



ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN



Л. Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л. Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY



Студенттер мен жас ғалымдардың
«Ғылым және білім - 2015»
атты X Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
X Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2015»

PROCEEDINGS
of the X International Scientific Conference
for students and young scholars
«Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96

«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: <http://www.eni.kz/ru/nauka/nauka-i-obrazovanie-2015/>, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2015

жесткой встречей, сближение с мягким контактом, сближение с пролетом ПО мимо КА на некотором расстоянии).

Таким образом, сравнивая значения требуемой угловой скорости линии визирования, полученные по результатам полного качественного исследования системы, с данными аналитического решения задачи можно установить в каких случаях при рассмотрении ближнего наведения ПО на КА допустимо пользоваться упрощенной математической моделью, а когда необходимо использовать более точную модель, в которой учитывается действие относительного гравитационного ускорения.

Список использованных источников

1. Циолковский, К. Э. Грезы о Земле и небе и эффекты всемирного тяготения / Циолковский, К. Э. Издательство «Луч», 1894, 368 с.
2. Иванов, В. А. Сближение в космосе с использованием тросовых систем / В. А. Иванов, С. А. Купреев, М. Р. Либерзон // Издание: Хоружевский. 2010. 360 с.
3. Андреев А. В., Хлебникова Н.Н. Космические системы с гибкими связями. // Итоги науки и техники. ВИНТИ. Т. 12, 1991, 195 с.
4. Асланов В.С., Ледков Н.Н., Стратилатов Н.Р. Пространственное движение космической тросовой системы, предназначенной для доставки груза на Землю. // Общероссийский научно-технический журнал «Полет». №2, 2007, с. 28-32.

ПОДСЕКЦИЯ 1.2 РАДИОТЕХНИКА, ЭЛЕКТРОНИКА И ТЕЛЕКОММУНИКАЦИИ

УДК 681.3

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ МОДЕЛИРОВАНИЯ ЛОКАЛЬНОЙ СЕТИ С ЛИНЕЙНОЙ АРХИТЕКТУРОЙ

Абдакаева Алия

alichka_1993@mail.ru

Студент физико-технического факультета ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Н.А.Бурамбаева

В настоящее время широкое применение получили локальные вычислительные сети (ЛВС), которые строятся на ПЭВМ, соединенных линией связи и аппаратурой, поддерживающей соответствующий интерфейс. Информация в таких сетях передается в виде пакетов стандартной длины и формата. Структура пакета и методы его обработки регламентируются специальными протоколами. Если передаваемое сообщение имеет большую длину, то оно представляется как последовательность пакетов. Такая операция выполняется с использованием сетевого оборудования и его программного обеспечения.

В качестве канала чаще всего применяют высокочастотный телефонный кабель с пропускной способностью 40 - 1000 Кбод. Для подключения к нему используют сетевые адаптеры (контроллеры, сетевые карты), в состав которых могут быть включены модемы.

Наиболее распространенными структурами сети являются:

- моноканал или шина (рис. 1.1), типичным примером которых служит Ethernet;
- звезда (рис. 1.2), например Fast Ethernet;
- петля (кольцо) - рис. 1.3, классическим примером которой является сеть Token

Ring.

В линейных сетях используется случайный метод доступа (захват канала в любой момент - CSMA/CD). При этом возможно наложение пакетов, передаваемых с разных станций, т.е. искажение информации. Оно обнаруживается оборудованием сетевых

адаптеров (СА). Случайный доступ реализуется двумя основными способами: с проверкой столкновений и несущей. Первый способ (с проверкой столкновений) только обнаруживает наложение передаваемого пакета на тот, который движется по каналу. При обнаружении столкновения передача прекращается, и следующая попытка предпринимается через случайный интервал времени τ . Этот способ применяется в слабо загруженных сетях. При проверке несущей адаптер прослушивает канал и начинает передачу только, если в ней отсутствует пакет (нет несущей частоты). Такой способ обеспечивает меньшую вероятность столкновения пакетов и лучшую загрузку линии связи.

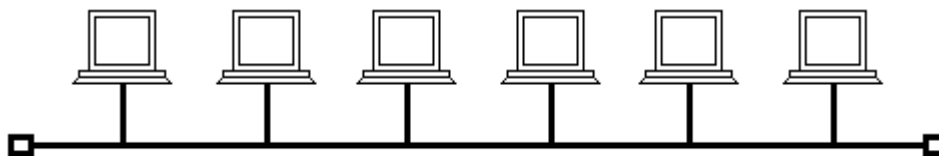
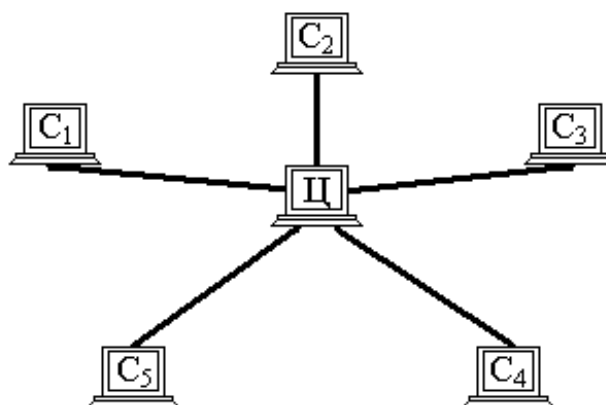


Рис. 1.1. Типовая структура линейной ЛВС

В настоящее время всё большее распространение получает звездообразная структура сети (рис. 1.2). Она наилучшим образом обеспечивает реализацию режима обработки задач «Клиент – сервер». В такой сети имеется мощная центральная ЭВМ, выполняющая функции файлового сервера и управляющая работой всей сети. Эта структура носит название активная звезда. Более простые сети вместо центральной ЭВМ используют концентраторы или коммутаторы. Их архитектура называется пассивной звездой.



Ц – Центральная ЭВМ, C_1 - C_5 – локальные станции

Рис. 1.2. Типовая структура звездообразной ЛВС

В кольцевых сетях используется детерминированный (маркерный, эстафетный) метод доступа. При этом сетевой адаптер получает разрешение на передачу пакета в момент поступления специального маркера. Обычно его роль играет пустой пакет. После получения заполненного пакета адаптер адресата освобождает его от информации и гонит по каналу.

При исследовании используется программа имитационного моделирования наиболее распространенной сети, имеющей архитектуру типа моноканала (аналога Ethernet). Программа составлена на языке Delphi 4.0. Она позволяет выполнить следующие операции:

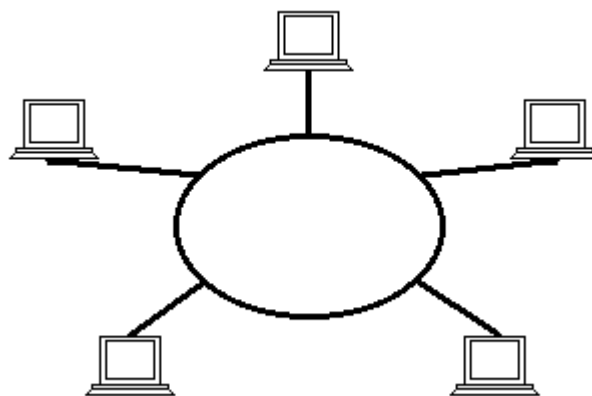


Рис. 1.3. Типовая структура кольцевой ЛВС

1. Варьировать пропускную способность линии связи от 40 до 1024 Кбайт.
2. Задать один из двух методов доступа к линии: с проверкой столкновений или с проверкой несущей.
3. Установить один из двух режимов моделирования: непрерывно или по тактам.

По умолчанию моделирование осуществляется в непрерывном режиме.

Моделируемая сеть может содержать до 10 станций, соединенных между собой каналом связи. Работа каждой станции представляется закраской ее на схеме соответствующим цветом. Станция может находиться в состоянии обслуживания программы или передачи пакета. Пакеты передаются в канал в случайные моменты времени, которые определяются с помощью генератора случайных чисел. Максимальное значение интервала времени между отправлениями двух соседних пакетов, как отмечалось выше, является характеристикой соответствующей программы. Передача пакета в модели представляется закраской канала цветом ее станции.

Как отмечалось выше, важной особенностью и недостатком случайного метода доступа к каналу являются наложения (столкновения) пакетов. В модели предусмотрено обнаружение этой ситуации, прекращение передачи и возобновление ее через случайный промежуток времени. Количество столкновений подсчитывается программой и является одной из характеристик сети.

Исполняемый модуль программы моделирования имеет имя **Lan.exe** и находится в папке **Lab 9**. Запуск программы осуществляется традиционным способом. После запуска на экране появляется первое окно, позволяющее задать параметры модели и режим моделирования.

В левой части окна находится панель управления приложением. На ней размещено несколько кнопок, каждая из которых снабжена всплывающей подсказкой. Кнопка с изображением раскрытой книги переводит приложение в режим ввода характеристик или моделирования. После запуска установлен первый режим.

Все поле для ввода параметров разделено на четыре основных блока.

1. «Типы задач», обеспечивающий задание до двадцати различных типов задач, каждый из которых характеризуется числом пакетов, их размером и максимальным интервалом времени между двумя соседними пакетами;
2. «Линия связи», позволяющий ввести пропускную способность линии, которая может изменяться в пределах от 40 до 1024 Кбайт в секунду.
3. В блоке «Характеристики станции» задаются количество, типы задач и порядок их обслуживания для каждой станции в отдельности или для всех одновременно. Последняя операция обеспечивается выбором поля «Принять для всех станций». При этом необходимо выбрать тип задачи из соответствующего блока, а затем нажать кнопку пересылки.

Указанная кнопка находится между блоками. На ней изображена стрелка, направленная вправо. Задачи, которые приписаны станции, изображаются в ее списке в том порядке, в котором они будут впоследствии обрабатываться. Этот список можно очистить или удалить из него какую-либо запись с помощью соответствующих кнопок (название кнопки можно увидеть на всплывающей подсказке).

4. В последнем блоке, «Дисциплина доступа станций к линии связи», задаются методы доступа станций к каналу: с проверкой столкновений или несущей.

После того как ввод всех параметров закончен нужно переключиться на режим моделирования. Запуск модели осуществляется нажатием на кнопку с изображением зеленой лампочки. При этом будет поддерживаться непрерывный режим, а кнопка утоплена. В любой момент можно остановить моделирование повторным нажатием на ту же кнопку, а затем – снова продолжить. Имеется возможность исследовать работу сети в каждом такте, определяемом ее новым состоянием (началом или окончанием передачи очередного пакета). Выполнение такта начинается после нажатия мышью кнопки с изображением красной лампочки.

Во время моделирования появляется окно приложения, в верхней части которого изображена структура сети (станции и линия связи), а в нижней - представлена трасса загрузки канала и станций. Каждой станции, как отмечалось выше, соответствует свой цвет. В нижней части экрана выводится столько трасс (временных диаграмм), сколько рабочих станций считалось активными в моделируемой сети. При возникновении конфликта через все диаграммы проводится вертикальная линия белого цвета.

В средней части экрана в процессе моделирования в полях «Прошло времени», «Количество конфликтов», «Среднее время выполнения» выводятся основные характеристики сети. После каждого запуска модели программа запоминает значение среднего времени выполнения задач и строит график этого времени, который располагается в рамке, находящейся в правой половине средней части экрана. Для его получения нужно запустить программу, по меньшей мере, дважды.

Необходимо провести следующие исследования.

1. Меняя количество программ, обрабатываемых сетью и станциями, при одинаковых параметрах самих программ определить времена их пребывания в сети и среднее время выполнения одной программы, а также количество столкновений для каждого из двух способов доступа.

2. Задавая разные параметры программ, обрабатываемых сетью и станциями, при постоянном общем количестве программ, определить времена их пребывания в сети и среднее время выполнения одной программы, а также количество столкновений для каждого из двух способов доступа.

3. Варьируя параметры станций и линии связи при постоянных параметрах программ и их количестве, определить времена их пребывания в сети и среднее время выполнения одной программы, а также количество столкновений для каждого из двух способов доступа.

4. Построить графики зависимости времени и количества столкновений от изменяемых параметров.

1. Графики следующих зависимостей для каждого из двух способов доступа к линии связи:

1) общего и среднего времени выполнения программ от количества программ;
2) количества столкновений от числа программ;
3) общего и среднего времени выполнения программ от длины пакета и максимального интервала времени между последовательными моментами отправления двух пакетов;

4) количества столкновений от длины пакета и максимального интервала времени между последовательными моментами отправления двух пакетов;

- 5) общего и среднего времени выполнения программ от заданного преподавателем параметра одной или нескольких станций или линии связи;
- 6) количества столкновений от заданного преподавателем параметра одной или нескольких станций или линии связи.

Список использованных источников

- 1) Таненбаум Э.С. Архитектура компьютера, 4-е издание. С-Пб: Изд. Питер, 2003. 704 с.
- 2) Столингс У. Структурная организация и архитектура компьютерных систем, 5-е издание. М: Изд. дом Вильямс, 2002. 896 с.
- 3) Локальные вычислительные сети. Справочник. Под ред. С.В. Назарова М.: Финансы и статистика, 2007. – 58 с.

УДК621.316.97

ЭЛЬ – ГАМАЛЬ ЖӘНЕ RSA АЛГОРИТМДЕРІНІҢ ЭЛЕКТРОНДЫ САНДЫҚ ҚОЛТАҢБАЛАРЫНЫҢ ҚАЗАҚСТАНДАҒЫ ҚОЛДАНЫСЫ

Алдашева Лаура Сабитхановна

aldasheva_ls@enu.kz

Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникациялар кафедрасының аға оқытушысы, Астана, Қазақстан

Майлыбаева Гүлжас Жаксылыковна

gul_zhas@mail.ru

Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникациялар кафедрасының оқытушысы, Астана, Қазақстан

Қазіргі ғылым мен техника қатар дамыған заманда криптографиялық жүйелер құпия ақпаратты оңай тасымалдау үшін қолданылады. Соның бір мысалы, электронды сандық қолтаңбаны қолданып, қағазсыз құжат айналымында дәстүрлі мөрді және қол қоюды ауыстыру болып табылады. Бұл жүйені қолданудың ең тиімді жақтарының бірі қаржылық шығындарды аз болуы мен уақыттың үнемді жұмсалыуында. *Электрондық сандық қолтаңба* – уақыттың жаңа талаптарымен бірге қадам басуды қалағандардың барлығы үшін тиімді шешім. Оны *жасанды көшіру мүмкін емес*.

Жасанды көшірмеден қосымша қорғау қолтаңбаның ашық кілті куәландырушы орталығының сертификатымен қамтамасыз етіледі. Одан басқа клиенттің қалауы бойынша, куәландырушы орталық клиенттің электрондық сандық қолтаңба сақтандыра алады.

Электронды сандық қолтаңба алгоритмі екі топқа бөлінеді:

- Қарапайым сандық қолтаңба
- Құжатты қалпына келтіретін сандық қолтаңба

Қарапайым сандық қолтаңбаға ГОСТ Р34.10-2001, ДСТУ, ECDSA стандарттары жатады.

Құжатты қалпына келтіретін сандық қолтаңбаларда қол қойылатын құжат болады: қолтаңбаны тексеру барысында автоматты түрде құжат та есептелінеді. Өте танымал алгоритмдердің бірі RSA осы топқа жатады.

Электронды сандық қолтаңбаны жасау үшін әртүрлі алгоритмдер қолданылады, олар: сандық қолтаңбаның RSA алгоритмі, сандық қолтаңбаның стандарттары және технологиялар ұлттық институтының DSA алгоритмі, Эль-Гамаль криптожүйесі, Окамото алгоритмі ESIGN, Шнорр сандық қолтаңбасы, Микали-Шамир цифрлы қолтаңбасы, ГОСТ Р34.10-94 және Р34.11-94 сандық қолтаңбасы, «Нотариус» сандық қолтаңбасы.