–	10	∞	30	100
1	{1, 2}	2	10	60	30	100
2	{1, 2, 4}	4	10	50	30	90
3	{1, 2, 4, 3}	3	10	50	30	60
4	{1, 2, 4, 3, 5}	5	10	50	30	60

Массив **P**: | | 1 | 4 | 1 | 3 |

Кратчайший путь из 1 в 5: {1, 4, 3, 5}

Рис. 1 - Схема работы алгоритма

Предложенный подход к планированию траектории показал свою эффективность при компьютерном моделировании автономного движения БЛА с использованием симулятора X-Plane.

Список использованных источников:

1. Берж К. Задача о кратчайшем пути // Теория графов и её применения = Theorie des graphes et ses applications / Под ред. И. А. Вайнштейна. — Москва: Издательство иностранной литературы, 1962. — С. 75-81. — 320 с.

2. Алексеев В.Е., Таланов В.А. Нахождения кратчайших путей в графе // Графы. Модели вычислений. Структуры данных. — Нижний Новгород: Издательство Нижегородского гос. университета, 2005. — С. 236-237. — 307 с.

3. Галкина В.А. Построение кратчайших путей в ориентированном графе // Дискретная математика. Комбинаторная оптимизация на графах. — Москва: Издательство "Гелиос АРВ", 2003. — С. 75-94. — 232 с.

4. Евстигнеев В. А. Итеративные алгоритмы глобального анализа графов. Пути и покрытия // Применение теории графов в программировании / Под ред. А. П. Ершова. — Москва: Наука. Главная редакция физико-математической литературы, 1985. — С. 138-150. — 352 с.

МОДЕРНИЗАНИЦИЯ СИСТЕМ БЕСПРОВОДНОГО ДОСТУПА В ОБЩЕЖИТИИ №1 БГУИР

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пригон А.Н.

Курилович А.В. – ст. преподаватель

Прогнозирование параметров распространения для радиосистем, работающих внутри помещений, несколько отличается от такового для наружных систем. Что касается наружных систем, то для них конечной целью является обеспечение эффективного охвата требуемой зоны (или обеспечение надежной передачи на трассе в случае систем связи пункта с пунктом), а также борьба с помехами как в пределах системы, так и для других систем. В случае же приема внутри помещений размеры зоны охвата вполне определяются геометрией здания, причем границы самого здания будут влиять на характеристики распространения.

Помимо повторного использования частоты на одном и том же этаже здания, такой способ использования частот зачастую желателен и между разными этажами здания, в результате чего проблема описания помех становится трехмерной. И, наконец, распространение на очень короткие расстояния, особенно при использовании миллиметровых волн, сопряжено с тем, что даже небольшие изменения в среде, непосредственно окружающей радиотрассу, могут существенно влиять на характеристики распространения.

Цель модернизации систем беспроводного доступа рассматриваемого объекта - выбор варианта, обеспечивающего наибольшую площадь территорий и помещений с устойчивой связью при минимальном количестве базовых станций.

Для достижения поставленной цели, решаются следующие задачи: изучение и экспериментальное измерение уровня затухания в стенах общежития №1, снятие данных о уровне сигнала действующей сети, создание электронной карты зданий и местности, моделирование различных вариантов реализаций Wi-Fi сети. Немаловажным фактором оптимизации цифровой сети является количество помещений, в которых сигнал будет достаточным для работы в интернете.

Рис. 1 – Расположение точек доступа в коридоре общежития №1 (уровень -80 дБ, -20 дБ)

Для выполнения модернизации действующей сети Wi-Fi в общежитии №1 БГУИР, данная задача была разбита на несколько этапов:

1) Первый этап заключается в изучении распространения сигнала внутри общежития.
2) На втором этапе снимаются данные о радиосигнале в действующей сети Wi-Fi.
3) На заключительном этапе модулируется распространение сигнала в свободном пространстве (на улице).

Список использованных источников:

1.Кочин, П. А. Методика быстрой оценки мощности Wi-Fi сигнала при прохождении препятствий в пределах здания / П. А. Кочин , Ю. И. Воротницкий, Д . А. Стрикелев Хорстманн, Кей С. Java. Библиотека профессионала. Основы / Кей С. Хорстманн, Г. Корнелл. – М: Вильямс, 2014. – 864 с.

2.Гавриленко В. Г. Распространение радиоволн в современных системах мобильной связи / В. Г. Гавриленко, В. А. Яшнов. – Нижегородский государственный университет им. Н. И. Лобачевского, радиофизический факультет, кафедра радиоастрономии и распространения радиоволн. – 2003. – 148 с.

3.Андреев, П.Г. Моделирование распространения электромагнитных волн в помещениях/ П.Г. Андреев., М.С. Ширшов, А.Н. Якимов // Современные охранные технологии и средства обеспечения комплексной безопасности объектов : материалы IX Всероссийской научно-практической конференции (Россия, Пенза- Заречный, 18-20 сентября 2012 г.). – Пенза: Изд-во ПГУ, 2012. – С.325-331.

ЗАЩИЩЕННЫЙ ВИРТУАЛЬНЫЙ СЕРВИС БАНКОВСКИХ УСЛУГ И ВЕДЕНИЯ БУХГАЛТЕРСКОГО УЧЕТА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сошенко М.С.

Смирнов Ю.В. – ассистент

Одним из ключевых трендов развития бизнеса становится цифровизация всех бизнес-процессов внутри организаций. Для полноценного учета всех экономических составляющих ведения бизнеса, организациям необходимы различные виды сервисов и услуг, которые связаны между собой, однако представлены разных системах. Создание защищенного виртуального сервиса банковских услуг и ведения бухгалтерского учета упростит взаимодействие между банком и организациями и поддержит концепцию «электронного государства»

Концепция «электронного государства» – это организация взаимодействия органов государственной власти и общества в целях предоставления государственных услуг и обеспечения возможности участия в осуществлении власти населения с использованием информационно-телекоммуникационных технологий.

В современном мире любое предприятие связано с большим количеством различных сервисов. Это и взаимодействие с налоговыми, страховыми органами, и подача отчетности, статистики, а также платежи, ведение бухгалтерии и банковское обслуживание.

В рамах концепции «электронного государства» в настоящее время идет развитие системы электронного декларирования. Организациям предоставляется возможность дистанционной подачи всех видов деклараций посредством электронных сервисов. Такие системы позволяют предоставлять налоговую отчетность, сократить бумажный документооборот, избавляют от необходимости личного посещения налогового органа. Распространенной услугой такой системы является электронная отчетность. Электронная отчетность – это передача налоговой и бухгалтерской отчетности в электронном виде используя обычный доступ в Интернет. Вся информация, передаваемая в налоговые органы, передается в защищенном и зашифрованном виде, подписывается электронной цифровой подписью и имеет юридическую силу.

Для обеспечения дистанционного банковского обслуживания для предприятий в настоящее время банки предлагают систему Клиент-Банк. Однако ее нельзя назвать полноэффективной и автоматизированной для бизнеса, так как отсутствует возможность сдачи отчетности, ведения бухгалтерского, налогового учета и других необходимых функций.

Поэтому для удобства ведения бизнеса и централизованного управления всеми его экономическими аспектами предлагается интеграция облачных виртуальных бухгалтерских сервисов и банка. Подобный сервис позволит в автоматическом режиме формировать все необходимые клиенту виды отчетностей и деклараций, совершать все виды платежей и налогов, сдавать отчетность в электронном виде в различные государственные и налоговые органы, вести бухгалтерский учет.

Решение организуется на основе облачной модели Software as a Service, в которой поставщик разрабатывает веб-приложения, самостоятельно управляет ими, предоставляя клиентам доступ через Интернет. Потребитель использует эти приложения, запущенные в облачной инфраструктуре, которые доступны ему через интерфейс (web-браузер) или интерфейс программы. Архитектура SaaS-приложений, в которой единый экземпляр приложения, запущенный на сервере, обслуживает множество потребителей, является мультиарендной, то есть каждому потребителю в процессе выполнения задач предоставляется свой экземпляр виртуального приложения.

Принцип виртуализации представлен на рисунке 1:

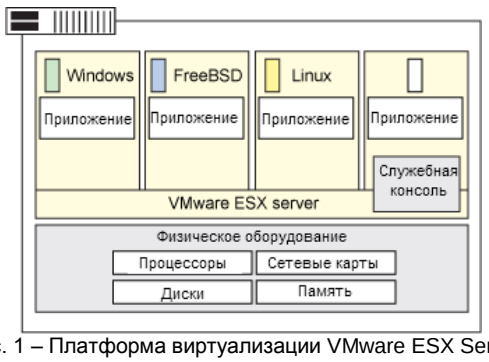


Рис. 1 – Платформа виртуализации VMware ESX Server

На рисунке видно, что операционные системы, работающие в виртуальных машинах, взаимодействуют с виртуальными ресурсами, как если бы это были физические ресурсы. ESX Server (гипервизор) исполняет одну виртуальную машину со служебной консолью и три дополнительные виртуальные машины, на которые устанавливаются приложения. Например, сервис для ведения

бухгалтерского учета.

Основными преимуществами виртуального сервиса являются:

а) единая точка доступа для пользования различными услугами;

б) интеграция сервисов и удобство пользования ими;

в) централизация и контроль в рамках «электронного государства».

Основными опасениями применения сервиса являются соображения безопасности и возможной утечки информации. Однако, защищенность SaaS-приложений находится на высоком уровне, поскольку данные системы развертываются в промышленных дата-центрах, использующих лучшие решения по информационной безопасности.

Список использованных источников:

1. VMware ESXi: Planning, Implementation, and Security – Dave Mishchenko, Course Technology, 2010.
2. Идеи электронного правительства для Беларуси [Электронный ресурс]. – Режим доступа : http://e-gov.by/.

МОДУЛЬ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ CRM-СИСТЕМЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гореликова Е.А.

Шевчук О.Г. – ассистент каф. СиУТ

С увеличением популярности электронного документооборота при взаимодействии с клиентами, требующего постоянной систематизации, растет необходимость в разработке системы, которая будет контролировать и управлять этим документооборотом, а также позволит упростить процедуру взаимодействия с клиентами.

CRM-система – это система управления взаимоотношениями с клиентами. Это специальные программные средства, позволяющие планировать задачи и контролировать их выполнение, вести учет клиентов, хранить документацию по проектам и автоматизировать ее создание, и многое другое.

Тестирование является неотъемлемой частью жизненного цикла для такого программного средства как CRM-система, так как эта система работает с важными данными и документами, то необходимо чтобы работа системы была налажена и не возникало никаких ошибок, которые могли бы привести к потере данных. Тестирование позволяет свести вероятность появления ошибки в системе к минимуму [1].

Автоматизация может помочь уменьшить время тестирования и упростить его процесс, используя различные инструменты для выполнения тестов и проверки результатов их выполнения.

Для автоматизации тестирования необходимо выбирать подходящие средства разработки и инструменты тестирования.

Схема взаимодействия модуля автоматизированного тестирования с CRM-системой представлена на рисунке 1:

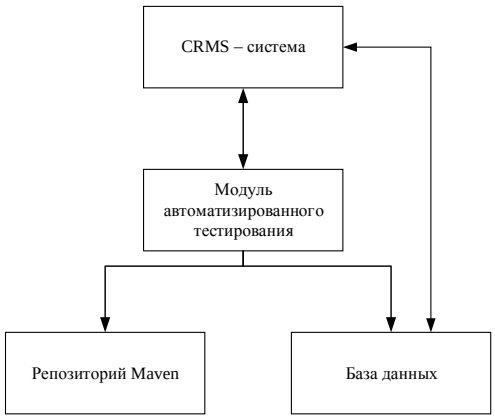


Рисунок 1 – Схема взаимодействия модуля автоматизированного тестирования с системой

На рисунке видно, что модуль автоматизированного тестирования напрямую взаимодействует с CRM-системой, выгружая всю необходимую информацию для проведения тестов.

Для построения архитектуры проекта используется репозирорий Maven. Maven – это инструмент для сборки Java проекта: компиляции, создания jar, создания дистрибутива программы, генерации документации.

Для подключения к базе данных используется JDBC драйвер. JDBC драйвер – это платформенно-независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД, реализованный в виде пакета java.sql, входящего в состав Java SE. Подключение к базе данных необходимо для проверки данных которые добавляются или удаляются из базы во время проведения тестов.

Smart Framework решение реализует шаблон PageObject. Шаблон PageObject упрощает поддержку тестов, уменьшает количество дублируемого кода.

Автоматизация позволяет ощутимо увеличить тестовое покрытие, но при этом столь же ощутимо увеличивает риски.

Преимуществами автоматизации тестирования являются:

– Скорость выполнения тест-кейсов может в разы и на порядки превосходить возможности человека.

– Отсутствие влияния человеческого фактора в процессе выполнения тест-кейсов (усталости, невнимательности).

– Минимизация затрат при многократном выполнении тест-кейсов (участие человека здесь требуется лишь эпизодически).

– Способность средств автоматизации выполнить тест-кейсы, в принципе непосильные для человека в силу своей сложности, скорости или иных факторов.

– Способность средств автоматизации выполнять низкоуровневые действия с приложением, операционной системой, каналами передачи данных и т. д.

Недостатками автоматизированного тестирования являются:

– Необходим высококвалифицированный персонал в силу того факта, что автоматизация – это «проект внутри проекта» (со своими требованиями, планами, кодом и т. д.).

– Высокие затраты на сложные средства автоматизации, разработку и сопровождение кода тест-кейсов.

– Автоматизация требует более тщательного планирования и управления рисками, т. к. в противном случае проекту может быть нанесён серьёзный ущерб.

– Средств автоматизации крайне много, что усложняет проблему выбора того или иного средства и может повлечь за собой финансовые затраты (и риски), необходимость обучения персонала (или поиска специалистов).

– В случае ощутимого изменения требований, смены технологического домена, переработки интерфейсов (как пользовательских, так и программных) многие тест-кейсы становятся безнадёжно устаревшими и требуют создания заново [2].

Привлечение средств автоматизированного тестирования может увеличить масштаб и размах тестирования в рамках ограниченных сроков и помочь исключить ручную, неинтересную и повторяющуюся работу, являющуюся трудоемкой и подверженной ошибкам. Автоматизированное тестирование позволит тестировщикам сосредоточить свои усилия на решении более сложных задач. Автоматизированное тестирование представляет собой инвестирование, которое требует тщательного планирования, определенного структурированного процесса, а также привлечения профессионалов в области программного обеспечения для выполнения и поддержки тестовых скриптов.

Эволюция автоматизированного тестирования породила многие должности для инженеров-программистов. Эта тенденция поддерживается международными стандартами качества и основами зрелости программного обеспечения, которые уделяют большое внимание тестированию программного обеспечения и другим дисциплинам по обеспечению качества продукта. Однако совершенно неверно полагать, что ручное тестирование будет полностью вытеснено автоматизацией, поскольку остаются множество видов работ, которые может выполнить только человек.

Список использованных источников:

1. The CRM: A Business Guide to Customer Relationship Management / Dyche J. – Addison-Wesley Professional, 2001. – 336 с.

2. Куликов С. С. Тестирование программного обеспечения. Базовый курс / С. С. Куликов. – Минск: Четыре четверти, 2015. – 294 с.

СИСТЕМА МОНИТОРИНГА ДЛЯ АНАЛИЗА И КОНТРОЛЯ ТРАФИКА СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров А.Ю.

Рассмотрены вопросы обеспечения мониторинга и управления сетью передачи данных, необходимые для этого протоколы и инструменты, а также преимущества использования комплексной системы управления и мониторинга сети. В качестве системы мониторинга и отслеживания статусов различных сервисов компьютерной сети, серверов и сетевого оборудования выбрана система Zabbix, имеющая ряд преимуществ по сравнению с другими.

Целью данной работы является анализ существующих решений по обеспечению мониторинга и управления сетью передачи данных, определение оптимального решения в отношении технических параметров и затраченных ресурсов для наладки и обслуживания выбранной системы.

Для современных вычислительных сетей требуются дополнительные специальные средства управления помимо тех, которые входят в состав стандартных сетевых операционных систем. Это объясняется большим количеством различного коммуникационного оборудования, от надежности работы которого зависит работа всей сети. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляет эту информацию оператору сети.

Выше отмечалось, что система управления работает обычно в автоматизированном режиме – выполняет наиболее простые действия по управлению сетью автоматически, а сложные решения, на основе подготовленной информации, реализуются при участии человека.

В связи с тем, что сами системы управления представляют собой сложные программноаппаратные комплексы, существует граница целесообразности применения системы управления, которая определяется сложностью сети, разнообразием применяемого коммуникационного оборудования и степенью его распределенности по территории. Однако при росте сети может возникнуть необходимость объединения разрозненных программ управления устройствами в единую систему управления, в связи с чем, возможно, придется отказаться от этих программ и заменить их интегрированной системой управления. Для поиска оптимальной системы управления проведем сравнение систем мониторинга по следующим параметрам.

1. Формирование отчетов SLA (Service Level Agreement). Контроль гарантированных параметров качества обслуживания SLA, определяющих межоператорские взаимоотношения.

2. Формирование трендов. Выявление основных тенденций динамики показателей качества работы телекоммуникационной сети.

3. Прогнозирование трендов. Прогнозирование изменения динамики показателей качества работы телекоммуникационной сети.

4. Анализ топологии сети. Сбор информации об элементах сети.

5. Использование агентной модели мониторинга. Наличие устройств, осуществляющих сбор и передачу информации о работе сети.

6. Поддержка SNMP (Simple Network Management Protocol). Использование протокола SMNP для обмена информацией о состоянии объектов наблюдения в режиме реального времени.

7. Протоколирование событий. Формирование подробных записей о состоянии элементов сети.

8. Датчики внештатных ситуаций. Наличие устройств для оповещения о возникновении критических ситуаций, негативной тенденции к изменению показателей качества работы телекоммуникационной сети.

9. Распределенный мониторинг. Мониторинг сигнального обмена на предмет соответствия работы оборудования определенным спецификациям протоколов.

Результаты сравнительного анализа приведены в табл. 1.

Таблица 1.**Сравнительный анализ систем мониторинга**

Системы мониторинга	Параметры								
Argus									
Intellipool Network Monitor									
IPHost Network Monitor									
NetMRI									

NetQoS Performance Center									
OPNET ACE Live									
Opsview									
Scrutinizer									
Orion									
Zenoss									
Nagios									
Zabbix									

Анализ показал, что системы мониторинга, предлагаемые на мировом рынке, сходны по выполняемым функциям. Все они предоставляют почти одинаковый минимальный набор возможностей, однако каждая из них характеризуется определенными недостатками: в большинстве систем вообще не реализованы возможности прогнозирования трендов, а в системах, где они реализованы, построение происходит на основе устаревшей статистической информации. Подобное прогнозирование не учитывает фрактальность трафика, нелинейность характеристик и не стационарность процессов. Обобщив предложенные выше решения, можно синтезировать общую архитектуру системы мониторинга и управления. Все рассмотренные системы мониторинга основаны на использовании агентного подхода. Агенты собирают статистическую информацию о работе элементов сети и передают ее в центральную базу данных, затем собранная информация обрабатывается управляющими модулями. В состав системы мониторинга должны входить следующие компоненты: формирование отчетов, модуль управления SNMP, архив и консоль управления. Модуль формирования отчетов позволяет формировать из имеющихся данных информацию для принятия управленческих решений. Модуль управления SNMP отвечает за сбор информации с агентов мониторинга и взаимодействие с системами управления. Архив позволяет упорядочить хранение статистической информации и организовать последующую работу с ней. Консоль управления реализует функции конфигурирования и управления системой.

Для корпоративной сети передачи данных наиболее полезным инструментом будет протокол NetFlow, т. к. в связке с этой утилитой могут использоваться пакеты данных для представления данных в более удобном пользователю виде. По результатам анализа инструментов и средств мониторинга сделан вывод о том, что наибольшая надежность сети и наиболее эффективная передача данных обеспечиваются при использовании комплекса протоколов NetFlow и SNMP

Список использованных источников:

1. Simple Network Management Protocol (SNMP). [Электронный ресурс]. – Режим дос- тупа: http://www.ieft.org/rfc1157.txt.. – Дата доступа: 12.06.2016

2. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil [Электронный ресурс]. – Режим дос- тупа: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html... – Дата доступа: 13.06.2016

3. Olups R. Zabbix 1.8 Network Monitoring. [Электронный ресурс]. – Режим дос- тупа: http://www.amazon.co.uk/Zabbix-Network-Monitoring-Rihards-Olups/dp/184719768. – Дата доступа: 18.07.2016

THE SIMULATING PROGRAM OF INFORMATION TRANSFER BY MEANS OF THE CODES SUPERVISING ERRORS

The Belarus state university of computer science and radio electronics
P.Brovki, 6, Minsk, 220013, Belarus

IBRAHIM JAD, NADJAFI HADI MOHAMMED
I. I. ASTROVSKY – PhD, associate professor

Considering the questions on working out a complex of programs in MATLAB programming system, that simulates systems of information transfer with the help of block codes that are considered to control the errors. Mathematical apparatus polynomial algebras to describe the signals and the ways of their processing are used.

Keywords: telecommunications, signals, noise, information transfer, MATLAB, binary polynomes, noise proof coding

Introduction

Nowadays it is impossible to present the communication outer-space systems, the space research systems, radar-tracking systems, radio-navigating systems, reserved and even usual telecommunication systems without application of noiseproof signals coding. Each engineer working in the field of telecommunications is obliged to know methods of spectral processing, correlation processing and the co-ordinated filtration of signals.

It is well known that side by side with the lectures materials studying laboratory works play the important role in the research allowing visually to consider and comprehensively to study processes of transfer and reception of the information and the methods of struggle against hindrances and interference. From the end of 1980th, MATLAB became very popular [1,2]. MATLAB programming system often are used by engineers and scientists because of its big possibilities and relative simplicity of programming.

Modeling of telecommunication systems

To study the process of information transfer of the codes supervising errors, in the complex of programs are used a block codes. Despite presence of huge number of functions in system MATLAB including operations with polynomial equations, it was necessary to add a class of functions with the methods, capable to carry out operation over binary polynomes. It allowed to model and consider binary signals from the polynomial view and matrix algebra that facilitates and simplifies the description and study processes of the signals. Initial signals are set by factors of binary polynomes, but with a view of control on the screen their record in the form of polynomes is deduced.

In the developed complex of programs all commands and processes of processing of signals, since the task of signals and hindrances, are set in a command window (fig.1-7) and results of their performance are displayed in an additional window (fig.8).

Interaction of the user occurs to a program complex in an interactive mode. The program prompts possible actions of the user, and in case of incorrect commands or the data specifies in errors and offers ways of their elimination.

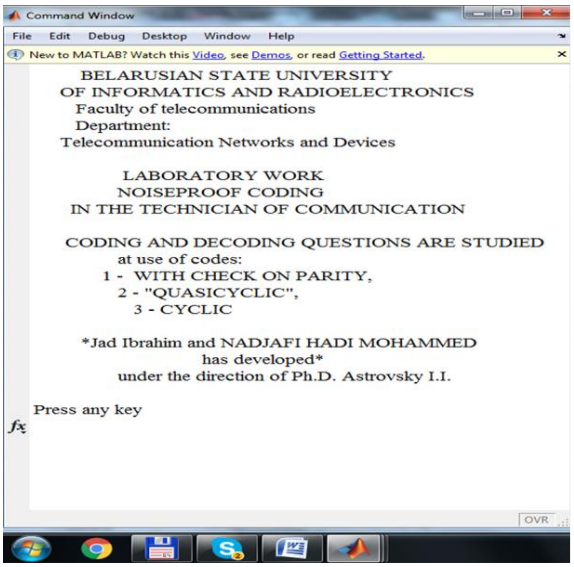


Fig. 1 Header window of the program

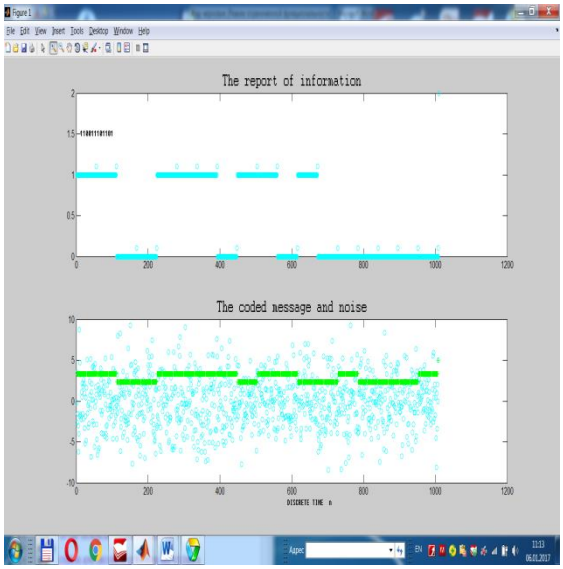


Fig. 2 Signal and mix of a signal with noises

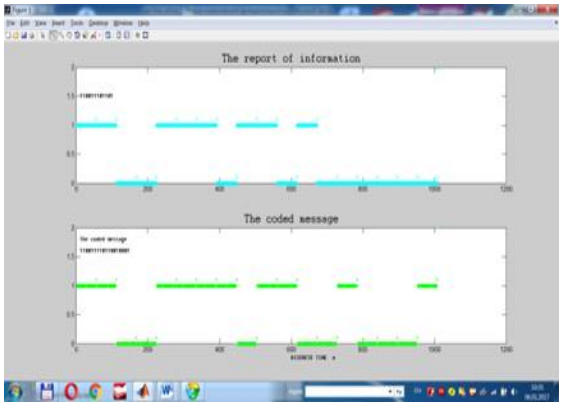


Fig. 3 Coding with parity check

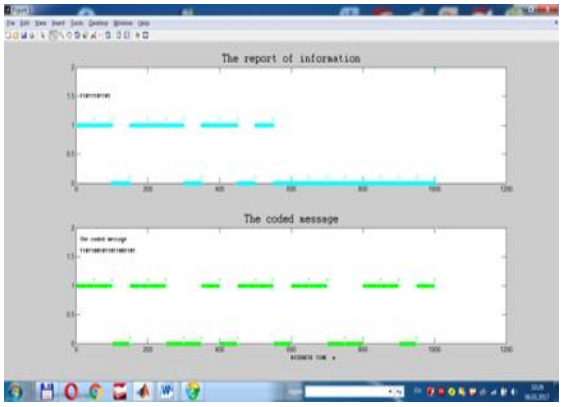


Fig. 4 Matrix coding

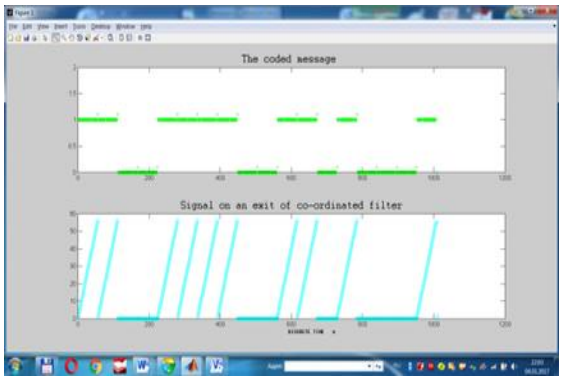


Fig. 5 Processed by means of the co-ordinated filter in the absence of noise

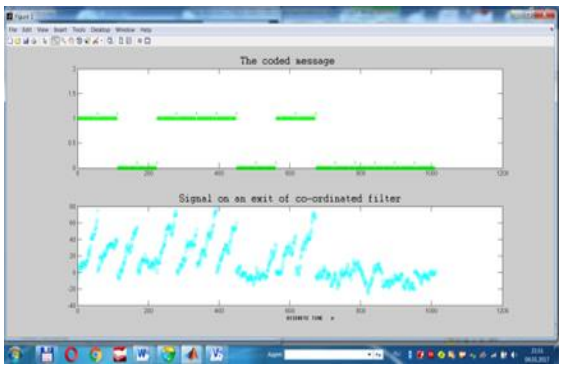


Fig. 6 Processed by means of the co-ordinated filter in the presence of noise

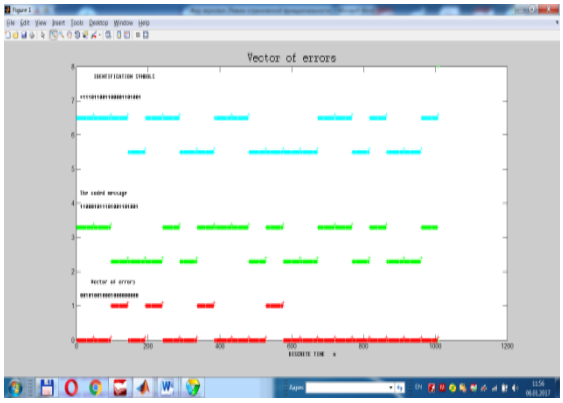


Fig. 7 Identification symbols an accepted signal at coding by noiseproof algorithms

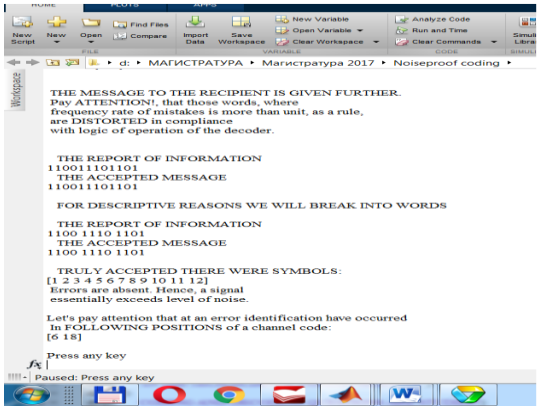


Fig. 8 Identification symbols an accepted signal at coding by noiseproof algorithms

Conclusion

The presented screenshots show separate stages of the program, including the preliminary task, the task for performance, theoretical data and methodical instructions on work with software product. The program is supplied by its own calculator to calculate the generalized characteristics of signals and noises under the set experimental conditions.

References

1. Сергиенко, А.Б. Цифровая обработка сигналов/ А.Б. Сергиенко. – СПб.: Питер, 2003. – 604 с.
2. Цифровая обработка сигналов и МАТЛАБ: учеб. пособие/ А.И. Солонина, Д.М. Клионский, Т.В. Меркучева, С.Н. Перов. – СПб.: БХВ-Петербург, 2014. – 512 с.
3. King, P.R. Modeling and Measurement of the Land Mobile Satellite MIMO Radio Propagation Channel/ P.R. King // University of Surrey. – 2007.

ИСПОЛЬЗОВАНИЕ BIG DATA В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Шишпорёнок С.С., Сергеев Н.Н.

Урядов В.Н. – к.т.н.,доцент

«Big Data» — комплекс технологий, которая активно обсуждается многими, в том числе и телекоммуникационными компаниями. Некоторые из них успели разочароваться в «Big Data», другие — напротив, максимально используют для бизнеса.

Big data, на сегодняшний момент, является одним из ключевых векторов развития информационных технологий. Это направление, относительно новое, получило широкое распространение в западных странах. Связано это с тем, что в эпоху информационных технологий, особенно после бума социальных сетей, по каждому пользователю интернета стало накапливаться значительное количество информации, что в конечном счете дало развитие направлению Big Data.

Термин «Big Data» вызывает множество споров, многие полагают, что он означает лишь объем накопленной информации, но не стоит забывать и о технической стороне, данное направление включает в себя технологии хранения, вычисления, а также сервисные услуги.

Следует отметить, что к данной сфере относится обработка именно большого объема информации, который затруднительно обрабатывать традиционными способами. Ниже в таблице 1 представлена сравнительная характеристика традиционной базы и «Big Data».

Сфера «Big Data» характеризуется следующими признаками:

Volume – объем, накопленная база данных представляет собой большой объем информации, который трудоемко обрабатывать и хранить традиционными способами, для них требуются новый подход и усовершенствованные инструменты.

Velocity – скорость, данный признак указывает как на увеличивающуюся скорость накопления данных (90% информации было собрано за последние 2 года), так и на скорость обработки данных, в последнее время стали более востребованы технологии обработки данных.

Variety – многообразие, т.е. возможность одновременной обработки структурированной и неструктурированной разноформатной информации. Главное отличие структурированной информации – это
то, что она может быть классифицирована. Примером такой информации служит информация о клиенте.

Неструктурированная информация включает в себя видео, аудио файлы, свободный текст, информацию, поступающую из социальных сетей. На сегодняшний день 80% информации входит в группу неструктурированной. Данная информация требует комплексного анализа, чтобы сделать ее полезной для последующей обработки.

Veracity – достоверность данных, все большее значение пользователи стали придавать значимость достоверности имеющихся данных. Так, у интернет-компаний есть проблема по разделению действий, проводимых роботом и человеком на сайте компании, что приводит в конечном счете к затруднению анализа данных.

Value – ценность накопленной информации. Big Data должна быть полезны компании и приносить определенную ценность для нее. К примеру, помогать в усовершенствовании бизнес-процессов, составлении отчетности или оптимизации расходов.

При соблюдении указанных выше 5 условий, накопленные объемы данных можно относить к числу «Big Data».

Таблица 1. Сравнительная характеристика традиционной базы данных и «Big Data»

Характеристика	Традиционная база данных	«Big Data»
Объём информации	От гигабайт до терабайт	От петабайт до эксабайт
Способ хранения	Централизованный	Децентерализованный
Структурированность данных	Структурирована	Неструктурирована
Модель хранения и обработки данных	Вертикальная модель	Горизонтальная модель
Взаимосвязь данных	Сильная	Слабая

По данным опроса Accenture, в более чем 50% компаниях, использующих технологии «Big Data», затраты на Big Data составляют от 21% до 30%.

Согласно следующими анализу Accenture, 76% компаний, считают, что данные расходы увеличатся в 2015 году, а 24% компаний не изменят своего бюджета на технологии «Big Data». Это говорит о том, что в данных компаниях Big Data стали уже устоявшимся направлением ИТ, ставшим неотъемлемой частью развития компании.

Результаты опроса Economist Intelligence Unit survey подтверждают положительный эффект от внедрения Big Data. 46% компаний заявляют, что с помощью технологий «Big Data» они улучшили клиентский сервис более, чем на 10%, 33% компаний оптимизировали запасы и улучшили продуктивность основных активов, 32% компаний улучшили процессы планирования.

По состоянию на сегодняшний день, отечественный рынок «Big Data» не настолько популярен как в развитых странах. Большинство отечественных компаний проявляют интерес к big data, но воспользоваться возможностями не решаются.

Примеры крупных компаний, которые уже извлекли выгоду от использования технологий «Big Data», расширяют осознание возможностей данных технологий. У аналитиков также достаточно оптимистичные прогнозы относительно рынка.

По итогам 2016 года рынок «Big Data» характеризуется следующими параметрами:

- объем рынка составил 28,5 млрд долл. США, увеличившись на 45% по сравнению с предыдущим годом;
- большую часть выручки рынка Big Data составили сервисные услуги, их доля была равно 40% в общем объеме выручки;
- 36% выручки принесли приложения и аналитика «Big Data», 17% вычислительное оборудование и 15% — технологии хранения данных;
- наибольшей популярностью для решения проблем «Big Data» пользуются in-memory платформы таких компаний, как SAP, HANA и Oracle.
- на 125% увеличилось количество компаний с реализованными проектами в сфере управления «Big Data»;

Прогноз рынка на следующие годы выглядит следующим образом:

- в 2015 году объем рынка достигнет 38,4 млрд долл. США, в 2020 году – 68,7 млрд долл. США;
- средний темп роста будет равен 16% ежегодно;
- средние затраты компании на технологии «Big Data» составят 13,8 млн долл. США для крупных компаний и 1,6 млн долл. США для малого и среднего бизнеса;
- технологии будут иметь наибольшую распространенность в сферах клиентского сервиса и точечного маркетинга;
- в 2017 году изменится общемировая структура рынка в сторону преобладания компаний-пользователей из развивающихся стран. Российский рынок «Big Data» находится на стадии формирования, результаты 2014 года выглядят следующим образом:
- объем рынка достиг 340 млн долл. США;
- средний темп роста рынка в предыдущие годы составил 50% ежегодно;
- общий объем накопленной информации составил 155 эксабайт;
- 10% российских компаний начали использовать технологии «Big Data»;
- большей популярностью технологии «Big Data» пользовались в банковской сфере, телекоммуникациях, интернет-компаниях и ритейле.

«Big Data» получили широкое распространение во многих отраслях бизнеса. Их используют в здравоохранении, телекоммуникациях, торговле, логистике, в финансовых компаниях, а также в государственном управлении.

В телекоммуникационной отрасли широкое распространение «Big Data» получили у сотовых опер ато-ров.

Операторы сотовой связи наравне с финансовыми организациями имеют одни из самых объемных баз данных, что позволяет им проводить наиболее глубокий анализ накопленной информации. Главной целью анализа данных является удержание существующих клиентов и привлечение новых. Для этого компании проводят сегментацию клиентов, анализируют их трафики, определяют социальную принадлежность абонента.

Так же широкое распространение базы больших данных могут получить в системах контроля и управления, поскольку с увеличением числа абонентов будет неуклонно увеличиваться размер сетей и объём данных в них. Использование баз больших данных позволит производить более быстрый и детальный анализ данных об ошибках, параметров устройств и т.д., что позволит повысить качество услуг связи.

Одним из ярких примеров данной отрасли является российская компания Вымпелком. Компания применяет «Big Data» для повышения качества обслуживания на уровне каждого абонента, составления отчетности, анализа данных для развития сети, борьбы со спамом и персонализации услуг.

По результатам анализа можно сделать вывод о том, что рынок Big Data все еще находится на ранних стадиях развития, и в ближайшем будущем мы будем наблюдать его рост и расширение возможностей данных технологий. Внедрение Big Data в сетях телекоммуникаций требует дополнительных вложений, например, на переписание структуры традиционных реляционных баз данных. Поэтому для внедрения Big Data в сетях телекоммуникациях требуется провести анализ количества данных, используемых в базе.

Список использованных источников:

1. Habrahabr: Аналитический обзор рынка Big Data. [Электронный ресурс].–Режим дос-тупа: https://habrahabr.ru/company/moex/blog/256747/.–Дата доступа: 26.03.2017.

2. Московская Биржа: Глобальный обзор рынка Big Data. [Электронный ресурс].–Режим дос-тупа: http://moex.com/n14540/?nt=120.–Дата доступа: 26.03.2017.

ВЛОЖЕННОЕ И ЭНТРОПИЙНОЕ КОДИРОВАНИЕ ГИПЕРСПЕКТРАЛЬНЫХ СПУТНИКОВЫХ ИЗОБРАЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ловецкий М.Ю., Мирончик Д.Ю.

Рост объёма данных, передаваемых по различного рода сетям, в настоящее время опережает рост пропускной способности каналов, на которых эти сети построены. Примером сети с ограниченной пропускной способностью является система дистанционного зондирования земли (ДЗЗ), требующая алгоритм сжатия изображений, который обладал бы высоким коэффициентом сжатия и потенциалом для распараллеливания вычислений.

Как правило, соседние пиксели изображения имеют близкие значения яркости, т.е. коррелированы. Следовательно, сжатие изображений можно осуществлять с помощью декорреляции – такого перераспределения общей энергии изображения, что большая её часть лежит в относительно узком диапазоне. На сегодняшний день наиболее эффективны (по качеству и быстродействию) спектральные алгоритмы сжатия изображений, одним из которых является вейвлет-преобразование – стандарт в области декорреляции пикселей.

Полученную в результате такого преобразования матрицу вейвлет-коэффициентов необходимо развернуть в одномерный массив так, чтобы сохранить вложенность её пространственно-частотных диапазонов (это особенно важно для сжатия с потерями, т.к. поток должен быть упорядочен по убыванию значимости его составляющих) – эту задачу выполняет Z-развёртка. Её алгоритм может быть описан так: матрица разделяется на четыре равные части и считывается в следующем порядке – верхний левый сегмент, верхний правый, нижний левый, нижний правый. Процедура повторяется вплоть до отдельных элементов.

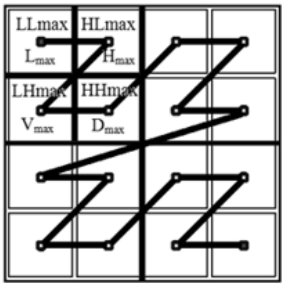


Рис. 1 – Z-развёртка на примере матрицы 4 на 4

В целях снижения объёмов используемой памяти и создания возможности распараллеливания вычислений было принято решение разбивать матрицу вейвлет-коэффициентов на блоки размером 32 на 32. Каждый из этих блоков проходит Z-развёртку и вложенное кодирование; результат становится частью выходного потока.

После Z-развёртки одного блока образовывается одномерный массив из 1024 элементов, который содержит вейвлет-коэффициенты в виде целых чисел со знаком. Точно так же, как все эти числа представимы в виде значений двоичных разрядов, блок представим в виде набора битовых плоскостей, каждая из которых (под номером n) содержит n-ые разряды этих чисел. Одна из таких плоскостей будет являться плоскостью знаков.

Битовые плоскости кодируются по убыванию, при этом номер старшей битовой плоскости определяется номером старшего разряда самого большого абсолютного значения среди кодируемого блока. Используется бинарное кластерное дерево с размером кластера, равным четырём, показавшем в ходе экспериментов наилучшие показатели сжатия. Число уровней кластерного дерева выбирается из нулевого (отсутствие вложенного кодирования), первого и четвёртого – на каждом шаге алгоритма из трёх вариантов для записи в выходной поток выбирается кратчайший. Принцип прост – один элемент текущего уровня соответствует четырём элементам предыдущего уровня. Если среди этих четырёх элементов есть хоть одна единица, то соответствующий элемент следующего уровня равен единице, иначе – нулю.

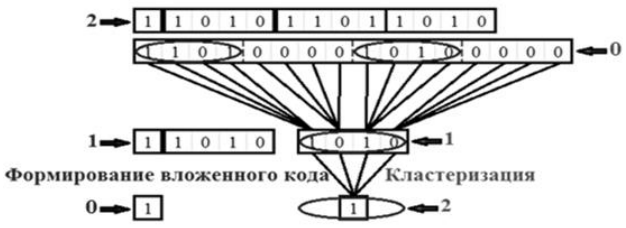


Рис. 2 – Формирование вложенного кода

Помимо формирования вложенного кода, отдельно обрабатываются знаки значащих (ненулевых) бит блока. Поскольку некоторое количество вейвлет-коэффициентов равно нулю, то выделение значащих бит на каждой битовой плоскости позволит помимо обеспечения прогрессивности потока сжать плоскость знаков (нули не имеют знака). Принцип формирования кода знаков тоже несложен: если число значащее – в выходной поток передаётся его знак. Для этого достаточно проверки знаковой плоскости на неравенство нулю. Если элемент плоскости не равен нулю, происходит сверка с маской – не была ли произведена запись знака данного элемента. Если маска в этом месте пуста – в код знаков добавляется знак данного элемента, а маска обновляется.

Итоговый выходной поток состоит из набора последовательностей «четыре бита, в которых закодирован номер старшей битовой плоскости – флаг, указывающий на уровень вложенного кода – вложенный код – код знаков», соответствующих каждому закодированному блоку.

Дальнейшее увеличение коэффициента сжатия возможно при использовании энтропийного кодирования.

Энтропийное кодирование основывается на следующем факте: если вероятности появления различных символов в последовательности одинаковы, то энтропия – количество информации, приходящейся на один символ источника – максимальна. Таким образом, необходимо усреднить вероятности появления символов в описанном выше потоке, для чего используется код Хаффмана.

Кодирование по Хаффману состоит в сопоставлении наиболее вероятным символам исходной последовательности кодов наименьшей длины, а менее вероятным – кодов большей длины. Соответственно, предполагается, что вероятности появления тех или иных символов известны, так что необходимо провести статистический анализ выходного потока.

Из проведённого для разнородных изображений анализа следует, что распределение вероятностей появления различных символов в сегментах вложенного кода (EC) не является равномерным, что означает возможность их сжатия. Поскольку эти сегменты состоят из четырёхбитных кластеров, сплошное энтропийное кодирование с четырёхбитным окном требует мало аппаратных ресурсов и показывает неплохие результаты, однако для дальнейшего повышения эффективности нужно учесть внутреннюю структуру этих сегментов.

Вложенный код нулевого уровня (EC0) отличается от других вариантов вложенного кода своей шумоподобностью, так что энтропийное кодирование таких сегментов существенного выигрыша не принесёт (однако в целом оно возможно для 8-битных символов). Сегменты EC4 и EC1 похожи по структуре, но каждый из них следует разбить далее – на первый уровень сегмента и оставшуюся часть сегмента, которая получается из первого уровня путём логического суммирования битов кластера.

Сегменты кода знаков (SC) ещё более шумоподобны, чем EC0, и энтропийному кодированию не подлежат.

Таким образом, задача энтропийного кодирования заключается в построении деревьев кода Хаффмана для первого и последующих уровней EC4 (окно 4-битное), для первого и второго уровня EC1 (окно также 4-битное) и, возможно, для EC0 (окно 8-битное) – итого пяти деревьев, которые достаточно построить один раз и занести в память, и замене исходных 4-битных и 8-битных символов на код Хаффмана. Служебная информация – первые четыре бита закодированного блока, флаги – остаётся неизменной, так как необходима для декодирования, сегменты кода знаков так же передаются без изменений.

Код Хаффмана строится так: символы располагают в порядке убывания их вероятностей, складывают вероятности двух последних символов, переписывают ряд снова с учетом новой вероятности (суммы). Операцию повторяют, пока не получится 1. Нижнюю букву всегда кодируют нулем, а верхнюю – единицей.

Код Хаффмана является префиксным, что означает выполнение условия Фано: никакое кодовое слово не может быть началом другого кодового слова. Это позволяет записывать получившийся код без каких-либо разделительных символов и при необходимости однозначно его декодировать.

Программное моделирование описанного алгоритма показало, что его коэффициент сжатия близок к таковому у эталонного JPEG2000, а скорость существенно больше за счёт высокой степени распараллеливания. Кроме того, данный алгоритм лучше подходит для реализации в ПЛИС.

Список использованных источников:

1. Новицкий В.В., Цветков В.Ю. Сжатие полутоновых изображений на основе кластеризации и прогрессивного вложенного кодирования вейвлет коэффициентов / В.В. Новицкий, В.Ю. Цветков // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. научно-технич. семинара. Минск, апрель–декабрь 2015 г. – Мн.: БГУИР, 2015. – С. 45-51.

2. Борискевич, А.А. Метод масштабируемого вложенного кодирования изображений на основе иерархической кластеризации вейвлет структур / А.А. Борискевич, В.Ю. Цветков // Доклады НАН Беларуси. − 2009. Т. 53, № 3. – С. 38 – 48.

3. Гонсалес Р. Цифровая обработка изображений. / Р. Гонсалес, Р. Вудс. – Пер. с англ. − Москва. – Техносфера, – 2006. − 1072 с.

АВТОМАТИЗАЦИЯ МАСШТАБИРОВАНИЯ ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ SDN

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пархомик С.Ю.

Селезнев И.Л. – к.т.н.,доцент

В современном мире, бизнес в сфере информационных технологий предъявляет большие требования к гибкости и масштабируемости компьютерных сетей. **С быстрым ростом объемов сетевого трафика и количества подключенных к сети устройств, конфигурирование крупномасштабных сетей превращается в сложную задачу.** В традиционных коммутаторах и маршрутизаторах процессы передачи трафика и управления им неотделимы друг от друга и реализованы в одной «коробке»: специальные микросхемы обеспечивают пересылку пакетов с одного порта на другой, вышележащее ПО определяет правила такой пересылки, выполняет необходимый анализ пакетов, производит изменение содержащейся в них служебной информации и т.п. Все узлы в сети конфигурируются индивидуально и остаются статичными.

В условиях быстрого роста компьютерных сетей, особенно актуальна задача упрощения добавления и настройки новых сетевых устройств, которая решается при помощи технологии SDN (software-defined networking, программно-определяемая сеть). С использованием технологии SDN пользователи получают возможность управлять, настраивать и контролировать сети с помощью отдельных контроллеров. Это обеспечивает систему, в которой управление различными узлами происходит через одно устройство, а не множество, как раньше. **Главная идея платформы SDN** заключается в отделении функций передачи трафика от функций управления (включая контроль как самого трафика, так и осуществляющих его передачу устройств). Контроллер предоставляет программные интерфейсы (API), наличие которых позволяет создавать приложения для управления сетью. Такие приложения могут выполнять самые разные функции (контролировать доступ, управлять пропускной способностью сети и т.п.) (рисунок 1).

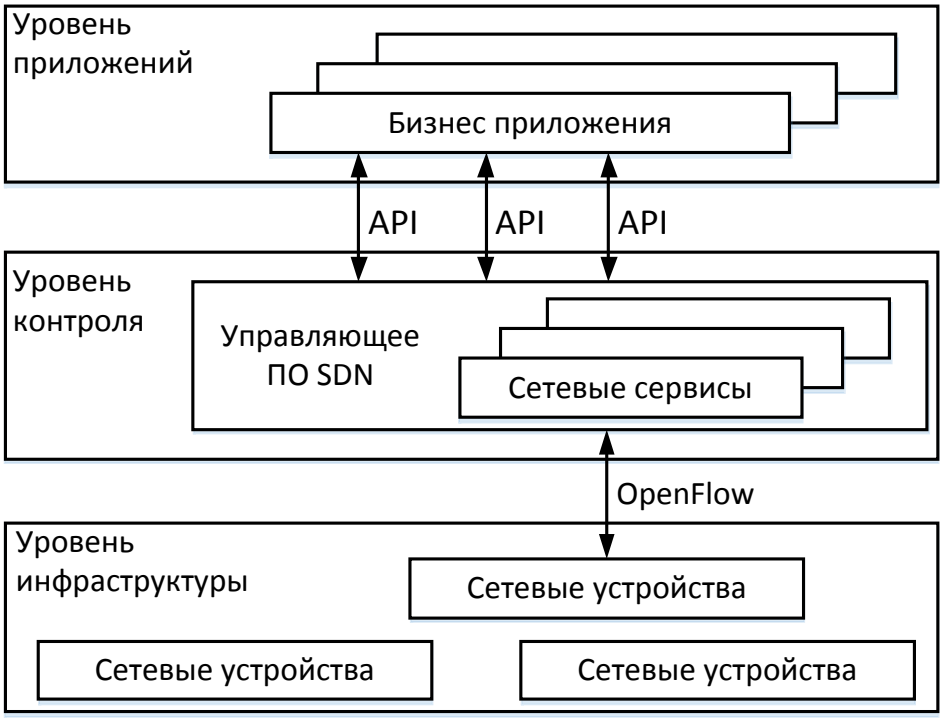
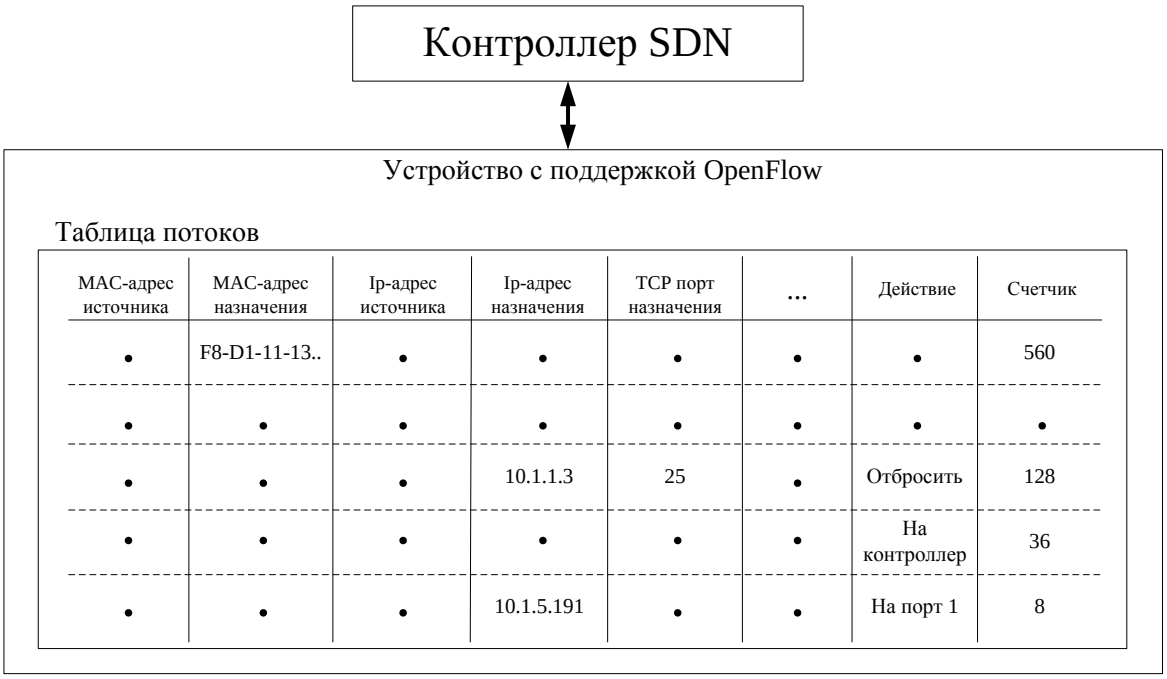


Рисунок 1 – Архитектура технологии SDN

Основным элементом технологии SDN является протокол OpenFlow, который обеспечивает взаимодействие контроллера с сетевыми устройствами. Контроллер используется для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом, в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами. Ключевым элементом коммутатора, поддерживающего Openflow, является таблица потоков (Flow Table) (рисунок 2).



MAC-адрес источника	MAC-адрес назначения	Ip-адрес источника	Ip-адрес назначения	TCP порт назначения	…	Действие	Счетчик
•	F8-D1-11-13..	•	•	•	•	•	560
•	•	•	•	•	•	•	•
•	•	•	10.1.1.3	25	•	Отбросить	128
•	•	•	•	•	•	На контроллер	36
•	•	•	10.1.5.191	•	•	На порт 1	8

Рис

унок 2 – Пример таблицы потоков протокола OpenFlow.

Группа столбцов в левой части таблицы формирует поля соответствия, где указаны характеристики потоков: это могут быть различные параметры, включая MAC- и IP-адреса отправителя и получателя, идентификатор VLAN, номера протокольных портов TCP и UDP, а также другая информация. Эти данные с помощью протокола OpenFlow записывает в таблицу коммутатора контроллер, он же определяет приоритет разных потоков: чем выше приоритет, тем выше соответствующая запись в таблице потоков. Используя протокол OpenFlow, контроллер добавляет, модифицирует и удаляет записи в таблице потоков. Кроме того, он может запрашивать у коммутатора его характеристики и собранную статистику, конфигурировать коммутатор и его отдельные порты.

Таким образом подход к управлению и автоматизации сети с использованием технологии SDN позволяет централизовать управление мультивендорной средой, значительно упростить обслуживание и модернизацию сети, а также сократить время на обновление настроек сетевого оборудование и внедрение новых сервисов.

Список использованных источников:

1. Смелянский Р.Л. Программно-конфигурируемые сети // Открытые системы [Электронный ресурс] – Режим доступа: http://www.osp.ru/os/2012/09/13032491/

2. Architecture SDN // Open Networking Foundation [Электронный ресурс] – Режим доступа: https://www.opennetworking.org/

3. Software-Defined Networking: The New Norm for Networks // Open Networking Foundation [Электронный ресурс] – Режим доступа: https://www.opennetworking.org/images/stories/downloads/sdn-resources/whitepapers/wp-sdn-newnorm.pdf.

ОБЛАЧНЫЙ СЕРВИС ВКС

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гороховик В.А., Тарасовец В.В.

Лагутин А.Е. – к.т.н.

Бизнес будет всегда стремиться к тому, чтобы увеличить скорость принятия решений и качество внутренних и внешних корпоративных коммуникаций. Сегодня особенно актуально при этом достичь ещё и максимальной экономии средств. Наиболее проверенный и эффективный способ сократить расходы – использовать видеоконференцсвязь (ВКС) вместо командировок для проведения совещаний и рабочих встреч. Многие компании строят собственную ВКС-инфраструктуру. Однако есть еще один способ, который позволяет избежать капитальных затрат на ее (инфраструктуру) создание или модернизацию, получив при этом требуемый для поддержания бизнес-процессов сервис. Это видеоконференцсвязь как услуга из облака.

Круг компаний, которым нужна видеоконференцсвязь, очень широк: промышленность, ТЭК, финансовой сектор, ритейл. Главные условия – наличие удаленных офисов и потребности в общении с сотрудниками, подрядчиками, партнерами не только на уровне директивных писем и отчетов. Любые совещания, переговоры, обучающие семинары могут проводиться с минимальным вложением средств. Благодаря ВКС исключаются расходы на авиа и ж/д билеты, на гостиницы и командировочные.

Сервис ВКС из облака позволяет участвовать не только в конференциях, но и пользоваться единым списком контактов, обмениваться мгновенными текстовыми сообщениями, совместно работать над документами, осуществлять запись видеосеансов.

Особенности подключения

Для подключения облачной видеоконференцсвязи не нужно ничего, кроме конечного оборудования в переговорных комнатах. Если у заказчика нет такого оборудования, его можно взять в аренду.

Принять участие в сеансе видеосвязи можно также и с мобильных устройств посредством программного клиента. Точно так же, как пользователи работают с облачной почтой или мессенджерами, они могут подключаться к ВКС со своих планшетов, телефонов или ноутбуков[1].

Структурная схема облачной видеоконференции представлена на рисунке 1.

Рисунок 1 – Структурная схема облачной видеоконференции

Внешние участники, компании которых не имеют собственной ВКС-инфраструктуры, подключаются через web-браузер или систему унифицированных коммуникаций Skype for Business (Microsoft Lync).

Одним из главных преимуществ облачной услуги ВКС является возможность не вкладываться в закупки дорогостоящего оборудования для проведения видеосеансов. Вместо этого заказчик по подписке получает сервис, уже развернутый в ЦОДе системного интегратора.

Управление и оптимизация

Облачной ВКС просто управлять и возможно быстро масштабировать по запросу, например, когда требуется провести расширенную встречу. И неважно, что такое может быть нечасто, а обычная нагрузка – совещание на 5–10 человек. Когда компания создает такую технологически гибкую ВКС на базе собственной инфраструктуры (иными словами обеспечивает на постоянной основе возможность проведения сеансов видеоконференцсвязи на 50–100 человек) техническое обслуживание и модернизация обходятся достаточно дорого[2].

Кроме того, с помощью облачной ВКС компания-заказчик может оптимизировать расходы на ИТ-персонал. Инфраструктуру на стороне системного интегратора нет необходимости администрировать, держать для этого отдельных сотрудников или давать дополнительную нагрузку на существующих. Для заказчика все происходит автоматически: пользователи звонят на номера общей конференции и включаются в нее. Но по желанию заказчика инструменты управления услугой могут быть предоставлены его ИТ-службе.

Безопасность передачи данных заказчиков при использовании услуги ВКС, как правило, обеспечивается на нескольких уровнях. В рамках первого уровня защита подключения к конференции осуществляется при помощи паролей (PIN-кодов) и управления списком участников заказчиком, в рамках второго – посредством подключения выделенного канала связи и специальных средств шифрования трафика, доступно опционально[2].

Записи переговоров заказчиков хранятся в дата-центре, который надежно защищен от сетевых угроз, будь то DDoS-атаки, попытки несанкционированного доступа или сетевое сканирование. Для этого применяются различные средства защиты: системы обнаружения и предотвращения вторжений (IDS/IPS), системы предотвращения DDoS-атак и пр.

Список использованных источников:

1. Polycom [Электронный ресурс]. – Режим доступа : http://www.polycom.com.ru.

2. Интернет-издание о высоких технологиях [Электронный ресурс]. – Режим доступа : http://www.cnews.ru.

ПРОЕКТИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Семак А.Д.

Селезнев И.Л. – к.т.н.,доцент

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Эта «комплексность» заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Значительное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Важнейшим устройством, обеспечивающим безопасность корпоративной сети предприятия, является межсетевой экран. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Существует два принципа обработки поступающего трафика. Первый принцип гласит: «что явно не запрещено, то разрешено». В данном случае, если межсетевой экран получил пакет, не подпадающий ни под одно правило, то он передается далее. Противоположный принцип – «что явно не разрешено, то запрещено» – гарантирует гораздо большую защищенность, так как он запрещает весь трафик, который явно не разрешен правилами.

В большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при их классификации (рисунок 1). Учитывая данную модель, различают следующие типы межсетевых экранов:

1) управляемые коммутаторы;
2) пакетные фильтры;
3) шлюзы сеансового уровня;
4) посредники прикладного уровня;
5) инспекторы состояния.

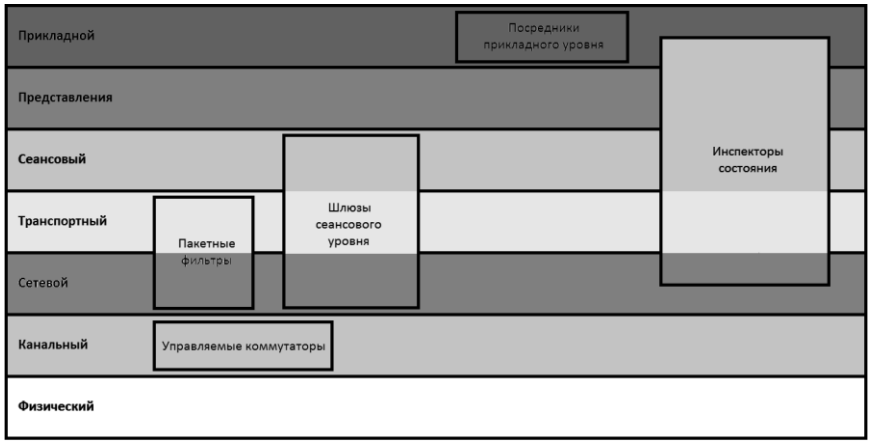


Рисунок 1 – Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

Существует два варианта исполнения межсетевых экранов – программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности: в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

Межсетевой экран не в состоянии решить все проблемы безопасности корпоративной сети. Имеется ряд ограничений в их использовании, а также существуют угрозы, от которых межсетевые экраны не могут защитить. Ниже представлены наиболее существенные ограничения в применении межсетевых экранов:

- неудовлетворительная защита от атак сотрудников компании;
- ограничение в доступе к нужным сервисам;
- ограничение пропускной способности;
- определенное количество остающихся уязвимых мест.

При подключении корпоративной или локальной сети к глобальным сетям при построении политики сетевой безопасности должны решаться следующие задачи:

1) защита локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;

2) скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;

3) разграничение доступа в защищаемую сеть из глобальной и из защищаемой сети в глобальную.

Часть задач по отражению наиболее возможных угроз для внутренних сетей могут решать межсетевые экраны. Использование межсетевых экранов дает возможность организовать внутреннюю политику безопасности сети предприятия, поделив всю сеть на сегменты, и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую.

Список использованных источников:
1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – ИНФРА-М, 2011. – 416 с.
2. Лапонина О. Р. Межсетевое экранирование. — Бином, 2014. — 343 с.
3. Бобов М.Н. Методы использования трансляции адресов в межсетевых экранах. Труды БГУИР N 5, 2009.

АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ В КОРПОРАТИВНОЙ СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Алисеенко М.А.
Цветков В.Ю. – д.т.н., профессор

Сегодня все более популярными становятся видеоконференции с абонентами любой сети, что обеспечивает независимость от городских сетей связи, позволяет повысить эффективность управления компанией, сэкономить время и расходы на командировки. Остро стоит проблема выбора оптимальной системы видеоконференцсвязи, которая обеспечит хорошее качество, надежность и безопасность связи.

Видеоконференцсвязь (ВКС) – это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном времени, с учётом передачи управляющих данных. Для общения в режиме видеоконференции абонент должен иметь терминал ВКС. Для подключения к сети передачи данных используются протоколы IP или ISDN.

Существуют следующие виды систем ВКС:

11) Аппаратные – это системы видеоконференцсвязи, в которых алгоритмы передачи видеосигнала реализуются исключительно на аппаратном уровне с помощью специального оборудования. Это могут быть как видеотелефоны, так и разнообразные групповые ВКС системы, включая системы телеприсутствия. Аппаратная система видеоконференцсвязи базируется на кодеках, средствах отображения видео, средствах воспроизведения и захвата звука, MCU-сервере и дополнительных модулях.

12) Программные – представляют собой программное обеспечение для персональных компьютеров или смартфонов, которые выступают как в роли серверов, так и в роли терминальных устройств видеосвязи. В качестве периферии для захвата и воспроизведения видео и звука могут использоваться, как встроенные в устройство камера, микрофон или динамик, так и внешние устройства [1].

Чтобы выбрать более эффективную систему ВКС, следует прибегнуть к анализу ее входящего и исходящего трафика. Мониторинг и анализ трафика также необходимы для более эффективной диагностики и решения проблем, чтобы не доводить сетевые сервисы до простоя.

Можно выделить следующие методы мониторинга сети:

а) ориентированные на маршрутизаторы;

б) не ориентированные на маршрутизаторы (активные и пассивные);

в) комбинированный метод.

Методы мониторинга, основанные на маршрутизаторе – жёстко заданы (вшиты) в маршрутизаторах и, следовательно, имеют низкую гибкость. SNMP − протокол прикладного уровня, который собирает статистику по трафику до конечного хоста через пассивные датчики, которые реализуются вместе с маршрутизатором. Хотя, SNMP может быть полезным инструментом, но он создаёт возможность для угрозы безопасности, потому что он лишён возможности аутентификации. Расширение RMON включает в себя различные сетевые мониторы и консольные системы для изменения данных, полученных в ходе мониторинга сети и позволяет настраивать сигналы, которые будут мониторить сеть, основанную на определённом критерии. Еще одно расширение – Netflow, которое было представлено в маршрутизаторах Cisco, позволяет собирать IP сетевой трафик, если это задано в интерфейсе. Анализируя данные, которые предоставляются Netflow, сетевой администратор может определить такие вещи как: источник и приёмник трафика, класс сервиса, причины переполненности [2].

Технологии, не встроенные в маршрутизатор всё же ограничены в своих возможностях, они предлагают большую гибкость, чем технологии, встроенные в маршрутизаторы. Эти методы классифицируются как активные и пассивные.

Активный мониторинг сообщает проблемы в сети, собирая измерения между двумя конечными точками. Система активного измерения имеет дело с такими метриками, как: полезность, маршрутизаторы/маршруты, задержка пакетов, повтор пакетов, потери пакетов, неустойчивая синхронизация между прибытием, измерение пропускной способности. Проблема, которая существует с активным мониторингом, – это то, что представленные пробы в сети могут вмешиваться в нормальный трафик.

Пассивный мониторинг не добавляет трафик в сеть и не изменяет трафик, который уже существует в сети. Также в отличии от активного мониторинга, пассивный собирает информацию только об одной точке в сети. Пассивные измерения имеют дело с такой информацией, как: трафик и смесь протоколов, количество битов (битрейт), синхронизация пакетов и время между прибытием. Пассивный мониторинг может быть осуществлён, при помощи любой программы, вытягивающей пакеты. С пассивным мониторингом, измерения могут быть проанализированы только офф-лайн, что создаёт проблему, связанную с обработкой больших наборов данных.

Комбинированные технологии используют лучшие стороны и пассивного, и активного мониторинга сред – это «Просмотр ресурсов на концах сети» (WREN) и «Монитор сети с собственной конфигурацией» (SCNM) [3].

Основными параметрами анализа трафика, для определения эффективности системы ВКС с помощью сетевого анализатора, являются:

– распределение сетевого трафика по ip-адресам и протоколам;

– распределение пропускной способности по ip-адресам и протоколам;

– распределение пиков нагрузки в реальном времени;

– временные параметры узлов.

Сетевой анализатор позволяет выделять из общего потока данных сеансы обмена данными между конечными узлами. Применительно к видеоконференцсвязи возможно выделение конкретного RTP сеанса, для оценки качества и параметров сеанса видеоконференцсвязи. Таким образом, на основе данных о загрузке различных оконечных устройств систем ВКС можно прогнозировать отказ в обслуживании или понижение качества передаваемой мультимедийной информации.

Список использованных источников:

1. Alisha Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques.
2. Амато, В. Основы организации сетей Cisco : учебное издание. В 2 т. / В. Амато. – М. : Вильямс, 2004. – 464 с.
3. M. Uma, G. Padmavathi, An Efficient Network Traffic Monitoring for Wireless Networks.

ДЕКОДИРОВАНИЕ БЛОЧНОГО ТУРБО-КОДА С КОМПОНЕНТНЫМИ РАСШИРЕННЫМИ КОДАМИ ХЭММИНГА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Якубенко П.Н.

Саломатин С.Б. – к.т.н., доцент

На сегодняшний день практически ни одна система связи не обходится без помехоустойчивого кодирования. Необходимость кодирования убедительно показана в широко известной работе К. Шеннона. С момента публикации этой работы было разработано множество различных кодов. Одним из таких кодов является блочный турбо-код (turbo-product code, TPC), в наиболее общем виде предложенный в 1993 году учеными К. Берроу, А. Главье и П. Ситимашимой. Ими было показано, что использование этого кода в канале с шумами позволяет очень сильно приблизиться к границе Шеннона.

Блочный турбо-код оказался полезным для различных каналов связи. Его использование можно обнаружить в самых разных системах, от спутниковой связи до сетей широкополосного доступа. Особенно хорошо использовать блочные турбо коды при высоких требованиях к пропускной способности, задержке, спектральной эффективности и помехоустойчивости.

Как и для большинства помехоустойчивых кодов, самой сложной задачей для применения блочного турбо-кода на практике является эффективное декодирование. Алгоритмы максимального правдоподобия имеют огромную вычислительную сложность, поэтому необходимы алгоритмы, имеющие оптимальное соотношение сложности и эффективности.

Целью данной статьи является представление одного из таких алгоритмов, который позволяет декодировать блочный турбо-код в случае, когда компонентным кодом является расширенный код Хэмминга. Алгоритм разработан для реализации на логической схеме на основе известного более общего алгоритма. Использование предлагаемой модификации позволяет достичь высокой пропускной способности по сравнению с известным алгоритмом. Также уменьшается количество ошибок при относительно высоком отношении сигнал-шум

В общем случае TPC строится следующим образом: выбирается два линейных кода в систематической форме с параметрами (n_1,k_1) и (n_2,k_2) соответственно. Из информационных бит формируется матрица размера $k_2 \times k_1$. Сначала строки этой матрицы кодируются первым кодом, и полученные проверочные биты приписываются к начальной матрице, образуя в итоге матрицу размера $k_2 \times n_1$. Затем все столбцы полученной матрицы кодируются вторым кодом, и в итоге получается матрица размером $n_2 \times n_1$:

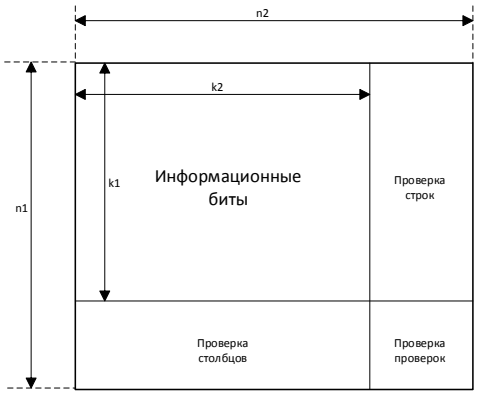


Рисунок 1 – матрица блока турбо-кода

Биты в части «проверка проверок» выражаются через суммы бит подматриц информационной матрицы и не зависят от порядка суммирования. Другими словами, строки с номерами, большими k_1, будут являться кодовыми словами первого кода как и остальные строки.

На вход декодера поступает матрица логарифмических отношений правдоподобия (LLR) размером $n_2 \times n_1$. Будем обозначать ее $\boldsymbol{R}$.

На верхнем уровне алгоритм декодирование разбивается на итерации, каждая из которых состоит из двух полуитераций. Первая полуитерация декодирует строки матрицы SISO алгоритмом, т.е. декодером с мягким входом и мягким выходом, вторая – столбцы. Внутри полуитераций декодирование может происходить последовательно или параллельно. Выходом полуитерации будет являться добавочная информация $\boldsymbol{W}(i-1) = \boldsymbol{R}' - \boldsymbol{R}(i-1)$, где $\boldsymbol{R}'$ – матрица из выходов SISO декодеров. На вход следующей полуитерации поступает матрица $\boldsymbol{R}(\boldsymbol{i})$, полученная по формуле:

$$\boldsymbol{R}(i) = \boldsymbol{R} + \alpha(i)\boldsymbol{W}(i)$$

На каждой полуитерации также генерируется флаг остановки, принимающий значение 1 тогда и только тогда, когда синдромы всех строк (столбцов) на входе равнялись 0. Если флаг остановки принимает значение 1 на двух полуитерациях подряд, это значит, что алгоритм сошелся и дальнейшего изменения бит не будет. В этой ситуации алгоритм прерывается, и выдает жесткое решение для бит информационной части матрицы. Если этого не происходит через некоторое число итераций, принятое максимальным, алгоритм выдает информацию.

Опишем работу SISO декодера для расширенного кода Хэмминга.

На вход декодера подается вектор $\boldsymbol{r}$, являющийся строкой или столбцом матрицы $\boldsymbol{R}(i)$. Генерируем вектор максимального правдоподобия $\boldsymbol{h}$, по принципу $r_i \geq 0 \Rightarrow h_i = 0$; $r_i < 0 \Rightarrow h_i = 1$.

Пользуемся фактом, что последний бит расширенного кода Хэмминга является суммой всех остальных. Находим сумму всех бит $\boldsymbol{h}$ по модулю два, а также синдром обычного (не расширенного) кода Хэмминга для вектора без последнего бита. Тогда $\boldsymbol{h}$ будет являться кодовым словом в том и только в том случае, когда сумма равна 0 и все компоненты синдрома равны 0. Далее выделяем из входной мягкой информации вектор надежности $\boldsymbol{m}$, получаемый взятием модулей компонент. Затем $\boldsymbol{h}$ корректируется так, чтобы синдром был ненулевым, а четность равнялась нулю. Для этого в случае ненулевой четности один бит меняет значение на противоположное, при этом выбирается либо бит с минимальной надежностью, либо второй минимальный в случае, когда изменение бита с наименьшей надежностью приводит к получению кодового слова. В случае когда $\boldsymbol{h}$ изначально является кодовым словом, два бита с минимальной надежностью изменяют значения на противоположные. Вместе с изменением битов в $\boldsymbol{h}$ изменяется также и $\boldsymbol{m}$: на тех позициях, где поменялся бит, надежность изменяется на отрицательную. Также модифицируется синдром, чтобы он соответствовал новому значению $\boldsymbol{h}$.

После модификации $\boldsymbol{h}$ и $\boldsymbol{m}$ список кандидатов формируется следующим образом. На сфере с центром в точке $\boldsymbol{h}$ и радиусом 2 (в метрике Хэмминга) выбираются все кодовые слова. Для этого все биты разбиваются на пары так, чтобы изменение двух бит в любой паре приводило к получению кодового слова. Чтобы получить пару для бита на некоторой позиции, нужно взять соответствующий столбец проверочной матрицы, вычесть из него синдром, и найти номер столбца проверочной матрицы, в которой стоит полученный вектор.

По итогу такого разбиения получаем список из $n/2$ кодовых слов. Аналогично с оригинальным алгоритмом [1], выбираем решение $\boldsymbol{d}$ по критерию минимальности нормы Евклида. При этом сами нормы можно не вычислять, если воспользоваться следующим преобразованием (полученным с учетом, что векторы $\boldsymbol{d}$ и $\boldsymbol{c}$ состоят из 1 и -1):

$$\frac{||\boldsymbol{c}-\boldsymbol{r}||^2 - ||\boldsymbol{d}-\boldsymbol{r}||^2}{4} = \sum_{c_j \neq d_j} d_j r_j = \sum_{c_j \neq d_j} d_j h_j m_j = \sum_{\substack{c_j \neq d_j \\ d_j = h_j}} m_j - \sum_{\substack{c_i \neq d_i \\ d_i \neq h_i}} m_i \qquad (1)$$

В нашем случае последнее выражение имеет простой смысл и легко вычисляется. Векторы $\boldsymbol{d}$ и $\boldsymbol{c}$ различаются в четырех компонентах, так как оба получены из вектора $\boldsymbol{h}$ изменением некоторой пары. При этом в первую сумму войдут те компоненты, которые менялись для получения вектора $\boldsymbol{c}$, а во вторую те, которые менялись для получения вектора $\boldsymbol{d}$. Значит, для нахождения вектора с минимальной нормой достаточно вычислить суммы в каждой паре и найти минимальную. Каждый бит входит в какую-то из пар, значит оценка надежности каждого бита может быть произведена по формуле (1). В случае, когда бит соответствует решению, вычитается минимальная сумма из второй минимальной.

Ниже приведены графики, которые получены в моделях с количеством итераций декодирования равно 8.

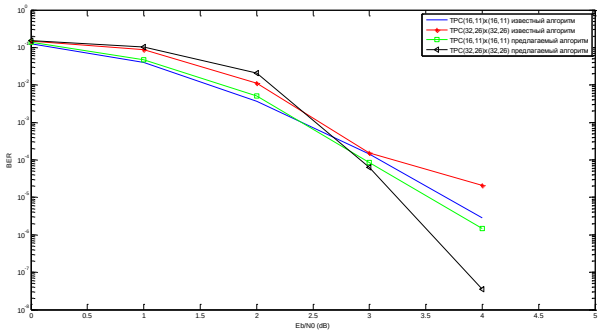


Рисунок 2 – сравнение BER оригинального и модифицированного алгоритмов.

Таблица 1 – сравнение сложности алгоритмов по количеству операций.

	Произведений	Сумм	Сравнений
Известный (16,11)	256	512	320
Предлагаемый (16,11)	0	160	280
Известный (32,26)	512	1040	700
Предлагаемый (32,26)	0	320	600

Список использованных источников:

1. R.Pyndiah, A.Glaviex, A.Picart, S.Jacq, ”Near Optimum Decoding of Product codes”, IEEE Globecom’94
2. C.Berrow, A.Glavieux, P.Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo-codes (1)”, IEEE Int. Conf. on Comm. ICC’93.

СЕТЬ UMTS 900 РАЙОННОГО МАСШТАБА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лагутик В.В.

Саломатин С.Б. – к.т.н.,доцент

Современные технологии уже давно стали неотъемлемой составляющей нашей жизни. Сегодня трудно представить современного человека без смартфона. Использование ноутбуков, планшетов, мобильных телефонов с возможностью выхода в Интернет для общения, работы, развлечений стало незаменимым и даже обыденным. Число интернет-пользователей возрастает в геометрической прогрессии на протяжении последних лет и эта тенденция, вероятно, продолжится в ближайшие годы. Появляется необходимость предоставления доступа к мобильному интернету абонентам, которые проживают за пределами крупных городов, в сельской местности. Поэтому крупнейшие операторские компании активно продолжают строительство региональных сетей сотовой связи.

UMTS (Universal Mobile Telecommunication System) — технология сотовой связи, разработанная Европейским институтом стандар-тов телекоммуникаций (ETSI). Сотовые сети, использующие данную технологию, относят к сетям третьего поколения (сетям 3G). К основным отличиям сетей UMTS от сетей GSM относят использование широкополосных сигналов, и внедрение широкополосной технологии множественного доступа с кодовым разделением каналов (W-CDMA). [1]

Сеть 3G UMTS-900 имеет множество преимуществ. В частности, низкий сигнал лучше проходит сквозь стены, зона покрытия намного шире, а это дает возможность развивать сеть в малозаселенных сельских районах.

Европейские сотовые компании смогли добиться, внедрив UMTS 900, следующих результатов:

– нарастили покрытие сети. Она появилась или заметно улучшилась в малонаселенных районах;

– существенно снизили операционные и капитальные затраты на 50 – 70% в зависимости от региона;

– получили возможность использования уже имеющихся площадок для нужд новых технологий;

– ускорили запуск сети, оптимизировали сайты, благодаря чему обслуживание абонентов стало еще качественнее;

– сделали голосовые услуги качественнее;

– значительно улучшили качество покрытия в закрытых помещениях, это стало возможно, так как частота 900 МГц намного ниже 2100 МГц, а значит, лучше проходит сквозь стены;

– смогли расширить перечень предлагаемых услуг. [2]

Смоделированная в Mentum Planet карта 3G радиопокрытия Молодечненского района для сетей UMTS 900 и UMTS 2100 представлена на рисунке 1.

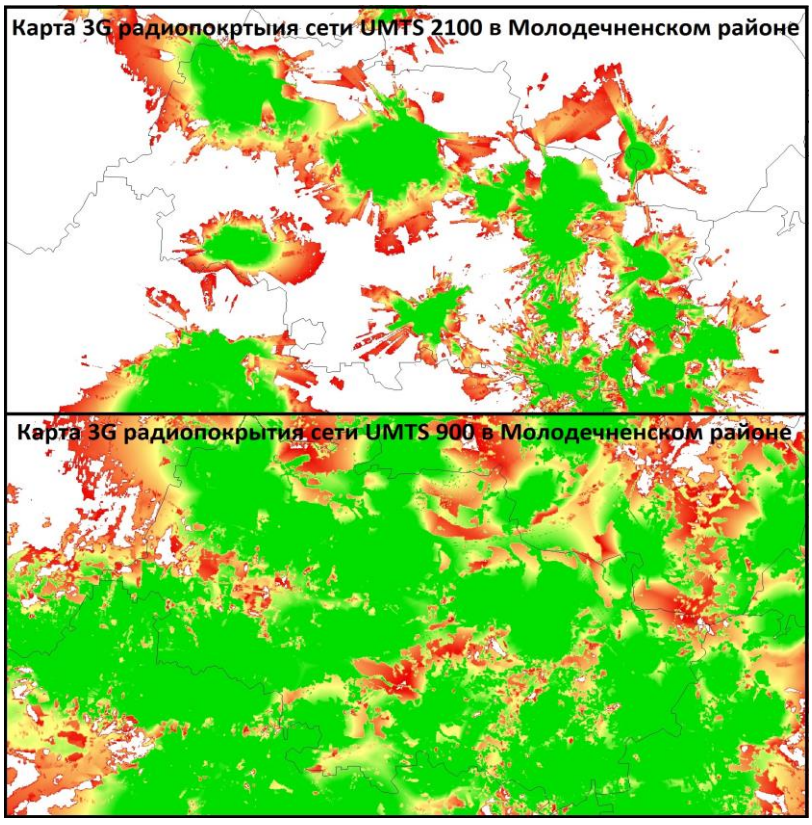


Рисунок 1 – Карта 3G радоипокрытия в Молодечненском районе для сетей UMTS 2100 и UMTS 900

Уровни сигнала окрашены на карте согласно Государственному стандарту Республики Беларусь СТБ 1904-2011.

Уровень полезного сигнала для сетей стандарта UMTS:

а) ≥–88 дБм: связь может быть установлена внутри помещений, внутри автомобиля и на открытых участках местности вне автомобиля (зеленый цвет на цифровой карте местности);

б) ≥–93 дБм: связь может быть установлена внутри автомобиля и на открытых участках местности вне автомобиля (желтый цвет на цифровой карте местности);

в) ≥–103 дБм: связь может быть установлена на открытых участках местности вне автомобиля (красный на цифровой карте местности);

г) <–103 дБм: связь отсутствует (белый цвет на цифровой карте местности).

По результатам моделирования зоны радиопокрытия технология UMTS 900 сможет обеспечить связью 99% площади Молодечненского, тогда как UMTS 2100 обеспечит покрытие всего 54% площади района. Для подтверждения результатов моделирования зон радиопокрытия произведен драйв-тест для технологий UMTS 900 и UMTS 2100 в Молодечненском районе на трассе Р28 от М14 до г. Молодечно. Результаты драйв-теста приведены на рисунке 2.

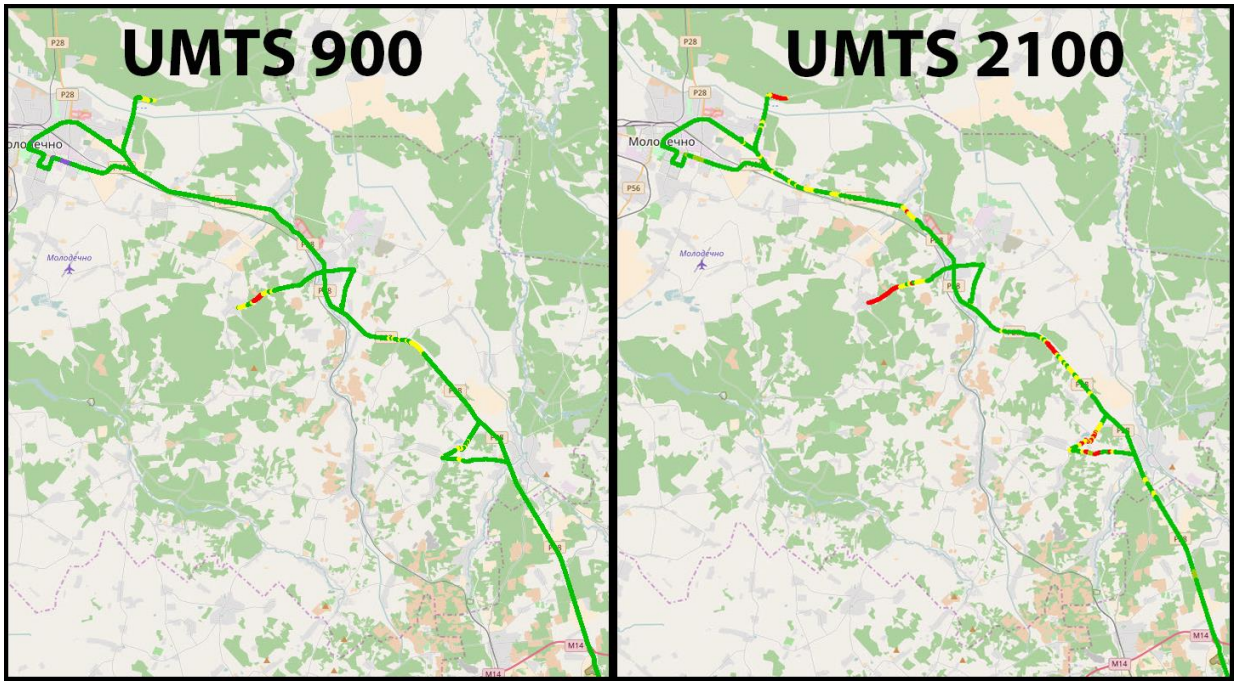


Рисунок 2 – Результаты драйв-теста в Молодечненском районе для сетей UMTS 2100 и UMTS 900

По результатам проведения драйв-теста в Молодечненском районе по трассе Р28 от М14 до города Молодечно видно, что рассчитанное в Mentum Planet радиопокрытие сетей UMTS 2100 и UMTS 900 совпадает с экспериментальными данными, из чего можно сделать вывод, что на остальной территории Молодечненского района зона радиопокрытия сети будет совпадать с расчетной. Также на территории, где и расчетно, и физически есть радиопокрытие сетей UMTS 900 и UMTS 2100, уровень сигнала при котором связь может быть установлена внутри помещений, внутри автомобиля и на открытых участках местности у сети UMTS 900 составляет 90.94%, а у сети UMTS 2100 – 82.76%, участков сети где связь отсутствует у сети UMTS 900 составляет 0.44%, когда как у сети UMTS 2100 – 6.16%.

Из моделирования карт 3G радиопокрытия сетей UMTS 900 и UMTS 2100, а также проведения драйв- теста в Молодечненском районе было доказано, что использование низкочастотного 900 МГц диапазона в сетях третьего поколения позволит, при уменьшенных собственных издержках, расширить зону уверенного приема 3G-сигнала как в малозаселенной, сельской местности, так и в крупных городах Беларуси. За счет большего радиуса действия и более высокой проникающей способности, базовые станций связи UMTS-900 более эффективны, нежели станции, функционирующие в диапазоне частот 2100 МГц. Внедрение технологии UMTS-900 в 3G-сетях предполагает улучшение качества голосовой связи и увеличение скорости мобильного интернета для большинства абонентов сотовой связи страны. [3]

Список использованных источников:

1. Попов, Е. А. Сотовые сети мобильной связи стандарта UMTS : учеб. пособие / Е. А. Попов, А. Л. Гельгор – СПб.: Политехн. ун-т, 2011. – 10 с.

2. Отличие 3G 2100МГц от 3G 900МГц [Электронный ресурс]. – Режим доступа : https://www.r2c-pro.ru/info/printsipialnye_otlichiya_3g_2100_mgts_i_3g_900_mgts/#gallery

3. Технология UMTS-900 в 3G-сетях Беларуси [Электронный ресурс]. – Режим доступа : http://моби.бел/2015/12/mts-velcom-life-umts-900-3g/

ВИДЕОНАБЛЮДЕНИЕ В МОБИЛЬНОМ ОБЪЕКТЕ С ТЕХНОЛОГИЕЙ WI-FI

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Высоцкая В.В.

Саломатин С.Б. – к.т.н., доцент

В настоящее время потребность в безопасности и контроле очень высока, т.к. современный мир ставит нас в условия быстро развивающихся технологий и криминогенной обстановки, которая во многом определяет желание большинства людей оградить себя от внешнего мира, построить вокруг себя надежную стену, чтобы устранить угрозы и риски на длительную перспективу, обезопасить себя и своих близких в общественных местах, контролировать работу персонала и различных систем.

Вышеуказанные действия было бы невозможно совершить без различных комплексов технических средств. В этом случае и становиться актуальным широкое использование возможностей инновационных технологий в области видеонаблюдения. Процесс видеонаблюдения осуществляется с помощью систем видеонаблюдения, которые представляют собой программно-аппаратный комплекс. Основными компонентами системы видеонаблюдения являются: видеорегистратор; камеры наблюдения; источники питания для систем видеонаблюдения; кожухи и кронштейны; мониторы; кабель; устройства защиты от природных явлений. Использование систем видеонаблюдения безгранично: фиксирование противозаконных действий в различных общественных и жилых местах, контроль за рабочим персоналом, обеспечение общей безопасности, применение в образовательных целях, высотное телевидение.

Целью данной статьи является обзор сетевой системы видеонаблюдения в мобильном объекте с технологией Wi-Fi. Мобильным объектов является военный автотранспорт, в котором нужно осуществить контроль за тремя рабочими местами и стойкой связи. Главным условие в том, что данный автотранспорт осуществляет движения на специально отведенной местности, радиусом в 2,5 км.

Система видеонаблюдения – это программно-аппаратный комплекс (видеокамеры, объективы, мониторы, регистраторы и др. оборудование), предназначенный для организации видеоконтроля на локальных, мобильных и территориально-распределённых объектах. Целью системы видеонаблюдения является получение, обработка, передача, регистрация и хранение телевизионных изображений из зоны наблюдения.

Структурная схема системы видеонаблюдения приведена на рисунке 1:

Рисунок 1 – Структурная схема системы видеонаблюдения

Как видно из структурной схемы данная система видеонаблюдения состоит из:

– четырех видеокамер с встроенным Wi-Fi модулем;
– беспроводной точки доступа;
– маршрутизатора;
– рабочего места оператора.

Беспроводная точка доступа представляет непосредственно саму точку доступа и PoE-инжектор. Технология Poe (Power of Ethernet) – технология, позволяющая передавать удаленному устройству вместе с данными электрическую энергию через стандартную витую пару в сети Ethernet, используется для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых коммутаторов и других устройств, к которым нежелательно или невозможно проложить отдельный электрический кабель. Если устройство не поддерживает данную технологию, то используются PoE-инжекторы. PoE-инжектор – это устройство предназначено, для «подмешивания» питания в существующую линию передачи Ethernet[1]. Беспроводная точка доступа WAP-800имеет выходную мощность 400 мВт, поддерживает 802.11a/b/g стандарты передачи данных, работает в диапазоне частот 2.40–2.48 ГГц, 5.15–5.35 ГГц, 5.47–5.85 ГГц, канальная скорость передачи данных достигает 108 Мбит/с, подключение точка-точка или точка-многоточка на расстоянии до десятков километров.

Видеокамера WIPH-SAD60 имеет Wi-Fi модуль стандарта 802.11g, следовательно полная совместимость с вышеуказанной беспроводной точкой доступа. Разрешение: 3.0 Мп. Формат сжатия видео: H.265.

H.265 или HEVC (High Efficiency Video Coding – высокоэффективное кодирование видеоизображений) – формат видеосжатия с применением более эффективных алгоритмов по сравнению с H.264/MPEG-4 AVC. Он был разработан таким образом, чтобы, используя новые технологии сжатия и более умную модель кодирования/декодирования, наиболее экономно использовать пропускные ресурсы канала.

Эффективность кодирования формата H.265 в сравнении с H.264 показана на рисунке 2[2].

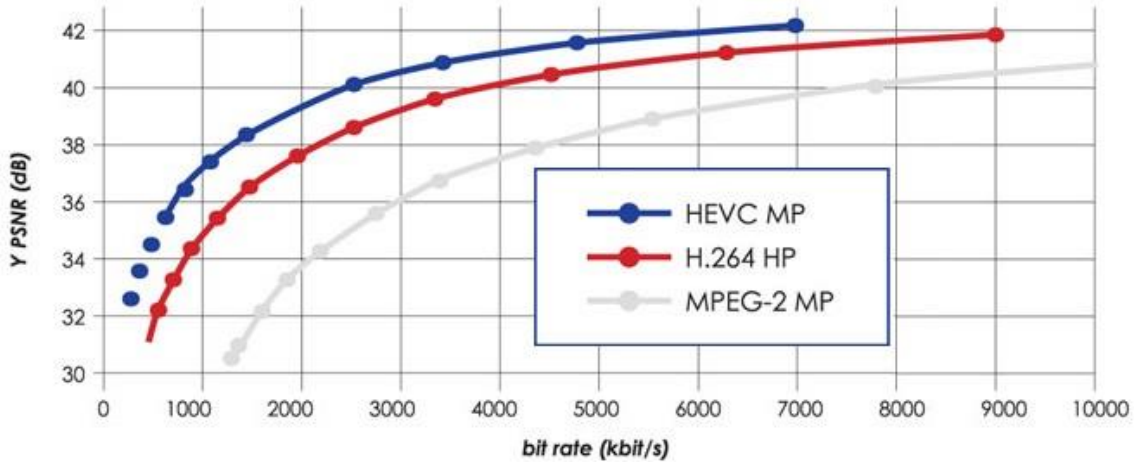


Рисунок 2 – Эффективность кодирования форматов сжатия видео

Сравнение по размеру файлов представлено на рисунке 3. При этом следует учесть, что речь шла исключительно о видео – звук не кодировался ни в одном из случаев. Размеры кодирования определялись настройками квантователя, где более низкие q-показатели соответствовали более высокому качеству (и большему размеру файлов). Базовый кодированный файл состоит из 500 кадров, его размер – 1,5 Гб, YUV 4:2:0, частота кадров – 50 в секунду. Для сравнения использовался элементарный размер потокового файла, потому что он отображает то, что передаётся на декодер для создания изображения на выходе[2].

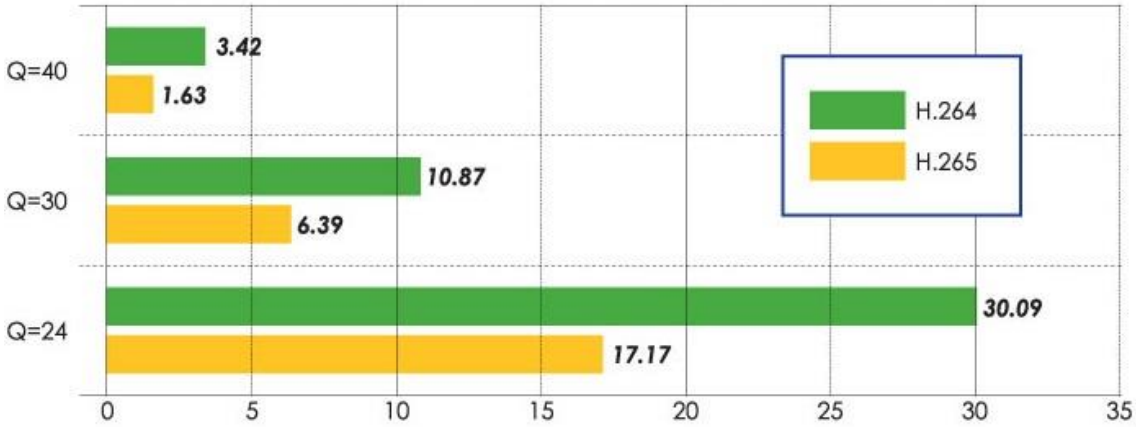


Рисунок 3 – Размеры файлов, сжатых с помощью H.264 и H.265

Из рисунка 2 видно, что при одинаковом уровне соотношения сигнал/шум для H.265 имеется снижение битрейта на 25–30% по сравнению с H.264. На рисунке 3 показано что объем файлов при использовании H.265 значительно ниже, чем при использовании H.264.

Таким образом, система видеонаблюдения в мобильном объекте основана на сети беспроводного доступа IEEE 802.11g, со скоростью передачи до 108 Мбит/с и дальность действия до десятков километров. Видеокамеры используют формата сжатия видео H.265, что позволяет улучшить качество принимаемого изображения, увеличить расстояние передачи видеоинформации с видеокамер до точки доступа, а так же не понизить заданную скорость передачи данных.

Список использованных источников:

3. Manikata Sanjaya, Power Over Ethernet Interoperability Guide.
4. Кодек H.265 [Электроннвй ресурс]. – Режим доступа: http://www.security-bridge.com/.

СИСИТЕМА ЦЕНТРАЛИЗОВАННОЙ КАРТОТЕКИ АБОНЕНТОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Настин А.А., Степанов Н.В.
Макейчик Е.Г. – ст. преподаватель

В настоящее время, в связи с повсеместной интеграцией информационных систем в работу предприятий различных направленностей и усложнением процесса принятия решений, скорость обработки информации напрямую зависит от того, как быстро и слаженно взаимодействуют его структуры.

В целях обеспечения взаимодействия между внутренними системами компании РУП «Белтелеком» было принято решение создать систему, которая отвечала бы всем требованиям компании и позволяла бы в одном месте хранить всю важную информацию об абонентах Республики Беларусь.

Централизованная система картотеки абонентов (ЦСКА) – это система, которую могут использовать все автоматизированные информационные системы предприятия РУП «Белтелеком».

ЦСКА включает в себя решение следующих технологических и технических заданий:

- организация единой картотеки абонентов предприятия;
- организация синхронизации карточки абонента между системой ЦСКА и другими АИС РУП «Белтелеком»;
- организация службы администратора ЦСКА;
- организация технического обеспечения и обслуживания сервера и ПО системы ЦСКА.

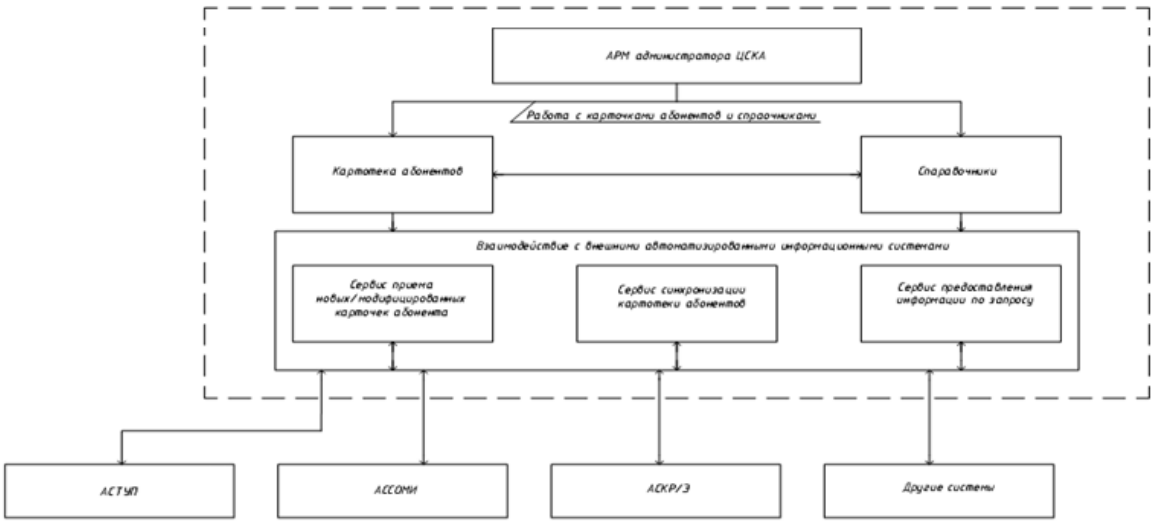


Рис. 1 – Структурная схема системы централизованной картотеки абонентов

Основные функции ЦСКА:

4) Прием и хранение новых или модифицированных карточек абонентов, созданных автоматизированными системами предприятия.

5) Автоматическое присвоение значения реквизита «Код абонента» для новых карточек абонентов.

6) Выдача информации о существующих абонентах по запросу автоматизированных систем предприятия.

7) Организация синхронизации картотеки абонентов.

8) Модификация существующих карточек абонентов посредством интерфейса администратора ЦСКА.

9) Снижение нагрузки на существующие автоматизированные информационные системы ЦСКА.

Список использованных источников:

4. Блинов, И.Н. Java. Методы программирования / И.Н. Блинов, В.С. Романчик. – Минск: Четыре четверти, 2013. – 896 с.

5. Хорстманн, Кей С. Java. Библиотека профессионала. Основы / Кей С. Хорстманн, Г. Корнелл. – М: Вильямс, 2014. – 864 с.

6. Фримен, Эр. Паттерны проектирования / Эл. Фримен, Б. Бейтс, К. Сьерра. – СПб: Питер, 2014. – 656 с.

МОДУЛЬНАЯ СИСТЕМА ТРАБЛШУТИНГА СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станевич М.А.
Макейчик Е.Г. – м.т.н.,старший преподаватель

На сегодняшний день практически все крупные компании сталкиваются с необходимостью контролировать инфраструктуру, обеспечивающую экономическую эффективность бизнеса.

Операторам отдела сервисного и операционного контроля необходима система для быстрого выявления и локализации аварий на сети, способная взаимодействовать с разными топологиями и типами сетей.

Решением стало начало постепенного наращивания функциональности утилит, добавления возможности корреляции, выявления и обогащения информации, анализа статистических данных: вплоть до выявления неизвестных проблем, возможности автономного траблшутинга и выяснения степени влияния ИТ-метрик на бизнес-метрики.

OSS (Operation Support System) – модульная система мониторинга, основанная на концепции управления системами связи (Telecommunication Management Networks – TMN).

По специализации системы управления и мониторинга можно разделить на три вида:

– низкоуровневые;

– зонтичные;

– унитарные.

Низкоуровневые системы предназначены обычно для управления оборудованием конкретного производителя или оборудованием определенного класса, например: оборудованием первичных сетей, телефонными станциями, оборудованием вторичных сетей и пр. Специализированные системы управления для своего оборудования производят такие компании как Ciena, Cisco, Keymile и другие.

Зонтичные системы Manager Of Managers, Orchestrators собирают данные от низкоуровневых систем, которые, в свою очередь, выполняют задачи управления и мониторинга отдельных частей инфраструктуры. По сути низкоуровневые системы становятся информационными агентами для зонтичной системы. Зонтичная система производит анализ всей поступающей информации с целью корреляции событий, траблшутинга, аварий, поиска первопричин сбоев, прогнозирования наступления нештатных ситуаций и т.д. Сетевые и системные администраторы в этом случае получают единую точку контроля состояния инфраструктуры и бизнес приложений, единую точку генерации отчетности. Ограничением для зонтичных систем зачастую становится невозможность управления элементами ИТ инфраструктуры, поскольку далеко не все низкоуровневые системы способны принимать к исполнению команды от вышестоящего программного обеспечения.[2]

Траблшутинг (англ. troubleshooting – устранение неполадок, работа над траблом) – форма решения проблем, часто применяемая к ремонту не работающих устройств или процессов. Представляет собой систематический, опосредованный определённой логикой поиск источника проблемы с целью её решения. Траблшутинг как поиск и устранение неисправностей необходим для поддержания и развития сложных систем (встречающихся, например, в таких областях, как связь, инженерия, системное администрирование, электроника, ремонт автомобилей, диагностическая медицина и организация бизнес процессов), где проблема может иметь множество различных причин.

В основные возможности зонтичного решения мониторинга сети входят:

1 Мониторинг опциональной сигнализации оборудования.[1]

2 Инвентаризацию сетевого и серверного оборудования.

3 Определение или расчет KPI (Key Performance Indicators): формулы для определения и анализа «эффективности» того или иного параметра сети.

4 Конфигурирование оборудования

5 Выдача рекомендаций по устранению неисправностей

Основной недостаток Зонтичных систем – стоимость такого решения. Высокая цена обусловлена несколькими недостатками:

1 Кастомизация решения. Как правило продукт из коробки не может быть интегрирован в большую инфраструктуру компании без дополнительной настройки. Некоторые сегменты сети не имеют базы данных с информацией о составе и количестве элементов в нем. В таких случаях ввод данных в систему мониторинга производится вручную. А при изменении структуры сети или адреса сетевого элемента, изменение информации так же будет производиться вручную

2 Статичность интеграции. Все системы, которые интегрируются в OSS, как правило со временем модернизируются, меняются вендоры, соответственно, и ПО. Поэтому будет изменяться тип коммуникации серверов с системой мониторинга, тип базы данных, для его считывания.

Список использованных источников:

1. АДВ [Электронный ресурс]. – Режим доступа : http://www.advc.ru/solutions/sistemi_upravlenija_i_monitoringa.html

2. NetCracker Technology® [Электронный ресурс] : Datasheet / NetCracker Technology. – Режим доступа : NetCracker Velcom CRIM project SOW.pdf.

ТЕХНОЛОГИЯ LORA

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сабко А.Н., Грудковский Н.А

Лагутин А.Е. – к.т.н.,доцент

Технология LoRa появилась на свет под эгидой некоммерческой организации LoRa Alliance, основанной такими компаниями, как IBM, Semtech, Cisco и др., с целью принятия и продвижения протокола LoRaWAN в качестве единого стандарта для глобальных сетей с низким энергопотреблением (LPWAN — от англ. Low Power Wide Area Network).

Собственно, аббревиатура LoRa объединяет в себе метод модуляции LoRa в беспроводных сетях LPWAN, разработанный Semtech, и открытый протокол LoRaWAN.

Разработчики LoRa Alliance позиционируют LoRa как технологию, имеющую значительные преимущества перед сотовыми сетями и WiFi благодаря возможности развертывания межмашинных (M2M) коммуникаций на расстояниях до 20 км. и скоростях до 50 Кбит/с., при минимальном потреблении электроэнергии, обеспечивающем несколько лет автономной работы на одном аккумуляторе типа AA.

LoRa позволяет демодулировать сигналы на уровне 20dB ниже уровня шумов, тогда как большинство систем с частотной манипуляцией (frequency shift keying, FSK) могут корректно работать с сигналами на уровне не ниже 8-10dB над уровнем шумов. Модуляция LoRa определяет физический уровень (physical layer, PHY, OSI level 1), который может использоваться в сетях с различной архитектурой – mesh-сети, звезда, точка-точка и другие.

Благодаря своей высокой чувствительности (-148dbm) LoRa идеально подходит к устройствам с требованиями низкого потребление электроэнергии и высокой устойчивости связи на больших расстояниях.

Диапазон применений данной технологии огромен: от домашней автоматизации и интернета вещей (Internet of Things, IoT) до промышленности и умных городов.

Архитектура LoRaWAN сетей.

Рассмотрим архитектуру LoRaWAN сетей. Типичная сеть LoRaWAN состоит из следующих элементов: конечные узлы, шлюзы, сетевой сервер и сервер приложений. Конечный узел (End Node) предназначен для осуществления управляющих или измерительных функций. Он содержит набор необходимых датчиков и управляющих элементов. Шлюз LoRa (Gateway/Concentrator) — устройство, принимающее данные от конечных устройств с помощью радиоканала и передающее их в транзитную сеть. В качестве такой сети могут выступать Ethernet, WiFi, сотовые сети и любые другие телекоммуникационные каналы. Шлюз и конечные устройства образуют сетевую топологию типа звезда. Обычно данное устройство содержит многоканальные приёмопередатчики для обработки сигналов в нескольких каналах одновременно или даже, нескольких сигналов в одном канале. Соответственно, несколько таких устройств обеспечивает зону покрытия сети и прозрачную двунаправленную передачу данных между конечными узлами и сервером. Сетевой сервер (Network Server) предназначен для управления сетью: заданием расписания, адаптацией скорости, хранением и обработкой принимаемых данных. Сервер приложений (Application Server) может удаленно контролировать работу конечных узлов и собирать необходимые данные с них.

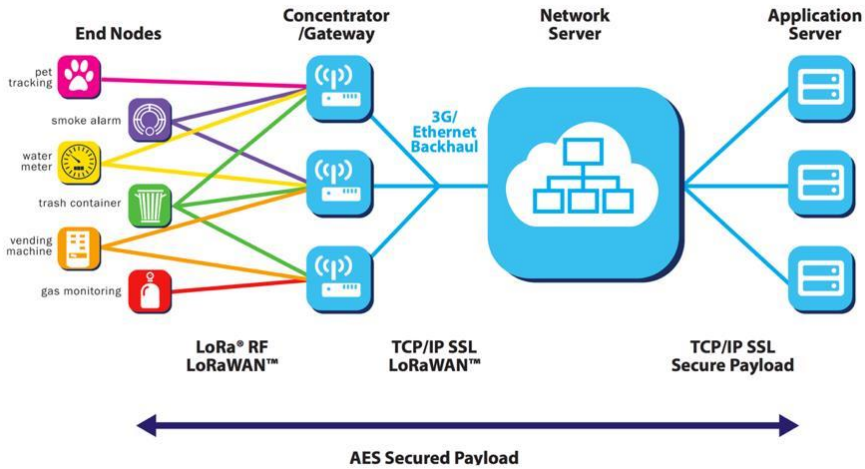


Рис. 1 - Архитектура LoRaWAN сети.

В конечном итоге, LoRaWAN сеть имеет топологию звезда из звёзд, имеет конечные узлы, которые через шлюзы, образующие прозрачные мосты, общаются с центральным сервером сети. При таком подходе обычно предполагается, что шлюзами и центральным сервером владеет оператор сети, а конечными узлами – абоненты. Абоненты имеют возможность прозрачной двунаправленной и

защищенной передачи данных до конечных узлов.

Т.к. LoRaWAN образуют глобальную сеть, то разработчики уделили особое внимание безопасности и конфиденциальности передаваемых данных, которые обеспечиваются шифрованием AES на нескольких уровнях:

1) На сетевом уровне с использованием уникального ключа сети (Unique Network key, EUI64).

2) Сквозную безопасность на уровне приложений с помощью уникального ключа приложения (Unique Application key, EUI64).

3) И специального ключа устройства (Device specific key, EUI128).

Для решения различных задач и применений в сети LoRaWAN предусмотрено три класса устройств:

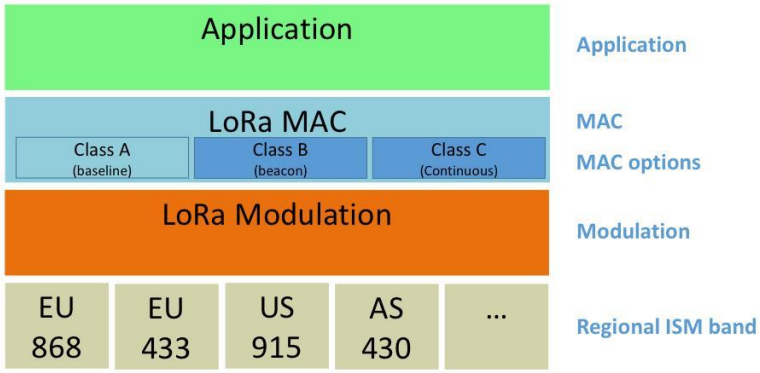


Рис. 2 - Классы устройств в сетях LoRaWAN.

А) Двунаправленные конечные устройства «класса А» (Bi-directional end-devices, Class A). Устройства этого класса применяются, когда необходима минимальная потребляемая мощность при преобладании передачи данных к серверу. В качестве инициатора сеанса связи выступает конечный узел, отправляя пакет с необходимыми данными, а затем выделяет два окна, в течении которых ждёт данных от сервера. Таким образом, передача данных от сервера возможна только после выхода на связь конечного устройства.

Б) Двунаправленные конечные устройства «класса Б» (Bi-directional end-devices, Class B). Основное отличие от устройств «класса А» заключается в выделении дополнительного окна приёма, которое устройство открывает по расписанию. Для составления расписания конечное устройство осуществляет синхронизацию по специальному сигналу от шлюза. Благодаря этому дополнительному окну сервер имеет возможность начать передачу данных в заранее известное время.

В) Двунаправленные конечные устройства «класса С» с максимальным приемным окном (Bi-directional end-devices, Class C). Устройства этого класса имеют почти непрерывное окно приёма данных и закрывает его лишь на время передачи данных, что позволяет их применять для решения задач, требующих получения большого объёма данных.

Итого, LoRaWAN позволяет строить глобальные распределённые беспроводные сети с большим числом конечных узлов. По заявлениям Semtech, один LoRa-шлюз допускает обслуживание до пяти тысяч конечных устройств, что достигается за счёт:

1. Топологии сети.
2. Адаптивной скорости передачи данных и адаптивной выходной мощности устройств, задаваемых сетевым сервером.
3. Временным разделением доступа к среде.
4. Частотным разделением каналов.
5. Особенностью LoRa-модуляции, позволяющей в одном частотном канале одновременно демодулировать сигналы, передаваемые на разных скоростях.

Список использованных источников:

1. http://www.zurich.ibm.com/pdf/lrsc/lmic-release-v1.5.zip

2. https://github.com/Lora-net/LoRaMac-node

3. Верхулевский К. Однокристальные ISM-трансиверы Semtech: уверенная связь в сложных условиях. // Компоненты и технологии. – 2013. – №6. – с. 110-116.

4. SX1272/3/6/7/8: LoRa modem design guide. // Application note 1200.13, rev.1, July 2013. // semtech.com.

5. Wireless RF Solutions. // Selector Guide. 2014. // www.semtech.com

АТАКИ НА ПАССИВНЫЕ ОПТИЧЕСКИЕ СЕТИ И МЕТОД ЗАЩИТЫ ОТ АТАК ПУТЁМ ПРИМЕНЕНИЯ СХЕМЫ WDM-PON

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сергеев Н.Н., Мелешко А.С.

Урядов В.Н. – к.т.н.,доцент

Переход от электронных технологий к фотонным несет не только существенные преимущества, но и новые проблемы для информационной безопасности. Появляются новые возможные угрозы. Сегодня можно получить доступ к информации, передающейся по пассивной оптической сети, а зафиксировать эту утечку практически невозможно. Поэтому проблема повышения живучести сетей доступа, построенных на основе технологии PON, стремительно возрастает. [1].

Основной особенностью всех PON сетей является то, что нисходящий поток достигает все оптические сетевые терминалы (ONT), подключенные к сети. Нисходящий поток (downstream) от центрального узла к абонентам идет на длине волны 1490 нм и 1550 нм для видео. Восходящие потоки (upstream) от абонентов идут на длине волны 1310 нм с использованием протокола множественного доступа с временным разделением TDMA. Следовательно, каждому абоненту, приходят пакеты информации адресованы всем абонентам, а он используя множественный доступ с временным разделением выбирает необходимый ему пакет. [2].

Используя оптическую розетку, а доступ к ней получить весьма легко, злоумышленник может вывести из строя весь сегмент сети, путём примитивного засвета лазером в линию. Это произойдёт в том случае, когда мощность излучаемого в линию сигнала превысит допустимую мощность фотодиода OLT. [3].

Злоумышленник после некоторых манипуляций с перепрограммированием ONT или подключением ПК с установленным специальным программным обеспечением к ONT может получать информацию, адресованную другим пользователям, всего лишь подобрав необходимый интервал. Это можно сделать с каждой оптической розетки (ОРА).

Эффективным методом защиты от такого рода атак является спектральное уплотнение каналов (wavelength division multiplexing). WDM-PON предлагает альтернативу схеме передачи, основанной на разделении во времени, как в GPON, схемой, где каждый ONT передает и принимает данные на определенной длине волны. Типичная архитектура WDM-PON будет заменять пассивные сплиттеры на волновые селективные фильтры, которые часто реализованы как решетка на основе массива волноводов (Arrayed Waveguide Grating - AWG). [4].

Принцип реализации WDM-PON представлен на рисунке 1:

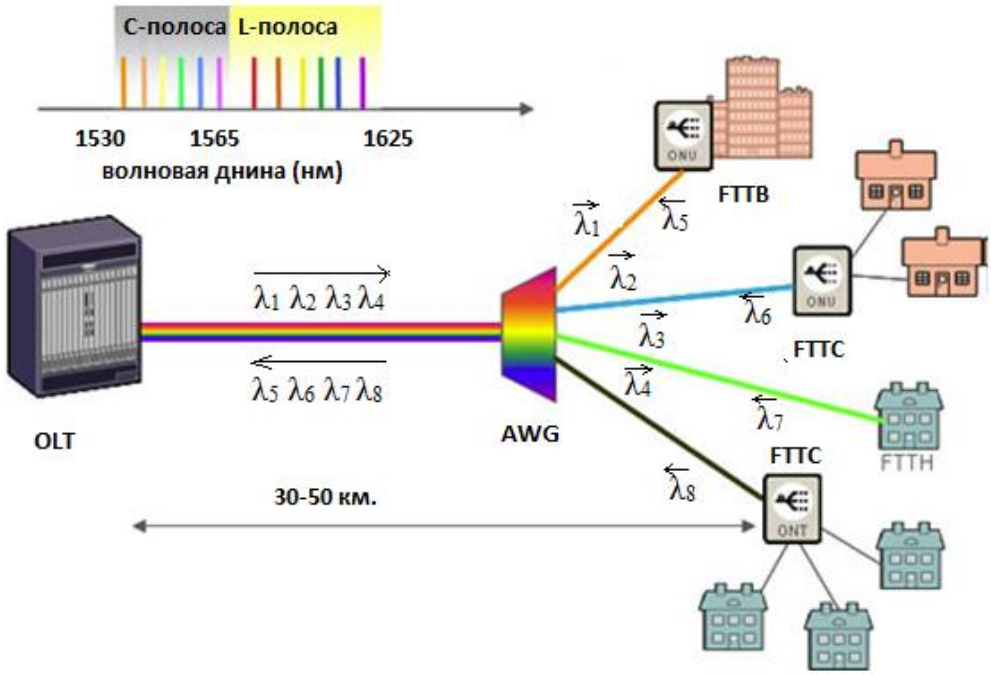


Рис.1. PON с разделением абонентов по длине волны

Архитектура WDM-PON идентична архитектуре FTTH у EPON и GPON. Удаленный узел (RN – Remote Node) в WDM-PON может быть выполнен либо с помощью оптического кросса или пассивного маршрутизатора длин волн. Оптически кросс распределяет все входящие сигналы на все выходные порты и, для этого используется фильтр длин волн у каждого ONU. Несмотря на то, что оптический кросс простой прибор, недорогой и распределенной структуры, данное исполнение требует оптические фильтры

с различными центральными длинами волны в каждом ONU. Кроме того, возрастают потери в оптическом кроссе, относительно длинны волны маршрутизатора.

Вместо оптического кросса на удаленном узле, можно использовать маршрутизатор с канальной решеткой, которая отделяет длины волн и направляет их на ONT.

Длины волн полностью отделены в нисходящем направлении для каждого пользователя. Это дает гораздо больше емкости для каждого пользователя, большую надежность и лучший контроль работы потому, что нет помех между различными длинами волн в исходящем направлении. [3].

В восходящем направлении при системе WDM-PON, каналы длин волн направляются от ONT к OLT, с помощью маршрутизатора и решетки волновода, AWG, которая размещается в удаленный узел RN , где находятся и оптические пассивные кроссы, которые используются в системе GPON. Каждому абоненту выделяется две длинны волны: одна для приёма, а другая для передачи. [4].

AWG (решетка волновода) - это пассивный оптический прибор, с особенной характеристикой циклической периодичности, которая позволяет использовать AWG, одновременно в роли мультиплексора и демультиплексора. Решетка AWG направляет каждую отдельную длину волны к одному выходному порту, отделяя, несколько длин волн одновременно. Вносимые потери в AWG около 4-5 дБ (независимо от количества каналов), и это гораздо меньше, чем у оптических кроссов. Однако, не смотря на это хорошее свойство прибора AWG, в результате изменения температуры, происходит сдвиг центральной длины волны из 0,01 nm/° C , что предотвращает использовать AWG в RN, потому, что RN в области больших температурных изменений, где предельные значения могут колебаться с -40°C под + 85°C. Такая температурная зависимость имеет причины в индексе изменения кремниевого волновода, что приводит к изменению в оптических длин. На рынке недавно, появились холодные маршрутизаторы AWG, которые разработаны с термической компенсацией, и у которых применяются материалы с температурным коэффициентом, отличающимся от кремния [5].

Достоинства WDM-PON:

1. абоненту предоставляется выделенная полоса для приёма и передачи (нет распределения на конкурентной основе);

2. сигналы абонентов физически изолированы;

3. эффективно используется волокно (до 64 абонентов на волокно);

4. возможно значительное увеличение дальности связи (используя AWG с низкими потерями вместо неэффективных с точки зрения потерь сплиттеров при стандартном для GPON бюджете в 28 dB, можно подключать абонентов на расстоянии порядка 80 км).

Основной недостаток WDM-PON — высокая стоимость, так как требуются узкополосные передатчики, излучающие на заданной длине волны. Это особенно критично для абонентских устройств ONT, так как их стоимость напрямую влияет на стоимость абонентской линии. С одной стороны проблема частично решается за счет унификации и уменьшения типов аппаратных компонент в оконечных устройствах (например, использование настраиваемых на заданную волну лазеров), с другой — не без оснований можно надеяться, что через несколько лет к моменту выхода стандарта стоимость оптических компонент для WDM-PON будет значительно ниже нынешнего уровня. [6].

Переход от TDM-PON к WDM-PON является залогом успешного будущего оптических сетей доступа в том числе и с точки зрения защиты информации**,** при этом можно также существенно увеличить еще и возможности сети такие как: предоставление абоненту требуемой полосы пропускания, значительное увеличение дальности связи а также и увеличение количества абонентов.

Список использованных источников:

1. Птицын Г.А. Живучесть динамических сетей телекоммуникаций / Под ред. Петракова А.В.: Учебное пособие. - М.: МТУСИ. 2008. - 48 с.

2. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей

3. Булавкин И.А. Вопросы информационной безопасности сетей PON // Технологии и средства связи — 2006. - IW2. - С. 104-108.

4. Kyeong-Eun Han, Design of AWG-based WDM-PON Architecture with Multicast Capability

5. Урядов В.Н., Глущенко Д.В. Использование технологии WDM для повышения эффективности пассивных оптических сетей // Международная научно-техническая конференция, посвященная 45-летию МРТИ-БГУИР : тез. докл. Междунар. науч.-техн. конф., Минск, 19 марта 2009. – Минск : БГУИР, 2009. – 19с.

6. Урядов В.Н., Глущенко Д.В. Коллективная пассивная WDM сеть с независимым доступом к оптической среде передачи // Современные средства связи : материалы XIV Междунар. науч.-техн. конф., 29 сент.-1 окт. 2009 года, Минск, Респ. Беларусь. – Минск : ВГКС, 2009. – 23с.

ВИДЕОКОНФЕРЕНЦИЯ КАК ИНСТРУМЕНТ ОБЩЕНИЯ МЕЖДУ ОРГАНИЗАЦИЯМИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Подлужный А.И, Смирнов Ю.В.

Смирнов Ю.В. – ассистент

В связи с бурным развитием сетевых и коммуникационных технологий, возросшей производительностью компьютеров, и, соответственно, с необходимостью обрабатывать все возрастающее количество информации возросла роль оборудования и программного обеспечения. Виртуальные средства обучения, удаленный доступ, дистанционное обучение и управление, а также средства проведения видеоконференций переживают период расцвета и предназначены для облегчения и увеличения эффективности взаимодействия как человека с компьютером, так и групп людей с компьютерами, объединенными в сеть.

Видеоконференция (англ. videoconference) – область информационной технологии, обеспечивающая одновременно двустороннюю передачу, обработку, преобразование и представление интерактивной информации на расстояние в режиме реального времени с помощью аппаратно – программных средств вычислительной техники. Взаимодействие в режиме видеоконференций называют сеансом видеоконференцсвязи.

Рисунок 1 – **Видеоконференция**

Видеоконференции характеризуются как комбинация звука и видео, а также технологиями работы с сетями связи для взаимодействия в реальном времени. Видеоконференция в этом плане очень схожа с телефонией, в которой происходят все те же действия по обеспечении связи, что и в видеоконференции. За исключением того, что в видеоконференции есть возможность передавать видео, файлы множества форматов, транслировать рабочий стол, записывать беседы, и все это делается параллельно. Поэтому для работы с видеоконференцией необходима большая ширина полосы пропускания, чем для телефона.
Видеоконференции можно разделить не только по техническим, но и на настольные (индивидуальные), групповые и студийные. Каждый из этих вариантов видеоконференций четко ориентирован на решение своих задач. Наиболее распространены благодаря относительно невысокой стоимости и быстроте окупаемости затрат сегодня настольные средства проведения видеоконференций.
Они применяется как средство оперативного принятия решения в той или иной ситуации; при чрезвычайных ситуациях; для сокращения командировочных расходов в территориально распределенных организациях; повышения эффективности; проведения судебных процессов с дистанционным участием осужденных, а также как один из элементов технологий телемедицины и дистанционного обучения. Во многих государственных и коммерческих организациях видеоконференция приносит большие результаты и максимальную эффективность, а именно: снижает время на переезды и связанные с ними расходы; ускоряет процессы принятия решений в чрезвычайных ситуациях; сокращает время рассмотрения дел в судах общей юрисдикции; увеличивает производительность труда; решает кадровые вопросы и социально – экономические ситуации; дает возможность принимать более обоснованные решения за счёт привлечения при необходимости дополнительных экспертов; быстро и эффективно распределять ресурсы, и так далее.
Однако до недавнего времени видеоконференцсвязь являлась недостаточно качественной и технически полноценной, чтобы начинать внедрять ее в рабочий процесс, в частности из-за ее дороговизны. Сейчас ситуация изменилась в лучшую сторону, причем стоимость даже наиболее сложных изделий мала, что позволяет устанавливать видеоконференцию практически любому человеку. Исторически видеоконференции часто использовались рабочими группами, которые собирались в специализированном месте, чтобы связаться с другими группами людей. Обычно это был зал заседаний, оснащенный специализированным оборудованием. Стоимость средств видеоконференций, используемых для этого, была велика из-за необходимости использования специализированного высококачественного оборудования и дорогих арендованных каналов связи.

Список использованных источников:
1 Интернет-портал http://www.newreferat.com/ref-1366-16.html
2 Интернет-портал http://uchebnik-online.com/132/1472.html

ЧАТ-БОТ КАК НОВЫЙ ЭТАП РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Завьялов А.А.
Макейчик Е.Г. – старший преподаватель

Чат-бот – это программа, имитирующая деятельность человека. Чат-боты имитируют собеседника в чате. Первые эксперименты по созданию подобных программ начались еще полвека назад. Один из успешных примеров придания взаимодействия с машиной иллюзии человеческого общения – Элиза, написанный в 1966 году чат-бот, имитирующий диалог с психотерапевтом.

Сегодня чат-боты способны и повсеместно заменяют собой службы поддержки всевозможных сервисом. Рынок мобильных приложений перенасыщен: их счет пошел на миллионы, но пользователи уже не горят желанием устанавливать что-то новое. Согласно исследованиям ComScore, 80% времени пользователи проводят всего в трех приложениях. На этом фоне сегмент мессенджеров продолжает активно расти. Мессенджеры приватны, требуют меньше ресурсов, работают на более дешевых устройствах.

Для начала работы с чат-ботом необходимо добавить его в список контактов и начать переписку. Чаще всего в ответ бот пришлет информацию о себе, список доступных команд или выведет на экран кнопки, превращающие окно диалога в интуитивно-понятное мини-приложение.

Выделяют 4 типа ботов:

1. Боты-помощники. Такие чат-боты всегда будут рядом, найдут нужную информацию, поставят будильник и решат ряд организационных задач: заказ пиццы, броня в гостинице, покупка билетов. Например: бот, который информирует о погоде – @weatherman_bot, или помогает найти нужную информацию на сайте фонда.
2. Боты – искусственный интеллект. Разработки в области искусственного интеллекта ведут к тому, что чат-боты смогут вскоре выполнять задачи, которые ранее требовали от человека много временных ресурсов. Например, ответы на вопросы теперь может найти головной ассистент Speaktoit.
3. Боты для бизнеса. Данные боты направлены на увеличение коэффициента полезного действия, то есть на оптимизацию бизнеса. Пример ботов для бизнеса – сервисы Битрикс24, SpyCat 2.0 (сервис, который оповещает о новых комментариях в социальной сети «ВКонтакте» с функцией автоответчика).
4. Игровые боты. Например: игра «Привет, незнакомец!»

Чат-боты получили широкое распространение не только в развлекательной сфере, но и в сфере телекоммуникаций. Крупные телекоммуникационные компании создают свои чат-ботов, чтобы задействовать новые каналы общения со своими клиентами. Чат-боты позволяют компаниям не только добиться лояльности клиентов, но и получать выгоду. Основным плюсом таких чат-ботов является то, что они позволяют компаниям сократить штат сотрудников колл-центров, тем самым съэкономив бюджет компании.

Современные чат-боты работают не только по запрограммированному алгоритму, они обладают возможностью обучения. Столкнувшись с новым запросом впервые, бот переадресовывает его реальному человеку, а получив ответ заносит в базу своих знаний, что позволяет в следующий раз ответить сразу.

В перспективах развития чат-ботов рассматриваются не только возможность распознавания и синтеза речи, но и подключения ботов к искусственному интеллекту, что позволит им полностью заменить сотрудника колл-центра любой телекоммуникационной компании и не только.

Тестируются различные API (Application Programming Interface), чтобы выбрать наиболее многофункциональный и продвинутый интерфейс. Очень скоро визуальные технологии останутся в прошлом, и чат-боты станут неотъемлемой частью технологического ландшафта.

По оценкам аналитиков, в ближайшем будущем чат-боты будут иметь все большую значимость. Они вполне могут заменить классические поисковые платформы и социальные сети. Преимуществами ботов станут простота взаимодействия с ними, скорость их реакции, и возможность их настройки под пользователя. Использование бота значительно упрощает взаимодействие с сервисами, предоставляя универсальный интерфейс.

Список использованных источников:
1. Фомичев Г. Chatbots формируют будущее технологий
2. Лоскутов А. Боты: что это такое, как они работают и почему пришла пора в них разобраться

ОЦЕНКА КАЧЕСТВА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Голик О.Д.

Цветков В.Ю. – д.т.н.,доцент

При использовании систем видеонаблюдения, одна из основных задач – это поиск оптимального качества получаемого изображения. Требуемое качество зависит от того, для чего видеонаблюдение используется (для определения движения на территории нет надобности в мелких деталях, а, например, распознавание лиц требует высококачественной съемки). Под качеством изображения понимается совокупность свойств изображения, объективных и субъективных, которые влияют на восприятие изображения человеком. Цель данной работы состоит в сравнении изображений, получаемых с одной видеокамеры при различных параметрах кодирования, с использованием размеров сегментов.

Предлагается для оценки качества изображений, получаемых с помощью цифровой видеокамеры при различных параметрах кодирования, использовать распределение вероятностей размеров сегментов. При сегментации, пиксели изображения, стоящие рядом и имеющие похожие яркостные характеристики, объединяются логически в одну область.

Предполагается, что изображение является более «качественным», т.е. несет больше полезной информации для наблюдателя, если содержит большее число сегментов малого размера, в то время как у визуально «некачественных» изображении количество мелких сегментов мало.

Для получения результатов использовались программные средства сегментации и оценки распределения вероятностей размеров сегментов, разработанные в среде Matlab, а также видеокамера D-link DCS-2230L. Камера DCS-2230L позволяет получать видео форматов MotionJPEG и H.264 с различными параметрами.

Для рассмотрения формата H.264 было взято 7 изображений одинакового размера, но с различными битрейтами (4M, 2M, 1M, 512K, 200K, 128K, 64K).

(А)

(Б)

Рис.1 Исходные изображения

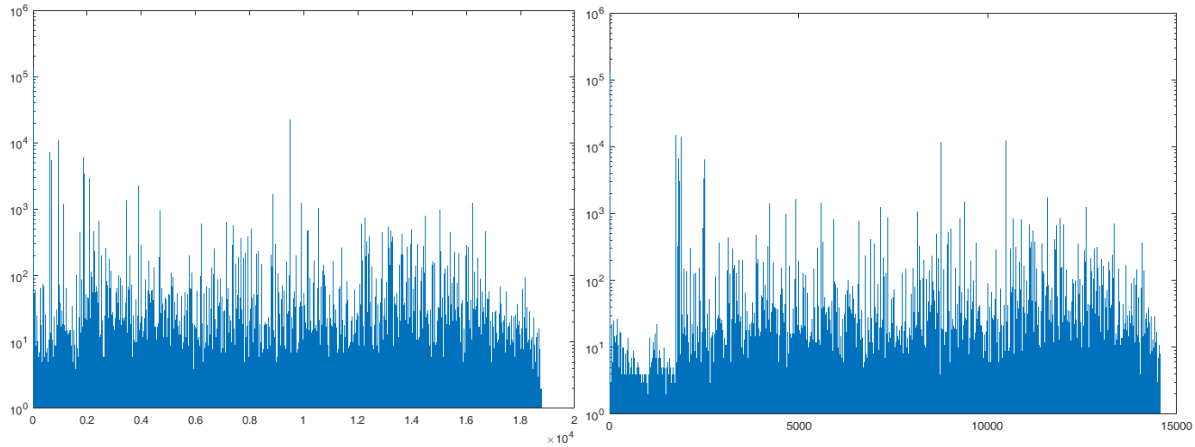


Рис.2 Гистограммы изображений А и Б, показывающие суммарное число пикселей в сегментах.

Гистограммы, полученные после сегментации изображений (рис.2), отражают, что у изображения А в наблюдается «проседание» гистограммы в области мелких сегментов. Так же, стоит заметить, изображения имеют различное число сегментов.

Для анализа MPEG были взяты 5 изображений различного размера (960x720, 800x592, 640x480, 480x352, 320x240), но с фиксированным значением качества в настройках камеры («excellent»).

Сегменты с размерами менее 20 пикселей были отнесены в группу «малые», 20-100 пикселей – «средние», и сегменты содержащие более 100 пикселей – в группу «крупные». На основе этого разбиения

были построены графики отражающие количество «мелких», «средних» и «крупных сегментов» в изображениях (рис.4).

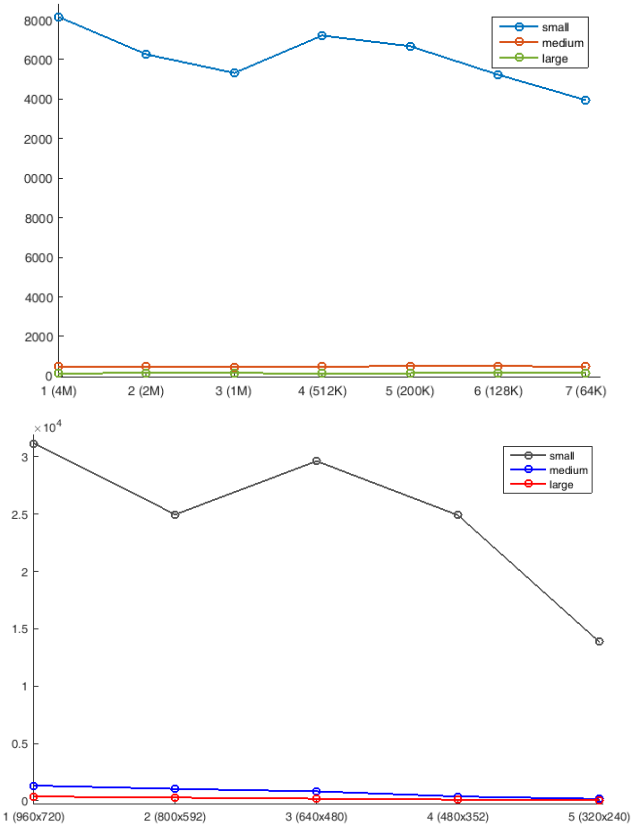


Рис.3 Количество сегментов (по верт.) для изображений с различным битрейтом (слева), с различным размером (справа)

Количество мелких сегментов уменьшается как и с уменьшением битрейта изображений, так с уменьшением размера изображения. Количество средних и крупных сегментов остается примерно одинаковым, либо незначительно падает (это обусловлено тем, что при уменьшении изображения уменьшается и общее число сегментов)

Таким образом, можно сделать вывод о том, что выдвинутое предположение соответствует действительности. Изображения, которые человек считает репрезентативными (крупные, четкие изображения) имеют большее число мелких сегментов, которые несут больше информации.

В обработке цифровых изображений для сравнения изображений широко используется метод СКО (среднеквадратическое отклонение, в английском варианте - MSE). MSE рассчитывается по формуле:

$$MSE = \frac{1}{NM}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}|I_o(i,j) - I(i,j)|^2,$$

где N, M –размер изображений в пикселях, Io и I – матрицы базового и искаженного изображения соответственно. Если изображения одинаковы, то MSE=0. Изображения приводятся к одному размеру путем масштабирования. Первое изображение принимается базовым, и MSE остальных изображений считается относительно его.

Для исходных изображений были построенные графики изменения СКО.

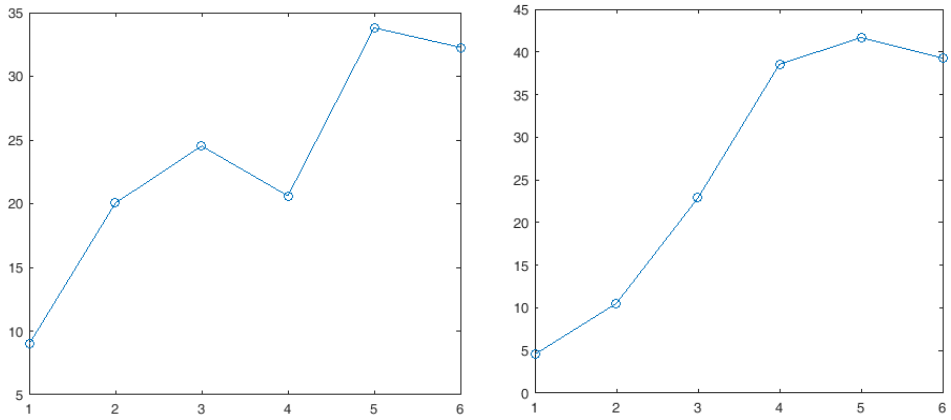


Рис.4 Изменение СКО изображений (H.264 – слева, JPEG – справа)

Среднеквадратическое отклонение увеличивается для изображений, которые визуально выглядят хуже, что подтверждает результаты, полученные ранее при оценке сегментов.

Список использованных источников:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений Издание 3-е, исправленное и дополненное Москва: Техносфера, 2012. – 1104 с.

2. http://www.dlink.ru/u/products/1433/2053_b.html

ИЗМЕРЕНИЯ ПАРАМЕТРОВ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Котов А.Р.

Белошицкий А.П. – к.т.н.,доцент

Актуальность разработки высокоэффективных, широкополосных, технологичных и удобных в эксплуатации экранирующих средств обусловливается не только проблемами биологического воздействия электромагнитных излучений на организм человека, но и проблемами защиты информации от утечки по техническим каналам. Одними из наиболее перспективных для этих целей являются экраны электромагнитного излучения (ЭЭМИ) на основе композиционных материалов.

В докладе рассматривается методика измерения ослабления ЭЭМИ для стандартов связи GSM 900, GSM 1800, UMTS 900, UMTS 2100 и приводятся результаты исследования экранирующих свойств различных экранов на основе композиционных материалов для этих стандартов связи.

Измерения проводились с использованием схемы, показанной на рисунке 1. Базовая станция сотовой связи использовалась в качестве генератора испытательного сигнала. Тестовый терминал Nokia 6720c выступал в качестве приемного устройства. Данные об уровнях сигналов с этого терминала, при использования ЭЭМИ и различных испытательных сигналов, передавались по кабельному соединению на персональный компьютер. В компьютере с помощью специализированного программного обеспечения выполнялась дальнейшая обработка результатов измерений с оценкой экранирующих свойств различных ЭЭМИ.

Рис. 1 – Схема измерений

Для проведения исследования были выбраны следующие экранирующие средства:

– экран электромагнитного излучения на основе модифицированных оксидов алюминия на алюминиевой фольге (экран №1);

– экран электромагнитного излучения на основе модифицированных оксидов алюминия на алюминиевой фольге (экран №2);

– экран электромагнитного излучения (эластичный пенополиуретан, содержащий частицы порошкообразного древесного угля) (экран №3);

– экран электромагнитного излучения на основе многослойного комбинированного материала (первый слой – хлопкополиэфирная ткань с наноструктурированным феромагнитным микропроводом, пропитанная 45%-м водным раствором хлорида кальция; второй слой – полиуритановая мастика; третий слой – фольгированный пенополистирол) (экран №4);

– экран электромагнитного излучения на основе многослойного комбинированного материала (первый слой – хлопкополиэфирная ткань с наноструктурированным феромагнитным микропроводом, пропитанная 45%-м водным раствором хлорида кальция; второй слой – фольгированный пенополистирол) (экран №5);

– экран электромагнитного излучения на основе многослойного комбинированного материала (первый слой – углеродосодержащий игольнопробивной материал, на поверхность которого, посредством распыленного клея нанесен порошковообразный шунгит; второй слой – фольгированный пенополистирол) (экран №6);

– фольгированная лавсановая пленка (экран №7);

В докладе приводятся результаты исследования различных ЭЭМИ на основе композиционных материалов. По результатам исследований средние уровни ослабления сигнала для каждого из ЭЭМИ в стандартах связи GSM 900, GSM 1800, UMTS 2100 и UMTS 900 представлены в таблице 1.

Таблица 1 – Средние уровни ослабления сигнала

Стандарт / № экрана	GSM 900 (925,2 МГц)	GSM 1800 (1866 МГц)	UMTS 2100 (2137,6 МГц)	UMTS 900 (935 МГц)
	Уровень ослабления, dBm	Уровень ослабления, dBm	Уровень ослабления, dBm	Уровень ослабления, dBm
Экран №1	+10	-17	+8	+1
Экран №2	-4	-17	-0,1	0
Экран №3 (внутренняя сторона)	-10	-35	-20	-15
Экран №3 (внешняя сторона)	-6	-30	-2	-21
Экран №4 (внутренняя сторона)	-16	-21	-11	-27
Экран №4 (внешняя сторона)	-29	-30	-25	-24
Экран №5 (внутренняя сторона)	-15	-25	-17	-30
Экран №5 (внешняя сторона)	-27	-42	-12	-12
Экран №6 (внутренняя сторона)	-8	-30	-23	-20
Экран №6 (внешняя сторона)	-21	-42	-16	-25
Экран №7	-21	-20	-24	-30

В результате этих исследований было показано, что ЭЭМИ, изготовленный из эластичного пенополиуретана, содержащего частицы порошкообразного древесного угля (экран №3), является наиболее универсальным экранирующим средством для стандартов сотовой связи указанных выше.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ШЛЮЗОВ БЕЗОПАСНОСТИ В ВЕДОМСТВЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Андриянов П.А., Андриянова Т.А.
Саломатин С.Б. – к.т.н.,доцент

Опыт создания и функционирования современных ведомственных телекоммуникационных систем подтвердил экономическую и техническую целесообразность формирования их на базе арендованных магистральных линий передачи (телефонных каналов общего пользования – ТКОП) и создания на их основе систем передачи данных (СПД). Современные СПД представляют собой программно-технические комплексы (ПТК), созданные на основе персональных компьютеров, высокоскоростных сетевых устройств и действующих каналов связи, в которых формирование и анализ сигналов выполняется как на аппаратном, так и на программном уровнях.

Характерной особенностью ПТК систем передачи данных является то, что в них интегрированы процессы ввода-вывода, защиты от ошибок, формирования и анализа сигналов. Кроме того, они выполняют и другие, не связанные с передачей данных, функции, такие как поиск и формирование файловых данных, компрессия и декомпрессия, защита от НСД и другие [1].

С точки зрения безопасности организуемых соединений можно выделить ряд способов: использование туннелей, шифрование, разделение потоков, аутентификация и управление доступом. При выборе конкретной технологии нужно учитывать следующие факторы:

вид передаваемого трафика (данные, голос, видео);

профиль трафика в течение суток и недели (передаются ли данные только днем или, например, ночью идет резервное копирование и сбор статистики);

иерархическую организацию площадок организации (один головной офис или структура, состоящая из головного офиса, кустовых узлов и оконечных узлов);

постоянство занимаемых площадей (собственность или аренда);

вид площадей (полноценные филиалы, пункты обслуживания клиентов или дата-центры);

организацию бизнес-процессов компании (как в плане операционной деятельности, так и временные параметры сбора информации и формирования отчетов);

требования к информационной безопасности;

общую политику организации (аренда каналов или собственные капитальные вложения) [2].

С точки зрения информационной безопасности стоит говорить об уровне конфиденциальности и ценности передаваемой информации, а также об уровне возможного ущерба в случае ее утечки, уничтожения, модификации или блокирования. Наиболее системный и общий подход состоит в том, что проводится классификация соединяемых территориально распределенных площадок организации по указанным признакам с объединением их в группы. Для каждой группы определяется оптимальный типовой вариант решения с возможностью расширения в будущем. В любом случае общая рекомендация сводится к использованию услуг сети MPLS (все основные операторы дальней связи предлагают услуги сети MPLS, а в тех регионах, где этого нет, надо использовать или выделенные каналы, или Frame Relay) и протокола IPSec. В качестве альтернативы протоколу IPSec для государственных организаций могут выступать отечественные аппаратно-программные разработки на основе алгоритмов шифрования и сертифицированного оборудования с поддержкой IPSec [2].

Защищенность соединений можно рассматривать с двух точек зрения: обеспечение защиты на технологическом уровне, за счет особенностей технологии (при этом трафик одного пользователя виртуально отделяется от трафика другого пользователя, и в нормальных условиях они не пересекаются) и обеспечение защиты с помощью шифрования трафика.

Рациональный выбор организационно-технологических и программных решений для защиты коммуникаций в территориально распределенных ведомственных информационных системах определяется несколькими факторами: архитектурой и масштабом сети, обрабатываемой в информационной сети информацией, используемой линейной и активной аппаратурой и собственно задачами обеспечения безопасности данных.

Программно-аппаратный шлюз, как средство сетевой безопасности, предназначен для обеспечения сетевой безопасности вычислительной сети любой топологии: выполняет функции шифрования, контроля целостности (криптографической защиты), а также фильтрацию как трафика подсетей, проходящего через них, так и защиту трафика самих шлюзов безопасности.

Средства сетевой информационной безопасности - это технологии виртуальных защищенных сетей (Virtual Private Network, VPN) и интегрированные с ними средства аутентификации и контроля доступа. Технологии VPN обеспечивают шифрование (конфиденциальность), электронно-цифровую подпись (целостность, имитостойкость, аутентификацию) на уровне IP-пакетов. На основе технологии VPN обеспечиваются защищенные соединения между подсетями и компьютерами. При этом компьютеры могут идентифицироваться как "обезличенные" узлы сети (по IP-адресу) и как рабочие места заданных индивидуальных пользователей (такая идентификация проводится, как правило, по сертификату пользователя). Технологии VPN предоставляют гибкость в реализации политики сетевой защиты. Для защиты могут использоваться множественные алгоритмы шифрования, сложные конфигурации туннелей и

защищенных периметров. Технологии VPN обеспечивают высокую стойкость защиты информации; при необходимости защитить сложную сетевую инфраструктуру эти технологии не имеют практической альтернативы. Технологии VPN используют средства шифрования, хэширования и электронной цифровой подписи.

Рассмотрим технологию предоставления доступа к удаленным рабочим столам Virtual Desktop Infrastructure (VDI), которая в настоящее время получила особую популярность в качестве дополнительных средств защиты от несанкционированного доступа и других внешних угроз в сфере применения ведомственных информационных ресурсов в целях создания подконтрольных виртуальных рабочих мест. С помощью технологии VDI пользователи получают доступ к информационным ресурсам своей организации и необходимому программному обеспечению.

Способы защиты VDI:

1. Защита на основе SSL VPN с дополнительной аутентификацией.
2. Защита на основе IPsec VPN с дополнительной аутентификацией.
3. IPsec VPN на специализированном терминале. Предлагаемое решение совместимо с любыми системами VDI и соответствует требованиям законодательства в области информационной безопасности. Оно позволяет сотрудникам получить защищенный доступ к инфраструктуре виртуальных рабочих столов и приложений из любой точки.

В данном сценарии сотрудники работают на терминальных станциях с оптимизированной операционной системой, находящейся на защищенном съемном носителе. Аутентификация пользователя на рабочей станции происходит до загрузки операционной системы, а после загрузки - в самом VDI приложении. Защита данных при их передаче обеспечивается встроенным в ОС IPsec VPN клиентом. Защита от вредоносного ПО реализуется с помощью замкнутой программной среды и проверки целостности при запуске.

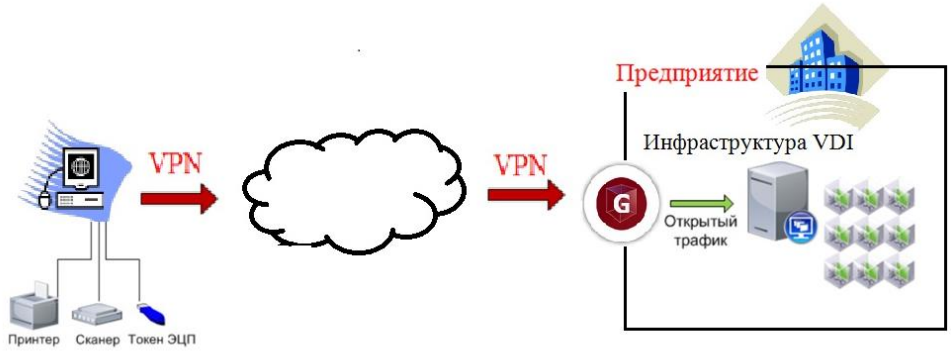


Рис. 1 - Пример защиты удаленного доступа к инфраструктуре VDI с использованием шлюзов безопасности.

Для защиты серверной части используется шлюз безопасности в виде виртуальной машины для популярных гипервизоров (VMware ESX, Citrix). Данные технологии защиты позволяют обеспечить:

Изолированное сетевое соединение с инфраструктурой VDI. Целевой трафик передается по защищенному VPN-туннелю, при этом обеспечивается конфиденциальность и целостность передаваемой информации. Остальной трафик либо запрещен, либо передается через ведомственный сервер, в зависимости от настроенных политик безопасности.

Итак, использование замкнутой программной среды и СЗН минимизирует воздействие агрессивной информационной среды на работу с важной информацией, а также снижает риски, связанные с возможными деструктивными действиями пользователей. Также можно отказаться от применения антивирусного программного обеспечения на рабочих местах пользователей и дополнительных средств защиты. Это позволяет не только сэкономить средства, но и существенно облегчить процесс эксплуатации терминалов, поскольку нет необходимости контролировать их конфигурацию и обновлять антивирусные базы данных.

Выделить какое-либо из упомянутых решений в качестве наиболее предпочтительного достаточно сложно, так как рациональная защита должна строиться с учетом характеристик информации, параметров информационной системы и уровня различных угроз.

Список использованных источников:

1. Буренин, А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А.Н. Буренин, Легков К.Е. // Наукоемкие технологии в космических исследованиях Земли. – №3. – 2015. т. 7. № 3. с. 46–61.

2. Романов С.А., Огородников Д.С., Защищенные коммуникации в территориально распределенных компаниях / Романов С.А., Огородников Д.С.// Журнал «BYTE» - №6 – 2015.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНЫХ СТРУКТУР ДАННЫХ ПРИ РАБОТЕ С БОЛЬШИМИ ОБЪЁМАМИ ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Закревский И.Е.
Гурский А.Л. – д-р физ.-мат. наук., профессор

Операции над большими массивами данных являются неотъемлемой частью ежедневной работы во многих областях информатики. Так как каждая операция над конкретным элементом применяется много раз, даже незначительное сокращение ресурсов в пересчете на одно действие может дать значительную экономию. Также, в виду бурного развития рынка интернета вещей, поднимается вопрос об энергопотреблении устройств и, как следствие, оптимизации их исходного кода. Растут объемы баз данных, что сказывается на скорости работы средств защиты информации, таких как средства аутентификации, DLP системы, анализаторы трафика и т.д. Одним из путей решения таких проблем является использование вероятностных структур данных, в частности — фильтр Блума.

Фильтр Блума — это вероятностная структура данных, позволяющая хранить и проверять принадлежность элемента к множеству[1]. В фильтре Блума возможны ложноположительные срабатывания, то есть структура данных может положительно ответить о наличии элемента, когда на самом деле его нет, в то время как ложноотрицательных срабатываний быть не может. Фильтр Блума не хранит элементы, а только предоставляет информацию об их наличии во множестве.

Фильтр Блума представляет собой битовый массив из m бит, которые по умолчанию обнулены. Далее, пользователю необходимо определить k независимых хеш-функций, которые будут преобразовывать массив входных данных произвольной длины в битовую строку фиксированной длины m достаточно равномерным способом. Процент ложноположительных срабатываний может быть уменьшен увеличением размера массива m и/или числа хеш-функций k [2].

Чтобы добавить новый элемент в фильтр Блума, необходимо пропустить его через k хеш-функций, которые вернут k номеров позиций в массиве, подлежащих установлению в 1.

Для проверки наличия элемента во множестве надо пропустить его через k хеш-функций, которые вернут k позиций массива. Если любой из битов в этих позициях равен 0 – данный элемент точно отсутствует в множестве, т.к. все биты должны были быть установлены в 1 во время вставки. Если все биты равны 1 – то либо элемент находится во множестве, либо значение 1 было установлено в результате коллизии хеш-функций и это приведёт к ложноположительному срабатыванию.

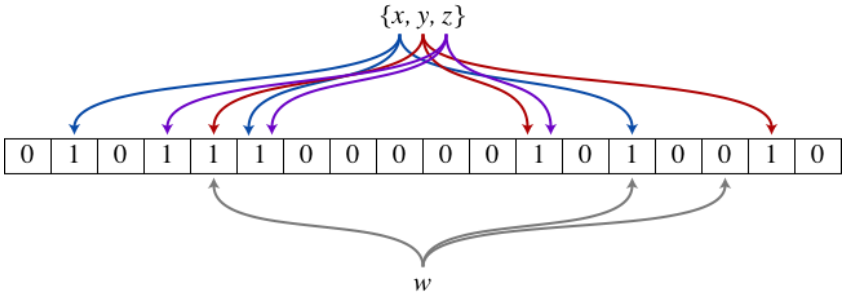


Рис. 1 - Пример фильтра Блума. Элементы x, y, z являются членами множества, w — нет

Если количество потенциальных значений невелико и многие из них могут быть уже во множестве, фильтр Блума легко превосходит детерминированный битовый массив, который требует только один бит для каждого потенциального элемента.

Дополнительным преимуществом фильтра Блума является тот факт, что время добавления и проверки наличия элемента в множестве постоянно и является $\theta(k)$ и не зависит от количества элементов в множестве. В виду того, что запросы к структуре независимы, они могут быть легко распараллелены.

В данной работе был реализован фильтр Блума (k = 3, m = 10^9) и использован для определения необходимости вызова удалённой БД. Использование фильтра Блума в качестве структуры данных для хранения информации о наличии элемента в БД позволило сократить на 77% используемую память по сравнению с хеш-таблицами, также незначительно уменьшило время на добавление состояния новых элементов в множество (>5%).

Список использованных источников:
1. Bloom, Burton H., Space/time trade-offs in hash coding with allowable errors,
2. Dillinger, Peter C.; Manolios, Panagiotis, "Fast and Accurate Bitstate Verification for SPIN"

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ НА ОСНОВЕ РЕШЕНИЙ SAP FOR BANKING

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Волынец П.Л.

Гурский А.Л. – д. ф-м. н., профессор

В последние годы бурное развитие информационных технологий, появление новых способов передачи информации, увеличение объемов и скорости передаваемой информации привело к необходимости смены действующих децентрализованных банковских систем на более современные централизованные комплексы. Централизация системы позволяет быстрее производить расчеты, выполнять клиентские операции и вести мониторинг своего бизнеса, сокращая издержки на сопровождение и развитие многих систем одновременно.

Система на основе решений от компании SAP является позволяет решать широкий спектр задач с ведением единой базы, возможностью интеграции с другими системами по различным каналам, имеет гибкую систему настроек и возможность самостоятельного создания необходимых программ для конкретной организации.

Однако при расширении функциональности собственными разработками внутри системы появляются проблемы с мониторингом работы пользователей в системе стандартными средствами для выявления ошибок и противоправных действий. Также появляются проблемы с ограничениями прав доступа к собственным разработкам стандартными средствами. Появляется также необходимость внедрения собственных расширений в стандартные программы для изменения работы базовых программ для определенных бизнес процессов.

Для решения указанных проблем были разработаны методы ведения журналов и информирования пользователей, реализованы методы проверки полномочий в собственных разработках и расширениях стандартных программ, реализуются и совершенствуются методы анализа программного кода на возможные уязвимости и ошибки, анализ противоречий в ролях доступа у пользователей, анализ тривиальности паролей у системных пользователей.

Для ведения журнала действий пользователей были созданы программные методы, которые в процессе выполнения программы сохраняют важную информацию, предупреждения о различных модификация. Созданы таблицы с ведением пользователей для рассылки определенных событий от пользователей. При возникновении критических ситуаций, указанные для этого события (группы событий) пользователи будут получать уведомления на экране в виде всплывающих окон с необходимой информацией. Так же рассылается сообщение по внутренней почте.

При запуске и выполнении разработанных программ используются методы проверки полномочий как стандартных объектов, так и созданных, которые включаются в стандартные роли доступа, но проверяются в необходимых местах и на определенные разрешения собственными методами. Так в рамках одной программы пользователю могут быть ограниченны права доступа к одним процессам и разрешены к другим.

Так же для обеспечения качества и бесперебойной работы системы при выполнении доработок, до переноса их в реальную систему они проходят проверку разработанными методами анализа программного кода, который находит потенциальные угрозы и предупреждает об них и предлагает возможные варианты решения.

Реализованы методы поиска и анализа конфликтующих ролей у пользователей, которые могут привести к несанкционированному доступу либо к нежелательному ограничению прав.

Преимуществом решений SAP является:

- за счет большого количества внедрений и долгого времени существования комплекса к настоящему времени большинство программных проблем были решены ранее, и заказчик получает хорошо оттестированный и проверенный продукт;
- быстрое разворачивание практически готового универсального решения, но требующего доработок под необходимости определенного направления;
- квалифицированная служба поддержки.

К недостаткам можно отнести:

- стоимость внедрения и сопровождения;
- длительность процесса внедрения и доработки, обусловленная необходимостью адаптации универсальной системы под определённые бизнес-процессы;
- сложность перехода к новым версиям программного обеспечения при большом объеме собственных доработок.

Переход к централизованным решениям благоприятно сказывается на скорости работы системе, едином ведении всей необходимой отчетности и позволяет контролировать все процессы в системе в любое время в реальном времени.

ИССЛЕДОВАНИЕ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ГЕНЕРАТОРА КАЧАЮЩЕЙСЯ ЧАСТОТЫ МИЛЛИМЕТРОВОГО ДИАПАЗОНА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пастор А.В.

Белошицкий А.П. – к.т.н.,доцент

В измерительной технике часто используют генераторы гармонических сигналов, частоту которых автоматически изменяют (качают) в пределах заданной спектральной полосы – генераторы качающейся частоты (ГКЧ). Освоение миллиметрового диапазона длин волн требует создания современных ГКЧ этого диапазона и исследования их метрологических характеристик (МХ).

Исследование МХ средств измерений проводится с использованием методик поверки или калибровки. В докладе приводятся результаты исследования метрологических характеристик ГКЧ КВЧ диапазона Г4-МВМ-118, разработанного в Центре 1.9 НИЧ БГУИР.

ГКЧ применяются в качестве самостоятельных источников сигнала для проверки и настройки КВЧ аппаратуры в условиях цехов, лабораторий, а так же в составе автоматизированных систем при работе с управлением от компьютера через USB.

Генератор предназначен для генерирования колебаний сигналов КВЧ в режимах непрерывной генерации на одной частоте (НГ) и перестройки частоты (ПЧ) в диапазоне частот от 78,33 до 118,10 ГГц.

Обобщенная структурная схема ГКЧ представлена на рисунке 1.

Рисунок 1 – Структурная схема ГКЧ

ГКЧ содержит задающий кварцевый генератор частоты 100 МГц, выходной сигнал которого поступает на синтезатор. Синтезатор формирует сетку высокостабильных значений частот в диапазоне от 13 до 20 ГГц. С помощью двух умножителей частоты обеспечивается рабочий диапазон частот генератора. Модулятор обеспечивает режим амплитудно-импульсной модуляции.

Основными МХ генератора являются :

1) Основная погрешность установки частоты в режиме непрерывной генерации.
2) Основная погрешность установки уровня выходной мощности.
3) КСВН выхода генератора.

Определение основной погрешности установки частоты в режимах непрерывной генерации проводилось с использованием схемы, представленной на рисунке 2. В результате исследований было установлено, что максимальное значение погрешности установки частоты не превышает $\pm 1 \cdot 10^{-7} \cdot f_y$, где f_y – номинальное значение частоты, установленное на генераторе, ГГц.

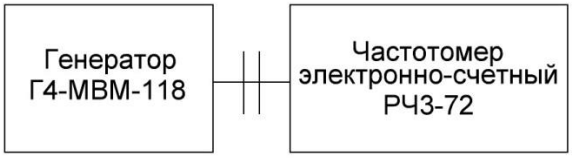


Рисунок 2 – Определение основной погрешности установки частоты в режиме непрерывной генерации

Определение основной погрешности установки уровня выходной мощности проводилось с использованием схемы, приведенной на рисунке 3, путем последовательной установки уровней мощности: -10; -15; -20 дБм на частотах 78,33; 88,00; 98,00; 108,00; 118,10 ГГц. Мощность сигнала измерялась ваттметром М3-75. В результате исследований было установлено, что максимальное значение погрешности установки уровня выходной мощности не превышает $\pm(1{,}0+0{,}1 \cdot P)$ дБ, где P – установленное значение мощности.

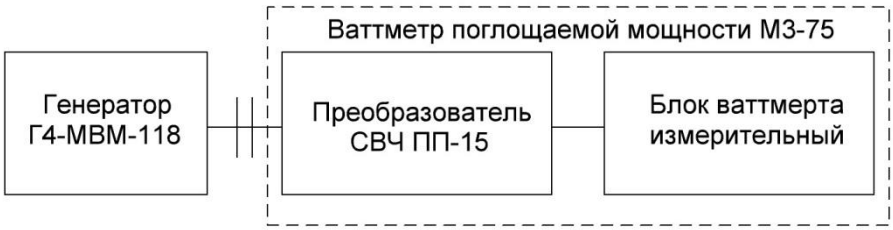


Рисунок 3 – Определение основной погрешности установки уровня выходной мощности

Определение КСВН выхода генератора проводилось в соответствии со схемой, приведенной на рисунке 4. С помощью панорамного измерителя КСВН и ослаблений последовательно измерялись значения КСВН выхода генератора на частотах 78,33; 88,00; 98,00; 108,00; 118,10 ГГц. В результате исследований было установлено, что КСВН выхода генератора не превышает 1,5.

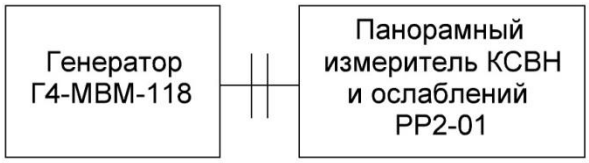


Рисунок 4 – Определение КСВН выхода генератора

Результаты исследования метрологических характеристик ГКЧ миллиметрового диапазона длин волн Г4-МВМ-118 показывают, что данный генератор отвечает современным требованиям метрологической практики.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ ПРИ ФОРМИРОВАНИИ СИГНАЛОВ ЦИФРОВОЙ АМПЛИТУДНОЙ МОДУЛЯЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Рыжков С.А.

Ильинков В.А. – к.т.н., доцент

Телекоммуникации являются наиболее динамичной областью науки и техники, которая, в частности, характеризуется использованием современных методов формирования, модуляции и передачи сигналов, все большим расширением функциональных возможностей и уменьшением времени жизни производимых моделей телекоммуникационной техники. С учетом сформировавшихся тенденций развития, основным методом исследования, проектирования и разработки систем телекоммуникаций (СТК) является математическое моделирование.

Известные программы математического моделирования сигналов цифровой модуляции (общего и специального назначения) обладают рядом существенных недостатков, не позволяющих полноценно применять их в научных исследованиях и учебном процессе. Поэтому весьма актуально создание программы математического моделирования основных функциональных преобразований при формировании сигналов цифровой модуляции, которые весьма широко применяются в современных СТК.

Разработка математических моделей функциональных преобразований сигналов

Сравнительный анализ методов и устройств формирования сигналов цифровой амплитудной модуляции (ASK-M, QAM-M) [1] показывает, что общая процедура преобразования исходного (модулирующего) сигнала в выходной (модулированный) распадается на следующие последовательно выполняемые этапы (процедуры): формирование временной реализации модулирующего сигнала и его огибающей амплитудного спектра; амплитудная компрессия; дискретизация модулирующего сигнала, включая формирование массива отсчетных значений; преобразование дискретных значений в цифровой код, включая формирование упорядоченной цифровой последовательности; формирование четной, нечетной последовательностей и блоков символов; преобразование блоков символов из двоичного кода в код Грея; формирование радиосимволов и образование сигнала цифровой амплитудной модуляции, включая формирование таблицы истинности, формирование радиосимволов ASK-M и QAM-M, отображение сигнальных созвездий; формирование операторной передаточной функции высокочастотного тракта; моделирование реализации прохождения модулированного сигнала через высокочастотный тракт.

С учетом ограниченного объема работы рассмотрим только некоторые процедуры функциональных преобразований.

1. Процедура формирования огибающей амплитудного спектра исходного сигнала

Все модулирующие сигналы обладают существенно неравномерным амплитудным спектром, огибающая которого непрерывно спадает, с ростом частоты (например, ТВ сигнал), либо имеет максимальное значение на некоторой центральной частоте f_0 (например, речевой сигнал). С учетом изложенного, целесообразно огибающую амплитудного спектра исходного сигнала представить зависимостью

$$c(f) = 1 - (1 - \mathrm{sgn}(f - f_0))A_L(f - f_0) - (1 + \mathrm{sgn}(f - f_0))A_U(f - f_0), \quad (1)$$

где $\mathrm{sgn}(f - f_0) = \begin{cases} 1, f \geq f_0 \\ -1, f < f_0 \end{cases}$; $A_{L(U)} = \dfrac{1 - 1/N}{2(f_{L(U)} - f_0)^2}$; $f_L(f_0, f_U)$ - нижняя граничная частота (центральная частота, верхняя граничная частота); N – коэффициент уменьшения уровней спектральных компонент на граничных частотах f_L и f_U.

Варьируя параметрами f_L, f_U, f_0 и N, можно задавать различные виды огибающей амплитудного спектра сигнала.

2. Формирование временной реализации модулирующего сигнала

Известно, что: реальные исходные сигналы представляют собой нестационарный случайный процесс, математическое моделирование которого весьма затруднительно [2]. Учитывая это, для упрощения, в качестве модулирующего сигнала используем полигармонический сигнал вида

$$U_{вх}(t) = \sum_{z=1}^{z} C(zf_1)U_m \cos(2\pi z f_1 t + \varphi), \quad (2)$$

где f_1 – частота первой гармоники (целесообразно $f_1 = f_L$); U_m – амплитуда гармоники на частоте f_0; φ – начальная фаза; Z – количество гармонических составляющих; $C(zf_1)$ – огибающая, представленная моделью (1).

Такой сигнал является периодическим с периодом повторения $T = \frac{1}{f_1}$, что весьма удобно для реализации последующих процедур. Варьируя параметрами Z, f_1 и U_m, можно получить различные реализации близкие по частотным и временным свойствам к реальному модулирующему сигналу.

Разработка программы моделирования функциональных преобразований сигналов

В соответствии с построенными математическими моделями разработаны схема программы-оболочки и схемы всех программ-процедур. Написана и отлажена (в среде .NET, системе программирования C#) моделирующая программа, которая работает в операционной системе Windows XP и её последующих версиях. Для работы требуется предустановленная платформа .NET Framework 4.0.

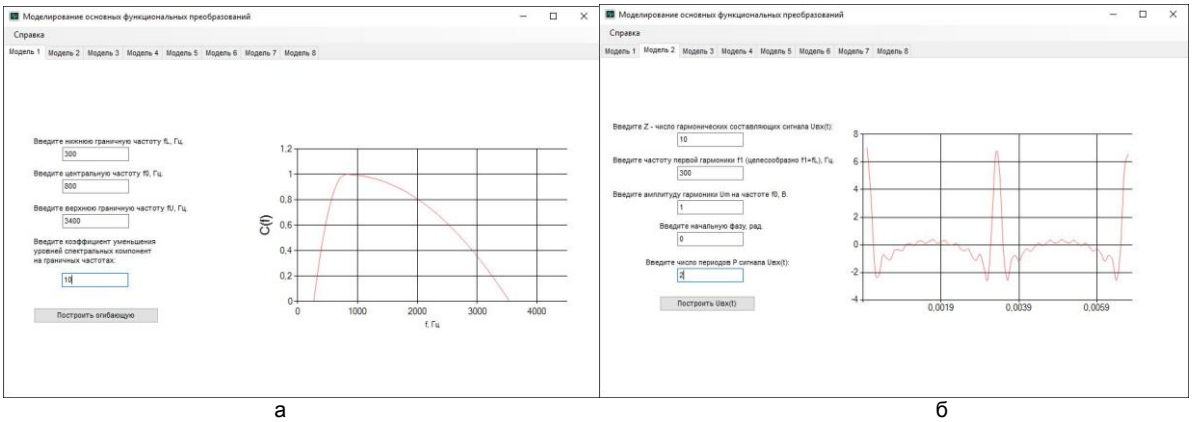
Программа реализована в виде файла с расширением “.exe”, занимает на жестком диске объем менее 2 Мбайт, поддерживает интерактивный режим работы, обладает интуитивно-понятным и дружелюбным интерфейсом. Она характеризуется высокой скоростью выполняемых операций и наглядно отображает результаты моделирования**.**

Навигация по моделям осуществляется с помощью подменю расположенного у верхнего края рабочей поверхности. Большинство моделей требует от пользователя выбора параметров или их ввода, для построения графиков сигналов необходимо нажатие соответствующей кнопки.

В разработанной программе предусмотрен механизм обработки исключений, который защищает пользователя от возможных ошибок и неверных шагов.

В меню справка находится необходимая информация для работы с каждой из моделей.

Скриншоты работы программы представлены на рис.1.



а б

Рис. 1 – Моделирование огибающей амплитудного спектра (а)
и моделирование исходного сигнала во временной области (б)

Для проверки работоспособности моделирующий программы, выполнено несколько циклов моделирования, при существенно различных конкретных значениях параметров. Результаты моделирования полностью подтвердили правомерность использования предложенных математических моделей.

Список использованных источников:

1. Прокис, Дж. Цифровая связь / Дж. Прокис ; пер. с англ. ; под ред. Д.Д. Кловского. – М.: Радио и связь, 2000. – 800с.

2. Электроакустика и звуковое вещание. Учебное пособие для ВУЗов / И.А. Алдошина [и др.]; под общ. ред. Ю.А. Ковалгина. – М.: Радио и связь, 2007. – 872с.

ИССЛЕДОВАНИЕ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ВЕКТОРНОНО АНАЛИЗАТОРА ЦЕПЕЙ КВЧ ДИАПАЗОНА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кирикович И.А.

Белошицкий А.П. – к.т.н.,доцент

Для определения комплексных параметров устройств КВЧ-диапазона используется векторный анализатор цепей (ВАЦ), который должен обладать высокими метрологическими характеристиками (МХ). Исследование метрологических характеристик таких анализаторов является весьма важной и актуальной задачей.

Исследования МХ средств измерений проводится с использованием методик поверки или калибровки. В докладе приводятся результаты исследования метрологических характеристик ВАЦ Р4-МВМ-37 КВЧ-диапазона разработанного в центре 1.9 НИЧ БГУИР.

Данный ВАЦ предназначен для автоматизированного исследования волноводных КВЧ устройств, работающих в диапазоне частот от 25,95 до 37,5 ГГЦ и измерения комплексных коэффициентов передачи (S_{21}) и отражения (S_{11}) этих устройств с цифровым отсчетом измеряемых величин и воспроизведением их частотных характеристик в декартовой системе координат на экране анализатора. В анализаторе реализован гомодинный метод измерения. Для получения информации об аргументах измеряемых S-параметров используются дискретные фазовращатели на pin-диодах и специальные алгоритмы калибровки и измерения.

Основными МХ ВАЦ являются :

1) Диапазон измерения модуля коэффициентов отражения $|S_{11(22)}|$ и погрешность их измерения.
2) Диапазон измерения модуля коэффициентов передачи (ослабления) $|S_{21(12)}|$ и погрешность их измерения
3) Диапазон измерения аргумента коэффициента отражения $\arg S_{11(22)}$ и погрешность его измерения.
4) Диапазон измерения аргумента коэффициента передачи $\arg S_{21(12)}$ и погрешность его измерения.

Определение диапазона измерения модулей коэффициентов отражения $|S_{11(22)}|$ и погрешностей их измерения, проводилось с использованием схемы представленной на рисунке 1. В результате исследований было установлено, что максимальное значение погрешности не превышает $\pm(0{,}2+0{,}03|S_{11}|)$.

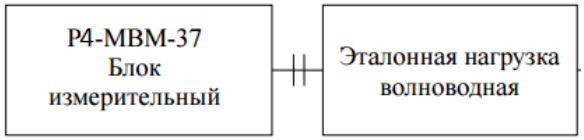


Рисунок 1 – Определение погрешности при измерении модуля коэффициента отражения

Определение диапазона измерения модулей коэффициентов передачи (ослабления) $|S_{21(12)}|$ и погрешностей их измерения, проводилось с использованием схемы представленной на рисунке 2. В результате измерений выяснилось, что максимальные значения погрешности $\Delta|S_{11(22)}|$ во всем диапазоне частот не превышают $\pm(0{,}2+0{,}02|S_{21}|)$.

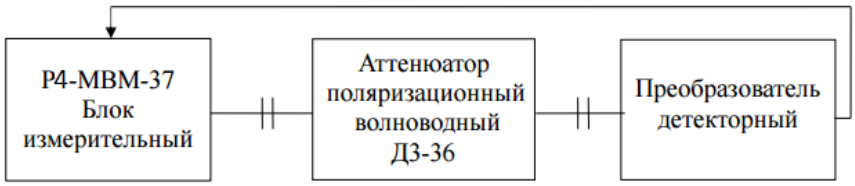


Рисунок 2 – Определение диапазона измерения и погрешности при измерении коэффициента передачи

Определение диапазона измерения аргумента коэффициента отражения $\arg S_{11(22)}$ и погрешности его измерения, проводилось с использованием схемы представленной на рисунке 3. В результате исследований было установлено, что максимальное значение погрешности измерения фазы коэффициента отражения не превышают ±5,0°.

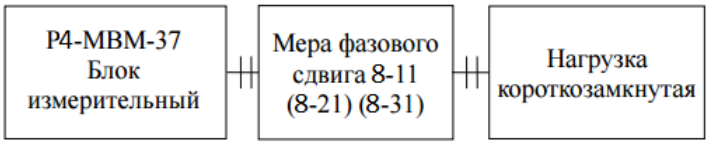


Рисунок 3 – Определение погрешности при измерении фазы коэффициента отражения

Определение диапазона измерения аргумента коэффициента передачи $argS_{21(12)}$ и погрешности его измерения, проводилось с использованием схемы представленной на рисунке 4. В результате измерений выяснилось, что максимальные значения погрешности измерения фазы коэффициента передачи не превышают ±4,0º.

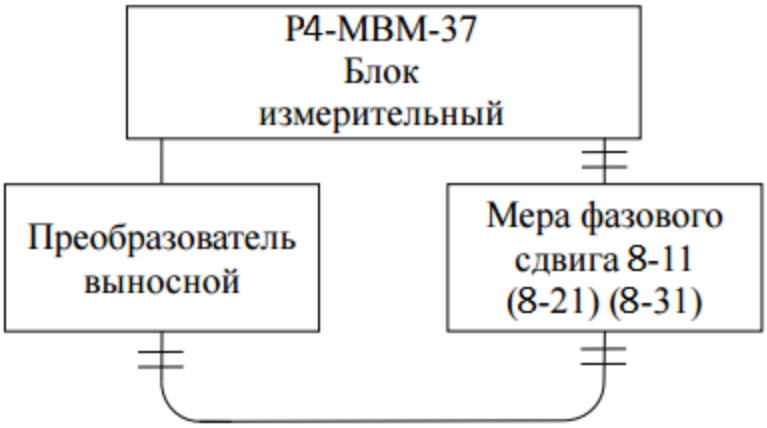


Рисунок 4 – Определение погрешности при измерении фазы коэффициента передачи

Результаты исследований МХ ВАЦ Р4-МВМ-37 показывают, что данный анализатор может использоваться для решения большинства метрологических задач КВЧ-диапазона

ИССЛЕДОВАНИЕ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК СКАЛЯРНОГО АНАЛИЗАТОРА ЦЕПЕЙ КВЧ ДИАПАЗОНА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Матющенко Е.А.

Белошицкий А.П. – к.т.н.,доцент

С освоением КВЧ диапазона длин волн возникает потребность в создании современных средств измерений этого диапазона и исследование их метрологических характеристик (МХ). Исследование метрологических характеристик проводится с использованием методик калибровки, поверки или метрологической аттестации.

В измерительной технике часто используются скалярного анализатора цепей (САЦ) КВЧ диапазона. В процессе проектирования, изготовления и эксплуатации СВЧ и КВЧ устройств и систем наиболее частыми измеряемыми параметрами являются модули коэффициентов отражения |S11| и передачи |S21|.

В докладе приводятся результаты исследования МХ САЦ Р2-78-ИХЧ КВЧ диапазона, разработанного в Центре 1.9 НИЧ БГУИР.

Принцип действия САЦ основан на измерении сигналов, полученных в результате раздельного выделения падающей на ОИ, отраженной от него и прошедшей через него волн КВЧ сигнала. Напряжения, пропорциональные амплитудам падающей, отраженной и прошедшей волн, поступает в измерительный блок. В этом блоке происходит обработка этих сигналов и вычисление измеряемых параметров: модулей коэффициентов отражения |S11|, (КСВН) и передачи |S21| (ослабления).

Структурная схема САЦ показана на рисунке 1.

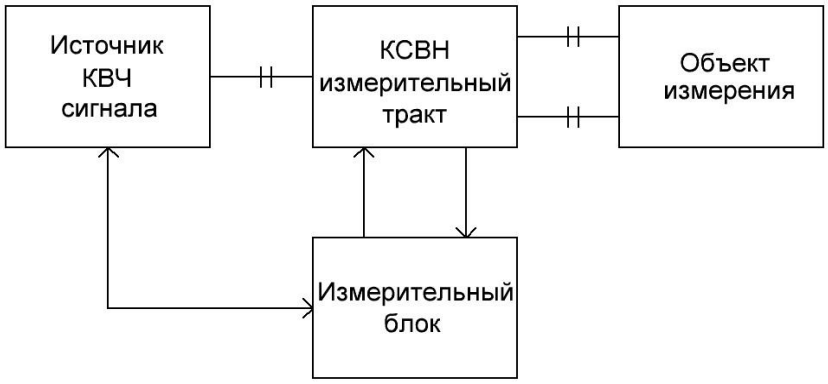


Рисунок 1 – Структурная схема САЦ

Источник КВЧ сигнала состоит из синтезатора и двух умножителей частоты.

КВЧ измерительный тракт состоит из трех направленных ответвителей, к выходам которых подключены предварительные усилители.

Для определения МХ САЦ была разработана программа и методика метрологической аттестации. С использованием этой методики были проведены исследования МХ САЦ.

На рисунках 2, 3 и 4 представлены структурные схемы, с использованием которых определялись МХ САЦ.

Определение диапазона рабочих частот анализатора и относительной погрешности установки и отсчета частоты проводилась по схеме приведенной на рисунке 2.

Рисунок 2 – Структурная схема для определения диапазона рабочих частот и относительной погрешности установки и отсчета частоты

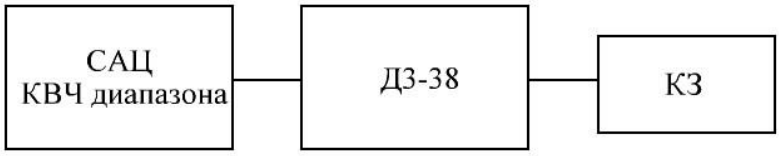


Рисунок 3 – Структурная схема для определения пределов измерения и основной погрешности измерения |S11|

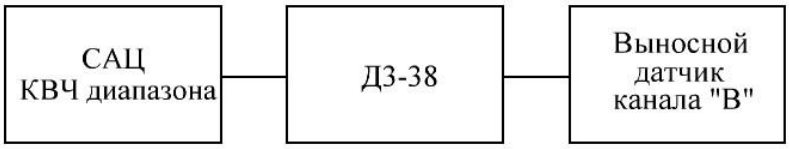


Рисунок 4 – Структурная схема для определения пределов измерения и основной погрешности измерения |S21|

В результате проведенных исследований были получены следующие МХ Р2-МВМ-78:

В результате исследований было установлено, что САЦ позволяет измерять модули коэффициентов отражения в диапазоне от 0 до минус 32 дБ с погрешностью не более ±(0,2+0,03·S11), а модули коэффициентов передачи в диапазоне от 0 до минус 40 дБ с погрешностью не более ±(0,2+0,02·S21) дБ. Пределы допускаемой относительной погрешности установки частоты не более ± 0,1 % от установленной частоты. Диапазон индикации КСВН от 1,1 до 5. КСВН волноводного СВЧ выхода измерительного блока не более 1,3. Нестабильность частоты его выходного сигнала – не более 1·10-6 от fmax. Пределы допускаемой относительной погрешности установки частоты не более ± 0,1 % от установленной частоты. Диапазон индикации КСВН от 1,1 до 5. КСВН волноводного СВЧ выхода измерительного блока не более 1,3.

Результаты исследований метрологических характеристик скалярного анализатора цепей КВЧ диапазона показывает, что данный измеритель отвечает современным требованиям метрологической практики.