

"Ассоциация ГЛОНАСС/ГНСС-форум"

Ваш гид в мире навигации!



**Ассоциация разработчиков, производителей и потребителей
оборудования и приложений на основе глобальных
навигационных спутниковых систем**

**Ассоциация, опираясь на опыт ведущих специалистов
в области использования спутниковых навигационных технологий,
предлагает сотрудничество по следующим направлениям:**

- консалтинг по внедрению навигационных технологий и их использованию;
- сертификация аппаратуры спутниковой навигации ГЛОНАСС/GPS и систем на ее основе;
- консультационное сопровождение при подготовке конкурсной документации по внедрению информационно-навигационных систем;
- экспертная оценка конкурсной документации и поданных заявок;
- содействие в организации международного сотрудничества;
- выполнение научно-исследовательских и опытно-конструкторских работ;
- разработка информационно-аналитических материалов;
- проведение маркетинговых исследований;
- организация и проведение мероприятий;
- нормативно-правовое обеспечение и юридическая поддержка деятельности.

**Адрес: 125167, Москва, 4-ая ул. Восьмого Марта, д.3.
Тел. +7 (499) 152 31 70. Факс: +7 (499) 152 96 35. E-mail: info@aggf.ru. URL: www.aggf.ru**

Учредитель

ООО "Издательский дом Медиа Паблшер"

Главный редактор: Легков К.Е.

HT-ESResearch@yandex.ru

Издатель: Дымкова С.С.

ds@media-publisher.ru

Редакционная коллегия**Бобровский В.И.***д.т.н., доцент***Борисов В.В.***д.т.н., профессор***Будко П.А.***д.т.н., профессор***Будников С.А.***д.т.н., доцент, член-корреспондент Академии информатизации образования***Верхова Г.В.***д.т.н., профессор***Гончаревский В.С.***д.т.н., профессор, заслуженный деятель науки и техники РФ***Комашинский В.И.***д.т.н., профессор***Кирпанев А.В.***д.т.н., с.н.с.***Курносков В.И.***д.т.н., профессор, академик Арктической академии наук, академик Международной академии информатизации, академик Международной академии обороны, безопасности и правопорядка, член-корреспондент РАЕН***Мануйлов Ю.С.***д.т.н., профессор***Морозов А.В.***д.т.н., профессор, член Академии военных наук РФ***Мошак Н.Н.***д.т.н.***Пророк В.Я.***д.т.н., доцент***Семенов С.С.***д.т.н., доцент***Синицын Е.А.***д.т.н., профессор***Тучкин А.В.***д.т.н., с.н.с.***Шатраков Ю.Г.***д.т.н., профессор*

СОДЕРЖАНИЕ

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Легков К.Е.

Актуальные направления развития автоматизированных систем управления специального назначения

5

ТЕХНОЛОГИИ

Данилов А.В., Малышко А.В.

Методика оптимальной аппроксимации заданного распределения вероятности простейшим показательным распределением

8

Безуглов Д.А., Швидченко С.А.

Кумулянтный метод определения закона распределения

11

ТЕЛЕКОММУНИКАЦИИ

Кисляков М.А., Божко Е.С.

К вопросу оценки качества протоколов сетей передачи данных

15

Белинский Д.В.

Анализ помех и типовых ошибок в каналах связи при приеме сообщений

19

Буренин А.Н., Легков К.Е.

К вопросу моделирования организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями

22

Жук А.П., Иванов А.С.

Повышение структурной скрытности системы передачи информации с кодовым разделением каналов

26

СТАНДАРТЫ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА

Федоренко И.В., Нерсисянц А.А., Мясникова А.И.

Технологии MIMO в мобильных сетях нового поколения

29

Мясникова А.И., Голубинцев А.В.

IEEE 802.16: управление качеством информационного обмена в системах специального назначения

33

СИСТЕМЫ СПУТНИКОВОЙ НАВИГАЦИИ

Орёл Д.В.

Пути защиты от угроз функционирования аппаратуры гражданских потребителей глобальных спутниковых радионавигационных систем

38

CONTENT

AUTOMATED CONTROL SYSTEMS

Legkov K.E.

Actual directions of development of automated control systems of a special purpose

5

TECHNOLOGIES

Danilov A.V., Malyshko A.V.

Technique of optimum approximation of the given distribution of probability the elementary demonstrative distribution

8

Bezuglov D.A., Shvidchenko S.A.

Cumulant method of determination of the distribution law

11

TELECOMMUNICATIONS

Kislyakov M.A., Bozhko E.S.

To a question of an assessment of quality of protocols of data communication networks

15

Belinski D.V.

The analysis of noises and standard errors in communication links in case of reception of messages

19

Burenin A.N., Legkov K.E.

Simulation of the information managing director of a network for modern infocommunication networks management system

22

Zhuk A.P., Ivanov A.S.

Increase of structural reserve of an information transmission system code-division channels

26

STANDARDS FOR BROADBAND WIRELESS ACCESS

Fedorenko I.V., Nersesyanc A.A., Myasnikova A.I.

Technology mimo in mobile networks of new generation

29

Myasnikova A.I., Golubintsev A.V.

IEEE 802.16: quality management information exchange in systems of special purpose

33

SATELLITE NAVIGATION SYSTEMS

Oryol D.V.

Ways of protection against threats of functioning of equipment of civil customers of global satellite radio navigational systems

38

Vol III
No. 1-2011



High technologies
in Earth space research

Периодичность выхода – 2 номера в год
Стоимость одного экземпляра 500 руб.

Тираж 1000 экз. + Интернет-версия

Тематические направления:

• Вопросы развития АСУ • Физико-математическое обеспечение разработки новых технологий и средств инфокоммуникаций • Условия формирования основных стандартов подвижной связи • Проектирование, строительство и интерактивные услуги в СПС • Биллинговые и информационные технологии • Электромагнитная совместимость • Антенно-фидерное оборудование • Источники электропитания • Волоконно-оптическое оборудование и технологии • Вопросы исследования космоса • Спутниковое телевидение, системы спутниковой навигации, GLONASS, построение навигационных систем GPS • Вопросы развития геодезии и картографии • Программное обеспечение и элементная база для сетей связи • Компьютерная и IP-телефония • Информационная и кибербезопасность • Вопросы исследования Арктики • Метрологическое обеспечение • Правовое регулирование инфокоммуникаций, законодательство в области связи • Экономика связи

Редакция

Издатель: Светлана Дымкова
ds@media-publisher.ru

Главный редактор: Константин Легков
HT-ESResearch@yandex.ru

Выпускающий редактор:
Ольга Дорошкевич
ovd@media-publisher.ru

Предпечатная подготовка
ООО "ИД Медиа Паблишер"

www.media-publisher.ru

Адрес редакции

111024, Россия, Москва,
ул. Авиамоторная, д. 8, офис 512-514
Тел.: +7 (495) 957-77-43

194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, корп. 1,
Тел.: +7(911) 194-12-42

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.

Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет.

Материалы, опубликованные в журнале – собственность ООО "ИД Медиа Паблишер". Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя

All articles and illustrations are copyright. All rights reserved.
No reproduction is permitted in whole or part without the express consent of Media Publisher JSC

© ООО "ИД Медиа Паблишер", 2011

10-я международная конференция

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ

24-25 марта 2011 г.
Москва, Марриотт Аврора

Конференция проводится общественно-государственным объединением «Ассоциация документальной электросвязи» при поддержке Министерства связи и массовых коммуникаций Российской Федерации.

Отличительной особенностью конференций АДЭ является высокий уровень представительства органов государственной власти и бизнеса, а также методологическая стройность, профессионализм, актуальность и практическая направленность программ, в реализации которых участвуют ведущие российские и зарубежные специалисты.

ОСНОВНЫЕ ТЕМЫ КОНФЕРЕНЦИИ:

- Обеспечение информационной безопасности социально значимых услуг
- Стандартизация безопасности телекоммуникаций
- Услуги информационной безопасности операторами связи
- Безопасность и доверие при работе в сети Интернет
- Стандартизация безопасности телекоммуникаций
- Обеспечение повышения уровня безопасности при предоставлении услуг потребителям
- Защита персональных данных (ПДн) в информационных системах операторов связи
- Реализация СОПМ в IP-сетях
- Безопасность облачных вычислений
- Подготовка и аттестация специалистов в области информационной безопасности
- Использование шифровальных (криптографических) средств на ССОП
- Управление идентификацией и конфиденциальностью
- Взаимодействие организаций по стандартизации
- Централизованное управление сетью связи общего пользования (ССОП) в повседневных условиях и в условиях чрезвычайных ситуаций

**ПРИГЛАШАЕМ ВАС НА МЕЖДУНАРОДНЫЙ ФОРУМ 2011 ГОДА
ПО ОБЕСПЕЧЕНИЮ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ!**



Оргкомитет:

тел.: (495) 673-34-28, 673-32-46, 673-48-83, 956-26-12, 995-20-11
факс (495) 673-30-29 • e-mail: info@rans.ru • <http://www.rans.ru>

Актуальные направления развития автоматизированных систем управления специального назначения

Главное направление разрешения информационно-управленческих проблем строительства сил специального назначения - это информационно-техническое объединение всех имеющихся и перспективных средств в единое информационное пространство (ЕИП) за счет развертывания базовой информационно-управляющей системы, их интеграции в систему оружия и органов управления. Такое объединение потребует соответствующего совершенствования средств связи и передачи данных, всех видов информационного обеспечения, автоматизации и информатизации управления. Очевидно, что создание столь сложной, пространственно-распределенной системы невозможно без решения целого ряда проблем технического и организационного характера. Техническую основу сегмента сил специального назначения в едином информационном пространстве должна составить многомерная защищенная высокоскоростная сеть, включающая в свой состав следующие информационные средства: добытия информации, ее обработки и передачи, а также синхронизации и передачи сигналов точного времени.

Ключевые слова: система управления, информационное взаимодействие, система связи, инфокоммуникационная система, комплекс средств автоматизации.

Легков К.Е.,
Северо-Кавказский филиал
Московского технического
университета связи и информатики

Actual directions of development of automated control systems of a special purpose

Legkov K.E.,
North Caucasian branch of the Moscow
technical university of communication
and informatics

Abstract

The principal direction of permission of information and administrative problems of construction of forces of a special purpose is an information and technical combining of all available and perspective means in the common information space due to deployment of basic management information system, their integration into system of the weapon and governing bodies. Such combining will demand the appropriate enhancement of means of communication and the data transfer, all types of information support, automation and control informatization. It is obvious that creation so difficult, spatial distributed system is impossible without solution of a number of problems of technical and organizational character. In a common information space the multivariate protected high speed network including in the composition the following information means shall make a technical basis of a segment of forces of a special purpose: gettings of information, its processing and transmission, and also synchronization and signal transmission of exact time.

Keywords: management system, information exchange, communication system, infocommunication system, complex of an automation equipment.

Одной из перспективных задач развития автоматизированных систем управления (АСУ) становится задача предвидения возможного развития оперативной и боевой обстановки, формирования рациональных способов боевых действий. При этом необходимо обеспечить соответствие между возможностями комплекса средств автоматизации (КСА) по формированию способов боевых действий, с одной стороны, и обязанностями, правами, ответственностью должностных лиц в каждом звене управления, с другой.

В иерархической системе управления формирование способа боевых действий сил заключается в определении пространства, времени и форм боевых действий, оперативного построения, маневра сил и средств подчиненных частей и подразделений для решения специальных задач.

Таким образом, как в повседневной деятельности сил, так и в компьютерных моделях поддержки принимаемых решений должны отражаться принципы управления, в частности:

- принцип единоначалия;
- принцип централизации управления с предоставлением подчиненным инициативы в определении способов выполнения поставленных специальных задач;
- принцип личной ответственности должностных лиц за принимаемые решения на применение подчиненных сил и результаты выполнения ими поставленных специальных задач.

Наряду с вышеизложенным, необходимо учитывать и достаточно важную тенденцию в

развитии автоматизированных систем управления силами, на основе информационно-управляющих систем реального времени (ИУС РВ).

Основу ИУС РВ составляют пространственно разнесенные источники информации, действующие на различных физических принципах и обеспечивающие сбор, сверхбыструю обработку информации компьютерные сети (сетевые технологии).

Функциональные подсистемы перспективной АСУ должны обеспечивать автоматизацию как целевых процессов управления применением сил, так и функций управления органами управления, а инфраструктурные подсистемы должны обеспечивать базовый набор услуг по управлению информационными и вычислительными ресурсами АСУ в интересах работы всех функциональных подсистем. Они должны создаваться в контексте единых архитектурных решений, использовать максимально унифицированные программные компоненты и общую технологическую и информационную среду совместного применения и функционирования данных программных компонентов.

Использование инфраструктурных систем позволит повысить технологичность разработки перспективной АСУ и функциональных подсистем, как ее компонентов. Применение унифицированных программных компонентов, разработанных в рамках инфраструктурных систем, должно позволить разработчикам функциональных подсистем максимально сосредоточиться на решении поставленных задач, стоящих перед конечными пользователями

АСУ. При этом разрабатываемыми средствами должно обеспечиваться сопряжение с существующими и перспективными системами освещения обстановки и управления.

Работа перспективной АСУ должна обеспечиваться инфокоммуникационной системой специального назначения (ИКС СН).

Основой создания АСУ СН должна стать реализация концептуальной модели сервис-ориентированной архитектуры, основными достоинствами которой являются возможность эволюционного развития, обеспечение совместимости между отдельными элементами, многократное (повторное) использование программных компонентов.

Эта модель должна состоять из следующих основных компонент:

- презентационный уровень описывает интерфейсные сервисы для взаимодействия пользователей с информационной системой, включая закрытые и открытые порталы, доступ с мобильных устройств, а также различные преобразования информации при взаимодействии с внешними системами и устройствами;

- на уровне функциональных сервисов формируются модели и осуществляется управление выполнением процессов АС с использованием специализированных средств (типа BPEL), а также координация автоматизированных и "ручных" операций;

- интеграционные сервисы обеспечивают взаимодействие между приложениями, которое может быть реализовано, в частности, с использованием средств обмена сообщениями или в рамках единой среды исполнения, такой как сервер приложений J2EE;

- сервисы уровня данных реализуют средства извлечения и повторного использования данных из СУБД и приложений. Явное выделение такого уровня позволяет изолировать вышестоящие компоненты архитектуры от изменений в технологиях, а также обеспечить единый унифицированный подход к выполнению операций с данными;

- уровень инфраструктуры, приложений и СУБД является как бы основой для всей структуры, и именно здесь концентрируются основные инвестиции в ИТ.

Взаимодействие между этими уровнями, однако, осуществляется не напрямую, а через сервисы, выделенные на уровень обработки

событий. Сервисы этой компоненты архитектуры обеспечивают сбор данных о событиях в масштабе АСУ, необходимое преобразование и маршрутизацию этих данных между разными уровнями, а также "обратную связь" между сервисами каждого отдельного уровня.

При формировании функциональных подсистем АСУ СН наиболее важным становится принцип, при котором каждый процесс должен автоматизироваться однократно, вне зависимости от принадлежности к виду и уровню управления. Для обеспечения специфики вида деятельности, налагаемой видовой принадлежностью или уровнем управления, необходимо обеспечить широкие возможности настройки ПО (по видам и источникам информации, применяемым информационно-расчетным задачам, УФД и т.д.).

В настоящее время в силах специального назначения на вооружении находится множество систем и комплексов, с той или иной степенью эффективности решающих различные задачи управления силами и средствами СН. Однако имеет место большая избыточность поступающих данных, сложность, а зачастую и невозможность организации взаимодействия и оперативной совместимости различных систем, а также несовершенство механизма распределения конечных результатов.

С технической точки зрения причиной изолированности систем и комплексов является излишнее разнообразие аппаратных и программных средств, платформ, архитектур и технологий, различие интерфейсов и протоколов, а также отсутствие изначально заложенных механизмов взаимодействия систем.

Необходима разработка и внедрение аппаратно-программных средств, обеспечивающих комплексирование информации от разнородных источников, автоматизацию процессов обработки и интерпретации поступающей информации, а также формирование общей базы данных с распределенным доступом к ней, что позволит создать единое информационное пространство, снизить избыточность поступающей информации, повысить качество ее представления, скорость поиска данных и их доведения до конечного пользователя.

Предусмотреть возможность эффективно-го решения сложных вычислительных задач, обеспечения взаимодействия программных

комплексов и систем путем организации распределенных вычислений в сетях на основе рационального использования сетевых ресурсов — процессоров, памяти, коммуникационного оборудования, алгоритмов и программ.

Функциональные подсистемы (ФПС) АСУ, должны быть определены как наборы унифицированных и не унифицированных программных компонентов — Функциональных сервисов, способных работать совместно, в соответствии с установленным формализованным регламентом деятельности. Функциональные подсистемы рассматриваются, как совокупности слабо связанных Функциональных сервисов, применяемый набор которых определяется задачами по управлению АСУ.

Инфраструктурные системы (ИС) обеспечивают предоставление функционально независимых услуг абонентам и элементам АСУ. Инфраструктурные системы должны рассматриваться как наборы Инфраструктурных сервисов, предназначенные для реализации технологической основы для Функциональных сервисов. Инфраструктурные сервисы должны предоставлять возможности функциональным подсистемам реализовывать свое назначение путем манипулирования набором применяемых Инфраструктурных систем и использования их функциональных возможностей. Инфраструктурные сервисы скрывают техническую реализацию от Функциональных сервисов, а специфицирование (описание и следование описанию) интерфейсов обеспечивает необходимую гибкость, возможности масштабирования, а также постепенного улучшения и наращивания функциональности подсистемы, путем замены реализации Инфраструктурного сервиса, без необходимости внесения изменений в Функциональную подсистему.

Обеспечение информационно-технического взаимодействия АСУ со сторонними (существующими, унаследованными) системами производится путем их интеграции в единую распределенную среду информационного взаимодействия через унифицированный механизм адаптеров. Далее этот механизм может быть применен как способ интеграции в АСУ СН.

Рабочее пространство пользователя (РПП) должно обеспечивать единую рабочую область для всех Функциональных подсистем, ко-

которые использует пользователь в рамках своей деятельности. Использование Рабочего пространства пользователя должно обеспечить преимущество сквозной идентификации пользователя для различных Функциональных подсистем, при выполнении всех функций АРМ, применяемых пользователем в рамках единой рабочей области. Для полного и эффективного взаимодействия пользователя с АСУ необходимо реализовать РПП на основе концепции "толстого" клиента. Для простого взаимодействия пользователя с АСУ и улучшения мобильности пользователя необходимо реализовать РПП на основе концепции "тонкого" клиента.

Реализация указанных направлений развития системы управления сил СН позволит:

— обеспечить планируемое повышение эффективности средств поражения до требуемых показателей;

— обеспечить создание системы разведки и контроля, позволяющую контролировать 100% зон ответственности;

— обеспечить автоматизированное решение 100% задач управления силами СН с высоким качеством реализации циклов управления силами.

Очевидно, что создаваемая система должна иметь открытую архитектуру и обеспечивать возможность оперативной адаптации к изменениям состава и структуры сил СН в целом и отдельных группировок, в частности, в том числе и оперативных формируемых на отдельных направлениях.

Литература

1. Трушин В.В. О сущности взаимодействия войск в операции (бою) // Военная мысль. — 2007. — № 4. — С. 16-18.

2. Шеремет И.В. "Сетецентрическая война": истоки и технические аспекты // Военно-промышленный курьер. — 2006. — № 7. — С. 22-24.

3. Легков К.Е. Сравнительная характеристика различных протоколов управления // Научные технологии в космических исследованиях Земли, 2010. — №1. — С.27-31.

XIII Международный конгресс «Инновационная экономика и качество управления»

14 апреля 2011 г.,
«Президент-Отель»
(Москва, ул. Б. Якиманка, 24)

15 апреля 2011 г.,
НИИ «Интерэкомс»
(Москва, ул. Народного Ополчения, 32)

Тематика конгресса:

- ◆ Совершенствование законодательного обеспечения инновационной и инвестиционной политики.
- ◆ Анализ современных проблем эффективного функционирования систем управления, информационных систем, электронного правительства.
- ◆ Вопросы соответствия систем управления и информационных систем международным стандартам.
- ◆ Повышение эффективности корпоративного и государственного управления.
- ◆ Обеспечение безопасности информационного общества.
- ◆ Эффективность применения инфокоммуникационных технологий в сфере управления в различных секторах экономики.

Методика оптимальной аппроксимации заданного распределения вероятности простейшим показательным распределением

Обоснована методика оптимальной аппроксимации заданного распределения вероятности простейшим показательным распределением, выполнен анализ сходимости полученной аппроксимации

Ключевые слова: Аппроксимация, плотность вероятности, критерий, негауссовская помеха.

Данилов А.В., Малышко А.В.,
Северо-Кавказский филиал
Московского технического
университета связи и информатики,
г. Ростов-на-Дону

Technique of optimum approximation of the given distribution of probability the elementary demonstrative distribution

Danilov A.V., Malysheko A.V.,
North-Caucasian branch of the Moscow
technical university relationship
and informatics

Abstract

The optimal approximation method of a given probabilities distribution by a simplified exponential distribution is proved, the convergence analysis of received approximation is performed.

Keywords: Approximation, probability density, criteria, nongaussian noise.

При решении задач статистической радиотехники, связанных с негауссовскими входными воздействиями, иногда возникает необходимость в вероятностном описании помеховых сигналов простыми аналитическими функциями. Такие задачи возникают, например, при построении приёмных устройств, адаптивных к распределению негауссовских помех, воздействующих на входе приёмника.

Исчерпывающей характеристикой негауссовской помехи с независимыми выборочными значениями является одномерная плотность вероятности (ПВ) $w_1(x)$. Помимо этой функции, можно также рассматривать связанную с ней характеристическую функцию $Q_1(v)$ — преобразование по Фурье данной плотности.

Описание помехового сигнала с помощью функций $w_1(x)$, $Q_1(v)$ характерно для негауссовского случайного процесса с широкополосным спектром. Если помеховое колебание является узкополосным случайным процессом (УСП), то вместо этих функций целесообразно задавать распределение огибающей $W(A)$, $A \geq 0$, связанное с функцией $Q_1(v)$ интегральным соотношением вида:

$$W(A)/A = \int_0^{\infty} Q_1(x) J_0(A \cdot x) x dx, \quad (1)$$

где $J_0(z)$ — функция Бесселя нулевого порядка.

Распределение $W(A)$ для большинства помеховых сигналов представляется сложной аналитической функцией, зависящей от некоторого параметра. Для построения приёмного устройства адаптивного к распределению помехового сигнала, требуется аппроксимировать реальную ПВ некоторой простой аналитической функцией $W_a(A)$, представляемой че-

рез элементарные функции. Особенно это важно в том случае, когда распределение реальных радиопомех неизвестно, и в процессе приёма требуется аппроксимировать неизвестную ПВ с помощью эмпирических моментов, получаемых на основании данных выборки.

Цель работы — обоснование методики оптимальной аппроксимации заданного распределения вероятностей простейшим показательным распределением; анализ сходимости полученной аппроксимации применительно к негауссовским помехам синусоидального типа; сопоставительный анализ двух видов аппроксимации с использованием ПВ $w_1(x)$ и $W(A)$.

Как уже отмечалось, основной характеристикой негауссовского УСП является функция $W(A)$. Будем считать, что эта функция непрерывна и дифференцируема на всей числовой оси ($A \geq 0$). Этим условиям удовлетворяют распределения реальных радиопомех.

В силу аналитичности заданного распределения его можно представить в форме показательной функции:

$$W(A)/A = C_1 \exp\left(-\sum_{k=1}^{\infty} \frac{a_k}{k} A^k\right), \quad (2)$$

где $C_1 > 0$ — нормировочная константа; коэффициенты полинома определяются как:

$$a_k = -\frac{1}{(k-1)!} \frac{d^k}{dA^k} \ln \left[\frac{W(A)}{A} \right], \quad (3)$$

Для построения приёмного устройства, адаптивного к ПВ $W(A)$, желательно ограничить сумму в показателе (2). Распределение вида

$$W_a(A)/A = C_a \exp\left(-\sum_{k=1}^n \frac{b_k}{k} A^k\right), \quad (4)$$

где $n \geq 1$ - целое число; C_a - нормировочная константа; при $b_k = a_k$ в общем случае не является лучшим приближением к (2). Существуют такие значения параметров $b_k = b_k^*$, не обязательно совпадающие с a_k , при которых распределение (4) наилучшим образом приближается к (2). Найдём связь параметров b_k^* с распределением (2).

За критерий наилучшего приближения $W_a(A)$ к $W(A)$ примем условие минимума ошибок приёма, соответствующих устройству, оптимальному к распределению $W_a(A)$, в условиях воздействия помехи с распределением $W(A)$. Для случая обнаружения слабых сигналов в когерентном полосовом тракте выбранный критерий совпадает с условием максимума параметра:

$$\mu_a = \frac{1}{2} m_2 \frac{\left\langle \frac{g_a(A)}{A} + \frac{dg_a(A)}{dA} \right\rangle^2}{\langle g_a^2(A) \rangle}, \quad (5)$$

где

$$g_a = -\frac{d}{dA} \ln \left[\frac{W_a(A)}{A} \right]; \quad (6)$$

m_2 - дисперсия помехи; угловые скобки $\langle \bullet \rangle$ - означают статистическое усреднение с учётом функции $W(A)$.

Коэффициент μ_a из (5) зависит от параметров (b_1, b_2, \dots, b_n) аппроксимации (4) и от моментов распределения (2). Определим параметры $b_k = b_k^*$, при которых коэффициент (5) достигает максимального значения. С этой целью представим выражение (5) с учётом (4), (6) в таком виде:

$$\mu_a = \frac{1}{4} M_2 \frac{\left(\sum_{k=1}^n k b_k M_{k-2} \right)^2}{\sum_{k,m=1}^n b_k b_m M_{k+m-2}}, \quad (7)$$

где

$$M_k = \int_0^\infty A^k W(A) dA \quad (8)$$

начальные моменты распределения $W(A)$ и при этом $M_2 = 2m_2$.

Из формулы (7) вытекает что параметр $\mu_a = \mu_a(\vec{b}, \vec{M})$ является функцией вектора $\vec{b} = (b_1, b_2, \dots, b_n)$ параметров аппроксимации

и вектора моментов распределения $W(A)$: $\vec{M} = (M_{-1}, M_0, M_1, M_2, \dots, M_{n-2})$.

Оптимальные коэффициенты аппроксимации $(b_1^*, b_2^*, \dots, b_n^*)$, удовлетворяющие условию $\mu_a(b_1^*, b_2^*, \dots, b_n^*) = \max \mu_a(b_1^*, b_2^*, \dots, b_n^*)$,

определяются по формуле:

$$b_k^* = B \cdot \det \|v_{rl}(k)\|, \quad B > 0, \quad (9)$$

где

$$v_{rl}(k) = \begin{cases} M_{r+l-2}, & l \neq k, \\ r M_{r-2}, & l = k, \end{cases} \quad (10)$$

$(r, l, k = 1, 2, 3, \dots, n)$

Величину коэффициента (7) при оптимальных значениях параметров (9) аппроксимации следует определять по формуле:

$$\max \mu_a = \mu_a(b_1^*, b_2^*, \dots, b_n^*) = \frac{M_2}{4 D_n} \sum_{k=1}^n k b_k^* M_{k-2}, \quad (11)$$

где D_n - определитель n -го порядка, составленный из элементов вида $v_{rl} = M_{r+l-2}$, $(r, l = 1, 2, \dots, n)$.

Отметим, что оптимальные значения коэффициентов b_k^* аппроксимации (4) могут быть получены из определителя D_n путём замены в нём k -го столбца значениями $\{ M_{-1}, 2M_0, 3M_1, \dots, nM_{n-2} \}$ из (10) в соответствии с выражением (9). Параметры b_k^* определяются из (9) с точностью до некоторой постоянной величины B . С целью однозначности аппроксимации B можно определить из условия равенства каких-либо моментов распределения, например, их дисперсий:

$$\frac{1}{2} C_a \int_0^\infty A^3 \exp \left(-\sum_{k=1}^n \frac{b_k^*}{k} A^k \right) dA = m_2.$$

Рассмотрим более подробно оптимальную аппроксимацию функцией (4) при $n = 2$. В этом случае аппроксимирующая функция примет вид

$$W(A)/A = C_a \exp \left(-b_1^* A - \frac{1}{2} b_2^* A^2 \right).$$

Оптимальные коэффициенты b_1^* , b_2^* функции (12) на основании (9) равны:

$$\left. \begin{aligned} b_1^* &= B(M_{-1}M_2 - 2M_0M_1) \\ b_2^* &= B(2M_0^2 - M_1M_{-1}) \end{aligned} \right\}, \quad (13)$$

где величина $M_0 = 1$ определяется на основании (8). Для записи коэффициен-

та (11) в этом случае запишем сначала выражение определителя

$$D_2 = \begin{vmatrix} M_0 & M_1 \\ M_1 & M_2 \end{vmatrix} = M_2 - M_1^2. \quad (14)$$

С учётом (13), (14), коэффициент (11) представляется в виде:

$$\begin{aligned} \max \mu_a &= \mu_a(b_1^*, b_2^*) = \\ &= \left(1 - M_1M_{-1} + \frac{1}{4} M_2^2 M_2 \right) / \left(1 - M_1^2 / M_2 \right). \end{aligned}$$

Таким образом, величина (15) численно определяет меру отличия функции $W_a(A)$ вида (4) от заданной плотности $W(A)$ при $n = 2$.

Значение (15) в точности соответствует аналогичному коэффициенту, полученному в работе. В данной работе рассматривалась возможность кусочно-линейной аппроксимации характеристики нелинейного преобразования в схеме амплитудного подавления негауссовской помехи со спектром полосового типа.

Рассмотрим погрешность аппроксимации (4) при $b_k = b_k^*$ на примерах. Для гауссовского случайного процесса с распределением огибающей по закону Релея [1]

$$W(A) = \frac{A}{\sigma^2} \exp \left(-\frac{A^2}{2\sigma^2} \right)$$

из (9), (10) получаем

$$b_k^* = \begin{cases} 2 \frac{B \cdot D_n}{M_2}, & k = 2, \\ 0, & k \neq 2; B = 1, \end{cases}$$

и в этом случае $W_a(A) = W(A)$ при всех A . Принимая во внимание выражения для моментов релеевского закона $M_{-1} = \sqrt{\pi/2}\sigma^{-1}$; $M_1 = \sqrt{\pi/2}\sigma$; $M_2 = 2\sigma^2$, с помощью (15) находим $\max \mu_a = B = 1$, что совпадает с предельным значением μ_a при $W_a(A) = W(A)$.

В качестве второго примера рассмотрим аналогичные вычисления для плотности вероятности вида

$$W(A) = \frac{3}{\sigma^2} A \exp \left(-\frac{\sqrt{3}}{\sigma} A \right),$$

которая определена в работе [3] как распределение предельного типа. Данная ПВ названа предельной так как для этой плотности характеристика нелинейного преобразователя в схеме амплитудного подавления [2] вырождается в «жесткий» ограничитель. Выполняя аналогичные вычисления с применением (9), (10), получаем

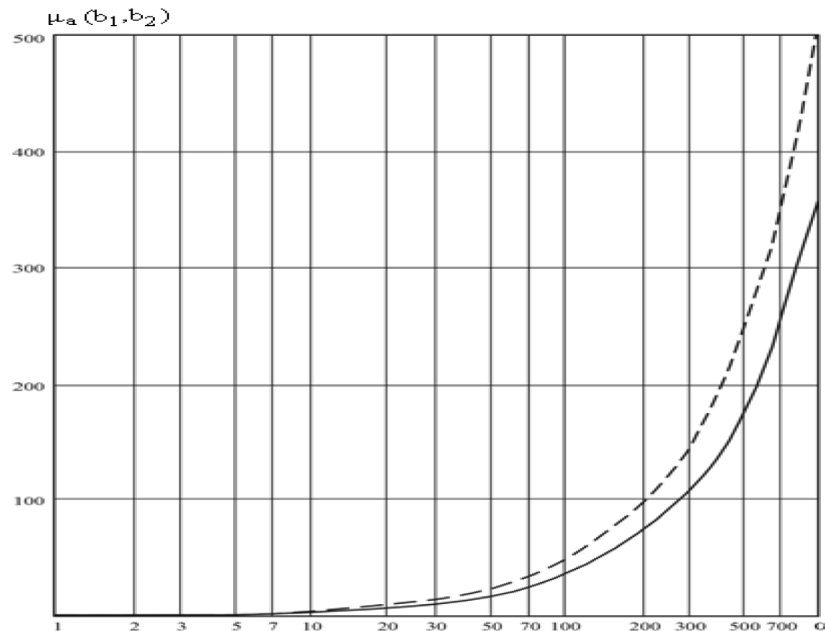


Рис. 1. Показатели качества аппроксимации для синусоидальной помехи

$$b_k^* = \begin{cases} \frac{B \cdot D_n}{M_1}, & k=1, \\ 0, & k \geq 1; B=1, \end{cases}$$

и в этом случае также $W_a(A) = W(A)$ при всех A . С помощью (15) находим $\max \mu_a = 3/2$, что совпадает с предельным значением при $W_a(A) = W(A)$. Отметим, что оба рассмотренных примера входят в состав простейшей аппроксимации (12) при $n = 2$. Для других негауссовских распределений равенство $W_a(A) = W(A)$ не выполняется.

В качестве примера аппроксимации более сложной функции рассмотрим распределение огибающей суммы ЧМ – процесса и гауссовского шума. В этом случае распределение огибающей подчиняется обобщенному закону Релея и имеет вид [1]:

$$W(A) = 2\alpha A \exp[-\alpha(A^2 + 1)] I_0(2\alpha A), \quad (16)$$

где α – параметр распределения, равный отношению мощности ЧМ – процесса к мощности гауссовского шума; $I_k(z)$ – модифицированная функция Бесселя порядка k .

Для расчёта характеристики $\max \mu_a$ по формуле (15) запишем требуемые выражения моментных функций, соответствующих (16)

$$M_{-1} = \sqrt{\pi\alpha} I_0(\alpha/2) e^{-\alpha/2},$$

$$M_1 = \frac{1}{2} \sqrt{\frac{\pi}{2}} \left[(1+\alpha) I_0\left(\frac{\alpha}{2}\right) + \alpha I_1\left(\frac{\alpha}{2}\right) \right] e^{-\alpha/2},$$

$$M_2 = (1+\alpha)/\alpha,$$

На рисунке 1 даны зависимости показателей качества аппроксимации $\max \mu_a$ от параметра распределения (16). Пунктирной кривой представлена зависимость предельного значения коэффициента (5) при $W_a(A) = W(A)$. Эти данные рассчитывались по формуле [2]

$$\mu_{p_0} = \frac{1}{2} m_2 \int_0^\infty \left(\frac{d}{dA} \ln \left[\frac{W(A)}{A} \right] \right)^2 W(A) dA, \text{ с}$$

учётом применения распределения (16). Сплошная кривая на рис. 1 соответствует аппроксимирующей функции (4) при $n = 2$. Данные этой кривой рассчитывались по формуле (15) с использованием моментных функций (17). Графики на этом рисунке подтверждают возможность достаточно точной аппроксимации распределений реальных радиопомех функций плотности (4) при двух членах в показателе $W_a(A)$.

Заключение

В результате проведенного анализа можно заключить, что применение экспоненциальной аппроксимации для

функции $W(A)$ обеспечивает приемлемые результаты уже при двух членах суммы в показателе. Данная двухчленная аппроксимация позволяет сравнительно просто описывать реальные функции $W(A)$, что очень удобно при анализе каналов амплитудного подавления, работающих в адаптивном режиме.

Также приведен сопоставительный анализ экспоненциальной аппроксимации для функций $w_1(x)$ и $W(A)$. Показано, что аппроксимация для $W(A)$ обеспечивает лучшую сходимость результата и является более адекватной для многих реальных ситуаций.

Литература

1. Тихонов В.И. Статистическая радиотехника. – М.: Радио и связь, 1982.
2. Акимов П.С., Бакут П.А., Богданович В.А. и др. Теория обнаружения сигналов / Под ред. П.А. Бакута. – М.: Радио и связь, 1984.
3. Данилов А.В., Жабинский Ю.В. Негауссовские распределения предельного типа // Сб. трудов НТК СКФ МТУСИ "Инфоком – 2010", Ростов-на-Дону, 2010.
4. Данилов В.А. Радиотехника, 1998, №2.
5. Градштейн И.С., Рыжик И.М. Таблицы интегралов, сумм, рядов и производений. – М.: Наука, 1971.
6. Данилов В.А. Радиотехника и электроника, 1984, Т.29, №9.

Кумулянтный метод определения закона распределения

Разработан новый кумулянтный метод определения закона распределения, позволяющий полностью автоматизировать процесс определения вида закона распределения результатов измерений. Правильность гипотезы может быть проверена в дальнейшем с помощью известных критериев, например Колмогорова или Стьюдента. Приведен пример реализации метода.

Ключевые слова: кумулянтный метод, закон распределения, моменты случайных величин, кумулянты случайных величин.

Безуглов Д.А., Швидченко С.А.,
Ростовский технологический институт
сервиса и туризма ЮРГУЭС
Северо-Кавказский филиал
Московского технического
университета связи и информатики

Cumulant method of determination of the distribution law

Bezuglov D.A., Shvidchenko S.A.,
Rostov Institute of Technology Service and
Tourism of the State educational institution
of higher professional education "South-
Russia State University of Economics and
Service" North-Caucasian branch of the
Moscow technical university relationship
and informatics

Abstract

A new Cumulant method for determining the distribution law, which allows to fully automate the process of determining the form of the distribution of measurement results. The correctness of the hypothesis can be tested further by using the known criteria, such as Kolmogorov or Student. An example of the method.

Keywords: Cumulant method, distribution law, moments of random variables, cumulants of random variables.

Под задачей идентификации закона распределения наблюдаемой случайной величины понимается нахождение такого закона, который бы в статистическом смысле не противоречил имеющимся наблюдениям. Практика использования нормального закона распределения для описания ошибок средств измерения, как выясняется [1, 5], не всегда оправдана. В основе измерительных приборов и систем лежат различные физические принципы, различные методы измерений и различные преобразования измерительных сигналов. Погрешности измерений являются следствием влияния множества факторов, случайного и неслучайного характера, действующих постоянно или эпизодически. Поэтому понятно, что только при выполнении определенных предпосылок (теоретических и технических) погрешности измерений достаточно хорошо описываются нормальным законом распределения.

При автоматизации обработки результатов измерений рассматривается задача идентификации закона распределения случайных величин, которая обычно решается с применением статистических критериев согласия Пирсона, Колмогорова, Колмогорова-Смирнова, омега-квадрат. Задача выбора закона распределения для данной выборки значений случайной величины решается в этом случае как задача приближения функции на заданных аналитических законах распределений. В качестве закона распределения выбирается такое распределение, которое находится на минимальном расстоянии (в качестве которого может быть выбрана статистика Пирсона, Колмогорова и др.) от эмпирического закона распределения, построенного по соответствующей выборке. Выбор числовых параметров законов распределений выполняется на основе обработки всех данных единственной выборки случайной величины, в то время как при использовании

критериев согласия параметры требуется определять по иной выборке значений случайной величины.

Однако недостатком всех рассмотренных выше подходов является то, что гипотеза о виде распределения определяется эмпирически. То есть исследователь должен по виду полученной функции распределения вероятностей - эмпирической функции распределения или гистограммы, исходя из своего опыта, определить теоретический закон, которым она описывается.

Целью данной работы является разработка кумулянтного метода идентификации вида закона распределения на базе анализа результатов измерений. В дальнейшем правильность гипотезы может быть проверена с помощью известных критериев, например Колмогорова или Стьюдента.

1. Кумулянтный анализ

Кумулянтное описание случайных величин дает столь же полное их статистическое представление, сколь и моментное, оно обладает, вместе с тем, важными и привлекательными преимуществами [3]. Первое преимущество заключается в том, что кумулянты, в отличие от моментов имеют четко выраженный самостоятельный статистический смысл и могут быть заданы в определенной степени независимо друг от друга, являясь в этом плане некоторыми "нормальными координатами" статистического описания. Это приводит, например, к тому, что различные статистические средние "выходов" нелинейных преобразований выражаются простым образом именно через кумулянты "входных" переменных [3, 5].

Второе преимущество кумулянтов связано с тем, что учет их высших порядков позволяет просто описать любую степень негауссовости случайных величин. По этой причине основную ценность кумулянтное описание имеет именно для негауссовых переменных [2,5].

Третье преимущество кумулянтного описания случайных величин обусловлено тем, что конечному набору кумулянтов всегда соответствует некоторая вещественная функция, аппроксимирующая вероятностное распределение. Это обстоятельство имеет особо важное значение при приближенном представлении вероятностных распределений тех случайных величин, для которых можно отыскать лишь конечные наборы кумулянтов [5].

2. Кумулянтный метод анализа результатов измерений

Рассмотрим сущность предлагаемого метода. Характеристическую функцию можно записать в виде $\Theta(u) = \exp(\beta(u))$, где, очевидно, должно быть $\beta(0) = 0$. Разложим функцию $\beta(u)$ в степенной ряд [3]:

$$\beta(u) = \ln \Theta(u) = \sum_{k=1}^{\infty} \frac{\chi_k}{k!} (ju)^k. \quad (1)$$

Коэффициенты этого ряда:

$$\chi_k = j^{-k} \beta^{(k)}(0) = j^{-k} \left[\frac{d^k \ln \Theta(u)}{du^k} \right]_{u=0} \quad (2)$$

так же, как и моменты, являются характеристиками распределения и носят название кумулянтов или семиинвариантов. Таким образом, характеристическую функцию можно представить в виде:

$$\Theta(u) = \exp \left[\sum_{k=1}^{\infty} \frac{\chi_k}{k!} (ju)^k \right]. \quad (3)$$

Кумулянты однозначно определяют случайную величину, если ряд (3) сходится для всех u . Поэтому набор кумулянтов $\chi_1, \chi_2, \chi_3, \dots, \chi_s$, также может служить тождественным представлением закона распределения.

Если известны моменты α_j^i , то кумулянты могут быть найдены из следующих соотношений [4,5]:

$$\begin{aligned} \chi_1^i &= \alpha_1^i = m; \quad \chi_2^i = \alpha_2^i - (\alpha_1^i)^2 = D; \\ \chi_3^i &= \alpha_3^i - 3\alpha_1^i \alpha_2^i + (2\alpha_1^i)^3; \\ \chi_4^i &= \alpha_4^i - 3(\alpha_2^i)^2 - 4\alpha_1^i \alpha_3^i + 12(\alpha_1^i)^2 \alpha_2^i - 6(\alpha_1^i)^4; \\ \chi_5^i &= \alpha_5^i - 5\alpha_1^i \alpha_4^i - 10\alpha_2^i \alpha_3^i + 20(\alpha_1^i)^2 \alpha_3^i + \\ &+ 30\alpha_1^i (\alpha_2^i)^2 - 60(\alpha_1^i)^3 \alpha_2^i + 24(\alpha_1^i)^5; \\ \chi_6^i &= \alpha_6^i - 6\alpha_1^i \alpha_5^i - 15\alpha_2^i \alpha_4^i + 30(\alpha_1^i)^2 \alpha_4^i - 10(\alpha_2^i)^3 + \\ &+ 120\alpha_1^i \alpha_2^i \alpha_3^i - 120(\alpha_1^i)^3 \alpha_3^i + 30(\alpha_1^i)^3 \alpha_2^i - 270(\alpha_1^i)^2 (\alpha_2^i)^2 + \\ &+ 360(\alpha_1^i)^4 \alpha_2^i - 120(\alpha_1^i)^6. \end{aligned} \quad (4)$$

Верхним индексом i в дальнейшем будем обозначать принадлежность моментов и кумулянтов к тому или иному распределению. В выражении (4) мы использовали только шесть первых кумулянтов. Это связано с тем, что как показали проведенные авторами исследования на различных выборках, такого количества кумулянтов достаточно для раскрытия сущности предложенного подхода. Однако при алгоритмической реализации предложенного метода число кумулянтов может быть увеличено.

В аналитическом виде моменты распределений могут быть вычислены через производящую функцию. Рассмотрим для примера выражения для моментов гауссовского, равномерного и экспоненциального законов распределения. В дальнейшем эти выражения мы используем для подстановки в (4) и определения кумулянтов соответствующих распределений.

Пусть имеется случайная величина X с распределением $P(x)$. Тогда её производящей функцией моментов называется функция, имеющая вид:

$$M_X(t) = E[e^{tx}] = \int_{-\infty}^{\infty} P(x) e^{tx} dx, \quad (5)$$

где $E[*]$ – оператор математического ожидания.

Моменты случайной величины вычисляются через производящую функцию следующим образом [4]:

$$E[X^n] = \frac{d^n}{dt^n} M_X(t) \Big|_{t=0}. \quad (6)$$

Для закона Гаусса с распределением

$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right), \quad (7)$$

производящая функция моментов будет иметь вид:

$$M_X(t) = \exp\left(\mu t + \frac{\sigma^2 t^2}{2}\right). \quad (8)$$

Соответственно, моменты могут быть вычислены в соответствии со следующими выражениями:

$$\begin{aligned} \alpha^e_1 &= m = \mu; \quad \alpha^e_2 = \mu^2 + \sigma^2; \\ \alpha^e_3 &= \mu^3 + 3\mu\sigma^2; \\ \alpha^e_4 &= \mu^4 + 6\mu^2\sigma^2 + 3\sigma^4; \\ \alpha^e_5 &= \mu^5 + 10\mu^3\sigma^2 + 15\mu\sigma^4; \\ \alpha^e_6 &= \mu^6 + 15\mu^4\sigma^2 + 45\mu^2\sigma^4 + 15\sigma^6. \end{aligned} \quad (9)$$

Для равномерного закона с распределением

$$P(x) = \begin{cases} \frac{1}{b-a}, & a \leq x \leq b; \\ 0, & x < a, \quad x > b. \end{cases} \quad (10)$$

производящая функция моментов будет иметь вид:

$$\begin{aligned} M_X(t) &= \frac{1}{t(b-a)} (e^{bt} - e^{at}), \\ E[X^n] &= \frac{d^n}{dt^n} M_X(0) = \frac{1}{n+1} \sum_{k=0}^n a^k b^{n-k}. \end{aligned} \quad (11)$$

Соответственно, моменты могут быть найдены из следующих выражений:

$$\begin{aligned} \alpha^{p_1} &= m = \frac{1}{2}(a+b); \\ \alpha^{p_2} &= \frac{1}{3}(a^2 + ab + b^2); \\ \alpha^{p_3} &= \frac{1}{4}(a^3 + a^2b + ab^2 + b^3); \\ \alpha^{p_4} &= \frac{1}{5}(a^4 + a^3b + a^2b^2 + ab^3 + b^4); \\ \alpha^{p_5} &= \frac{1}{6}(a^5 + a^4b + a^3b^2 + a^2b^3 + ab^4 + b^5); \\ \alpha^{p_6} &= \frac{1}{7}(a^6 + a^5b + a^4b^2 + a^3b^3 + a^2b^4 + ab^5 + b^6) \end{aligned} \quad (12)$$

Для экспоненциального закона с распределением

$$P(x) = \lambda e^{-\lambda x} \quad (13)$$

производящая функция моментов будет иметь вид:

$$M_X(t) = \left(1 - \frac{t}{\lambda}\right)^{-1}. \quad (14)$$

Соответственно, моменты могут быть найдены из следующих выражений:

$$\begin{aligned} \alpha^e_1 &= m = \lambda^{-1}; \quad \alpha^e_2 = \frac{2}{\lambda^2}; \\ \alpha^e_3 &= \frac{6}{\lambda^3}; \quad \alpha^e_4 = \frac{24}{\lambda^4}; \quad \alpha^e_5 = \frac{120}{\lambda^5}; \\ \alpha^e_6 &= \frac{720}{\lambda^6}. \end{aligned} \quad (15)$$

Для набора распределений вычисляются с использованием выражений (4), (9), (12), (15) теоретические значения кумулянтов. При этом при автоматизации предложенного подхода количество видов используемых распределений может быть значительно увеличено, и ограничивается лишь рамками решаемой при этом метрологической задачи.

Пусть имеются результаты измерений Y_m . Эмпирические моменты α_j^i могут быть найдены на основе обработки входной реализации:

$$\alpha_1^{i1} = \frac{\sum_{m=0}^{l-1} Y_m}{l}; \alpha_2^{i2} = \frac{\sum_{m=0}^{l-1} Y_m^2}{l-1};$$

$$\alpha_3^{i3} = \frac{l \sum_{m=0}^{l-1} Y_m^3}{(l-1)(l-2)};$$

$$\alpha_4^{i4} = \frac{l^2 \sum_{m=0}^{l-1} Y_m^4}{(l-1)(l-2)(l-3)};$$

$$\alpha_5^{i5} = \frac{l^3 \sum_{m=0}^{l-1} Y_m^5}{(l-1)(l-2)(l-3)(l-4)};$$

$$\alpha_6^{i6} = \frac{l^4 \sum_{m=0}^{l-1} Y_m^6}{(l-1)(l-2)(l-3)(l-4)(l-5)}, \quad (16)$$

где: l – размерность выборки, α_j^i – эмпирический момент j -го порядка i -го закона распределения.

По ним в соответствии с выражением (4) определяются эмпирические значения кумулянтов. При этом необходимо обеспечить нормировку по второму кумулянту.

В данном случае критерием «близости» исследуемого распределения к тому или иному виду может служить следующее выражение:

$$S_i = \min_i \sum_{j=1}^6 (\chi_j^i - \chi_j^{\text{э}i})^2,$$

где: i – вид распределения, $l=1, 2, 3$, χ_j^i – кумулянты, рассчитанные аналитически, $\chi_j^{\text{э}i}$ – кумулянты, рассчитанные эмпирически.

Предлагаемый метод может быть реализован, как это показано на рис. 1.

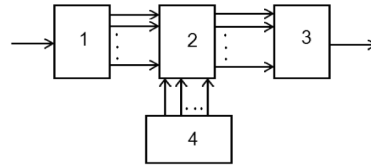


Рис. 1. 1 – блок вычисления эмпирических значений кумулянтов; 2 – блок вычисления значений критерия S; 3 – блок анализа и определения вида закона распределения; 4 – блок вычисления (хранения) аналитических значений кумулянтов

3. Пример

Для проверки метода был проведен вычислительный эксперимент. При этом использовался математический пакет Mathcad 14. Суть эксперимента состоит в следующем: с помощью датчиков случайных чисел генерировались реализации случайных чисел, распределенных по гауссовскому, равномерному и экспоненциальному законам распределения. При проведении вычислительного эксперимента размер выборки был $l = 2^{17}$. Сначала вычислялись теоретические значения кумулянтов в соответствии с выражениями (4), (9), (12), (15) При этом в качестве параметров законов распределений были выбраны следующие: для распределения Гаусса и равномерного распределения математическое ожидание $m = 0$, дисперсия $D = 1$, для экспоненциального

распределения $\lambda = 1$. Затем вычислялись значения эмпирических моментов в соответствии с выражениями (16), и значения эмпирических кумулянтов в соответствии с выражениями (4). Результаты сведены в таблицу 1.

Для каждого набора теоретических и эмпирических кумулянтов по формуле (17) вычислялись значения критерия S_i , которые сведены в таблицу 2.

Таблица 2

Значения критериев S_i для различных законов распределений

Распределение	S_1	S_2	S_3
Гаусса	$S_{1r}=0,0024$	$S_{2r}=0,55$	$S_{3r}=15028,65$
Равномерное	$S_{1p}=48,54$	$S_{2p}=0,0006$	$S_{3p}=13433,7$
Экспоненциальное	$S_{1e}=15477,09$	$S_{2e}=15417,43$	$S_{3e}=3,99$

Рассмотрим подробно алгоритм расчета первой строки таблицы 2. Каждая строка таблицы рассчитывалась следующим образом. В первой строке мы анализируем выборку, сгенерированную датчиком случайных чисел, распределенных по гауссовскому закону распределения. Расчет ведем в соответствии со следующими выражениями, при этом используем результаты расчета теоретических и эмпирических значений кумулянтов для гауссовского, равномерного и экспоненциального законов распределения из таблицы 1.

Таблица 1

Значения кумулянтов

Закон распределения		χ_1	χ_2	χ_3	χ_4	χ_5	χ_6
Гауссовский	Теоретические	$\chi_1^g = 0$	$\chi_2^g = 1$	$\chi_3^g = 0$	$\chi_4^g = 0$	$\chi_5^g = 0$	$\chi_6^g = 0$
	Эмпирические	$\chi_1^{g\text{э}} = -0,00071$	$\chi_2^{g\text{э}} = 1,0011$	$\chi_3^{g\text{э}} = -0,011$	$\chi_4^{g\text{э}} = 0,00082$	$\chi_5^{g\text{э}} = -0,0069$	$\chi_6^{g\text{э}} = -0,047$
Равномерный	Теоретические	$\chi_1^p = 0$	$\chi_2^p = 1$	$\chi_3^p = 0$	$\chi_4^p = -1,2$	$\chi_5^p = 0$	$\chi_6^p = 6,88$
	Эмпирические	$\chi_1^{p\text{э}} = -0,00074$	$\chi_2^{p\text{э}} = 1,011$	$\chi_3^{p\text{э}} = 0,0021$	$\chi_4^{p\text{э}} = -1,2$	$\chi_5^{p\text{э}} = -0,013$	$\chi_6^{p\text{э}} = 6,86$
Экспоненциальный	Теоретические	$\chi_1^e = 1$	$\chi_2^e = 1$	$\chi_3^e = 2$	$\chi_4^e = 6$	$\chi_5^e = 24$	$\chi_6^e = 120$
	Эмпирические	$\chi_1^{e\text{э}} = 0,99$	$\chi_2^{e\text{э}} = 0,99$	$\chi_3^{e\text{э}} = 2,011$	$\chi_4^{e\text{э}} = 6,11$	$\chi_5^{e\text{э}} = 25,024$	$\chi_6^{e\text{э}} = 121,69$

$$\begin{aligned}
 S_{1z} &= \sum_{j=1}^6 (\chi_j^z - \chi_j^{z2})^2; \\
 S_{2z} &= \sum_{j=1}^6 (\chi_j^p - \chi_j^{z2})^2; \\
 S_{3z} &= \sum_{j=1}^6 (\chi_j^3 - \chi_j^{z2})^2; \quad (18)
 \end{aligned}$$

Аналогичным образом рассчитаны остальные строки табл. 2. Из приведенной табл. 2 видно что, для первого эксперимента наименьшее значение критерия S_{1z} соответствует распределению Гаусса. Для второго эксперимента наименьшее значение критерия S_{2z} соответствует равномерному распределению, для третьего – наименьшее значение критерия S_{3z} – экспоненциальному распределению.

Заключение

Проведя вычисления по формулам (4), (9), (12), (15), (17) можно определить вид закона распределения, которым описывается выборка результатов измерений Y_m . Разработан новый кумулянтный метод определения вида закона распределения, позволяющий полностью автоматизировать процесс определения вида закона распределения результатов измерений. Правильность гипотезы может быть проверена в дальнейшем с помощью известных критериев, например Колмогорова или Стьюдента.

Статья выполнена в рамках проекта по аналитической ведомственной целевой программе «Развитие научного потенциала высшей школы (2009-2010 гг.)» на 2009 год, подраздел 2.1.2 «Проведение фундаментальных исследований в области технических наук», проект: «Теоретические основы решения задач управления – идентификации – оценивания на основе объединенного принципа максимума».

Литература

1. Алешкин А.Н., Лабутин С.А. Идентификация формы закона распределения случайных величин как задача приближения функций // Материалы заочных ВНТК "Современные проблемы математики и естествознания" и "Методы и средства измерений", 2002. – Н. Новгород: МВВО АТН РФ. – С. 6-9.
2. Безуглов Д.А. Кумулянтный метод оценки эффективности сегментированного зеркала адаптивной оптической системы // Оптика атмосферы и океана, 1996. №1. С.78-84.
3. Безуглов Д.А. Поморцев П.М. Скляров А.В. Обработка результатов измерений на базе аппроксимации плотности распределения сглаживающими кубическими В-сплайнами // Измерительная техника, 2000, №9. – С.32-36.
4. Крамер. Г. Математические методы статистики. – М., 1948. – 648 с.
5. Малахов А.Н. Кумулянтный анализ случайных негауссовых процессов и их преобразований. – М.: «Сов. радио», 1978. – 376 с.



Югтранс
VII Международный транспортный форум

Новороссийск
17-18 марта
2011

Форум «ЮгТранс» — это:

- традиционное открытие года
- 2 дня, 3 конференции, более 150 делегатов
- выступления экспертов в области транспорта
- обсуждение наиболее актуальных вопросов
- новые логистические решения
- транспортные проекты и международное сотрудничество
- внимание ведущих деловых и специализированных СМИ

www.konfer.ru

К вопросу оценки качества протоколов сетей передачи данных

Рассматривается подход к оценке качественных характеристик протоколов цифровых сетей связи, на основе анализа свойств корректности модели протокола. Определяется целевая функция оценки критериального показателя качества протокола, с учетом значения частного критерия качества программной реализации протокола.

Ключевые слова: сети передачи данных, протоколы, качество, корректность.

Кисляков М.А., Божко Е.С.,
Северо-Кавказский филиал
Московского технического
университета связи и информатики

To a question of an assessment of quality of protocols of data communication networks

Kislyakov M.A., Bozhko E.S.,
North-Caucasian branch of the Moscow
technical university relationship
and informatics

Abstract

The approach to assessing the quality characteristics of protocols of digital-communication networks, based on analyzing the properties of the correctness of the model protocol. Determined by the objective function evaluation criterion QualityProtocol, taking into account the importance of private quality criteria software implementing the protocol.

Keywords: data networks, protocols, quality and correctness.

Главной целью этапа исследования разрабатываемых протоколов является формулирование заключения о возможности протокольного объекта обеспечить достижение конечного результата своего функционирования. В этом случае мы имеем возможность говорить о качестве функционирования протокола. Для того чтобы построенный протокол обеспечивал получение требуемого результата необходимо, чтобы его структура отвечала требованию корректности [1]. Отсутствие в доступной литературе точного определения качества протокола и тот факт, что функции, выполняемые протоколом, при обеспечении условия его корректного исполнения, позволяют исключить ошибки пересылки данных (разрушение, потери, дублирование и нарушение очередности получения пакетов), вызываемых коммуникационными системами. Т.е. другими словами, пока программа, реализующая протокол, продолжает функционировать корректно, ошибки пересылки через ненадежную среду (характеризующие достоверность услуг связи) не будут влиять на правильное получение данных.

Соответствие остальных критериальных показателей, характеризующих качество услуг связи предоставляемых сервисом (оперативность, надежность), реализуемым коммуникационным протоколом, требованиям пользователя, определяется на этапе составления тактико-технического задания на разрабатываемый протокол. Выполнение этих требований также обеспечивается при условии правильного выполнения протоколом своих функциональных возможностей.

Вышесказанное позволяет определить качество протокола как степень соответствия свойствам, характеризующим его корректность. К таким свойствам относятся [2]:

1. Отсутствие статических блокировок, означающее, что в протоколе не существует такого состояния или набора состояний, из которых

не возможен переход в другие состояния.

2. Полнота, т. е. протокол обеспечивает реакцию на все возможные входные сообщения (отсутствуют ошибки неспецифицированных приемов).

3. Однозначность соответствия состояний, т.е. отсутствие таких протокольных объектов, у которых одно состояние может сосуществовать с несколькими различными состояниями какого-либо другого объекта.

4. Отсутствие избыточности, т. е. в спецификации протокола нет непустующих сообщений и невыполняемых действий.

5. Ограниченность, которая означает, что во время функционирования протокола число сообщений в каждом канале между протокольными объектами не превышает определенного значения, называемого емкостью канала.

6. Отсутствие динамических блокировок. Это значит, что в протоколе отсутствует бесконечный цикл функционирования, при котором не производится полезная работа. Различают динамические блокировки, выход из которых логически невозможен (свойство ба), и динамические блокировки, являющиеся следствием определенных временных характеристик протокола, например темпа обмена сообщениями (свойство бб).

7. Завершаемость (развитие), т.е. протокол всегда достигает конечного (терминального) состояния. Для циклических протоколов это свойство несколько видоизменяется. Эти протоколы должны обладать свойством развития, которое состоит в том, что протокол достигает своего начального состояния.

8. Самосинхронизация (восстановление после ненормальной ситуации). Это свойство подразумевает, что после возникновения ненормальной ситуации протокол за конечное время восстановит свое корректное функционирование.

Выделяются несколько основных групп свойств корректности протоколов, внутри каждой из которых протокол рассматривается с определенной точки зрения. В свою очередь, каждая из групп разделяется на две альтернативные категории.

Синтаксические свойства определяют логическую структуру обмена сообщениями (свойства 1–5). Семантические свойства связаны со смысловой правильностью процесса функционирования протокола. Различают свойства слабой семантики, которые связаны с эффективным развитием протокола (свойство 7), и свойства строгой семантики, связанные с конкретным назначением протокола (свойство 8).

К статическим свойствам относятся свойства 1 – 6а, а к динамическим свойствам 6б – 8.

Частичная корректность означает, что протокол обладает некоторым набором требуемых свойств, при условии, что в процессе функционирования он достигает заданного терминального состояния (или начального состояния в случае циклических протоколов). Это свойство означает лишь условную возможность выполнения требуемых свойств. Полная корректность протокола требует дополнительно доказательства свойства 7.

Методика оценки свойств протоколов [3], основывается на исследовании и оценке свойств достижимости, живости, ограниченности, безопасности и консервативности сетевых моделей протоколов.

1. Достижимость.

Для сети EN с заданной начальной разметкой M_0 требуется решить вопрос, достижима ли принципиально некоторая разметка $M \in R(EN)$ из M_0 , где $R(EN)$ – множество всех достижимых в EN разметок. В приложении к моделированию протоколов это свойство интерпретируется как возможность достижения протокольным объектом определенного состояния.

2. Живость.

Под живостью перехода сетевой модели понимают принципиальную возможность его срабатывания при любой достижимой из M_0 разметке:

$$\forall M \in R(EN), \exists M' \in R(EN): \\ M'(P_1(t)) \geq I(t),$$

(при M' каждое входное место перехода t имеет разметку не меньшую, чем кратность дуги, соединяющей p и t).

EN является живой, если все ее переходы живы. Следовательно, анализ на живость позволяет выявить возможные и невозможные события протокола.

3. Ограниченность и безопасность.

Позиция p_i является ограниченной, если существует такое целое неотрицательное число k_i , что при любой разметке количество меток в данной позиции не превышает k_i :

$$\forall p_i \in P(EN), \exists k_i > 0: M(p_i) \leq k_i.$$

Сеть является ограниченной в случае, когда все позиции ограничены, если все $k_i=1$, то сетевая модель называется безопасной. Следует отметить, что свойство ограниченности и безопасности вытекает из самого определения Е-сети, что упрощает анализ сетевой модели протокола на основе аппарата EN , в сравнении с классическими сетями Петри.

Анализ на ограниченность (безопасность) позволяет проверить возможность функционирования протоколов в заданных режимах, не выходя за установленные границы.

4. Консервативность.

Данное свойство означает неизменность суммы меток при любой маркировке сетевой модели:

$$\forall M_1, M_2 \in R(EN): \sum M_1(p) = \sum M_2(p).$$

Консервативность модели протокола позволяет выявить неизменность существующих ресурсов.

Для количественной оценки критериального показателя качества протокола определена [4] целевая функция F_{PR} :

$$F_{PR} = \frac{\sum_{i=1}^n k_i}{n}, \quad (1)$$

где $K = \{k_1, k_2, k_3, k_4, k_5, k_{6.1}, k_{6.2}, k_7, k_8\}$ – набор общих свойств протокола;

F_{PR} – количественная оценка качества протокола PR по множеству K_i ; $i = \overline{1, n}$ – свойства, учитываемые при оценке корректности протокола PR .

Для получения количественной оценки значения целевой функции (1) разработаны соответствующие алгоритмы и методы оценки статических и динамических свойств протоколов.

При оценке качества конечного протокола необходимо учитывать этап реализации, т.к. на этом этапе возможно внесение ошибок в конечную реализацию, за счет преобразования сетевой

модели в программную или программно-аппаратную реализацию. Использование допущения об отсутствии таких ошибок вносит неточность в оценку качества конечной реализации протокола.

Для устранения указанного недостатка введем в целевую функцию оценки протоколов частный критерий качества программной реализации – K_p .

$$F_{PR} = \frac{\sum_{i=1}^n k_i}{n} K_p, \quad (2)$$

Определим K_p через вероятность безошибочного перевода сетевой модели протокола в программную реализацию.

Анализ существующих систем программной реализации протоколов показал, что минимальный процент доли ручного программирования таких систем составляет 56% (4500 строк программы получено автоматически, 5700 вручную) [5]. С учетом того, что процент внесения ошибок в программный код при ручном программировании составляет в среднем 1% [70] (отношение числа ошибок к общему числу команд 10 к 1000). Следовательно при «ручном» программировании реализации протоколов $P_{ош.пр} = 0.01$.

В нашем случае необходимо учитывать вероятность внесения ошибок относительно общего размера программы. Рассчитаем этот показатель ($R_{отн.ош}$) как процентное отношение ошибочных строк $V_{ош}$ к общему объему программы в строках $V_{общ}$.

Для существующих систем этот показатель $R_{отн.ош} = 0,56$.

Для разработанной методики $R_{отн.ош} = 0,19$, основывается на проведенном эксперименте. Количество строк конечного программного кода составляет 9237, из них «вручную» написано 1755 строк, 7482 – автоматически. График зависимости доли ручного программирования от количества строк программы приведен на рис. 1.

Здесь:

1. Полностью «ручная» реализация протокола.

2. Существующие методы реализации, используемые в инструментальном комплексе НБС.

3. Предлагаемый подход, на основе методики трансляции сетевых моделей протоколов в программную реализацию.

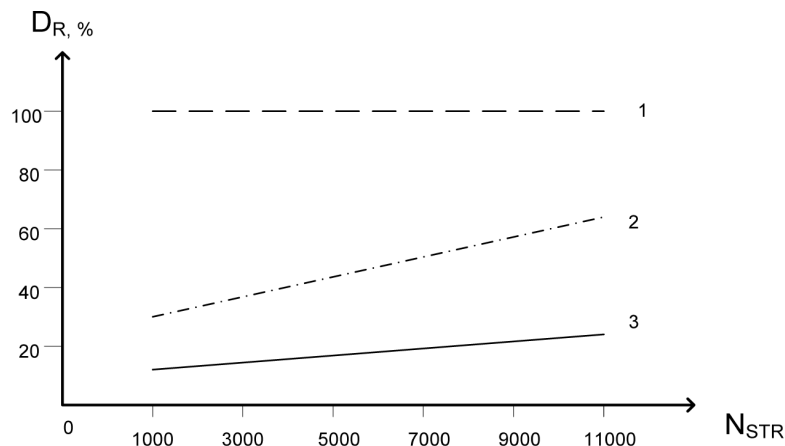


Рис. 1. Сравнительная характеристика методов реализации протоколов по показателю доли ручного программирования: D_R – доля ручного программирования в реализации протокола; N_{STR} – общее количество строк программы

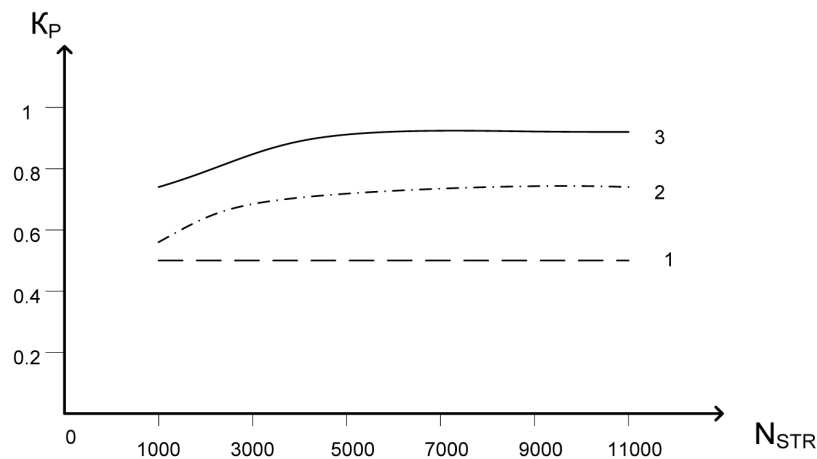


Рис. 2. Сравнительная характеристика методов реализации протоколов по критерию качества реализации: K_p – показатель качества программной реализации протоколов; N_{STR} – общее количество строк программы

Так как качество протокола повышается при безошибочной реализации, определим относительный показатель безошибочной реализации ($R_{отн.бэш}$) как:

$$R_{отн.бэш} = 1 - R_{отн.ош}$$

Тогда для существующих систем $R_{отн.бэш} = 0,44$.

Для разработанной методики $R_{отн.бэш} = 0,81$.

Проведем выбор диапазона численных значений критерия K_p . Очевидно, что безошибочная реализация модели протокола не приведет к снижению качества реализации, следовательно $\max K_p = 1$. С другой стороны – полностью «ручная» реализация программного исполнения протокола не может привести к 99-ти процентному снижению качества реали-

зуемого протокола, так как вносимые на этапе программирования ошибки могут приводить к различным последствиям. Для уточнения диапазона значений показателя качества реализации и выбора метода его вычисления воспользуемся данными из о том, что ошибки программирования приводят к критическим последствиям (сбою в работе системы) в 50% случаев. Таким образом, общий критерий качества программной реализации протоколов будет определяться как:

$$K_p = \frac{R_{отн.бэш} + 1}{2}. \quad (3)$$

Тогда для существующих систем $K_p = 0,72$.

Для разработанной методики $K_p = 0,905$.

Для полностью «ручной» реализации $K_p = 0,5$.

Проведем сравнение оценок качественных характеристик программной реализации протокола, полученных на основе нормированных показателей целевой функции (1) с учетом значений частного критерия качества реализации

На рис. 2. приведены зависимости, определяющие значение целевой функции (2) при различных размерах программной реализации протоколов. Значение целевой функции характеризует качество конечной реализации протоколов полученных различными способами.

Значение $\sum_{i=1}^n k_i$ принято равным 1, что соответствует корректной реализации протокола на этапе построения сетевой модели.

Здесь:

1. Полностью «ручная» реализация протокола.

2. Существующие методы реализации, используемые в инструментальном комплексе НБС.

3. Предлагаемый подход, на основе методики трансляции сетевых моделей протоколов в программную реализацию

Таким образом, применение метода трансляции сетевых моделей протоколов

в программную реализацию позволяет повысить качественные характеристики протоколов, за счет увеличения значения критериального показателя целевой функции F_{PR} , в 1,81 раза по сравнению с системами ручного программирования и в 1,26 раз по сравнению с существующими системами автоматизированной реализации протоколов.

Литература

1. Ракова И.К., Смирнова Н.Н. Методика анализа корректности протокольной реализации // АВТ. – 1986. – №6. – С.39-43.

2. Подлежанский А.А. Метод построения корректных протоколов сети радиотелефон-

ной связи: «Известия ВУЗов СКНЦ». – Ростов-на-Дону, 2006. – С.27-33.

3. Донченко А.А., Езимов А.В., Пряхин А.В. Сетевой аппарат формального описания динамических процессов // Теория и техника радиосвязи: Науч.-техн. сб. / ВНИИС.– Воронеж, 2002. – Вып. 2.–С.81–86.

4. Кирюхин В.В., Козлова Е.В. Автоматизация проектирования и оценка эффективности протоколов вычислительных сетей. – Киев: Общество “Знание”. Препринт, 1990.– 20 с.

5. Кисляков М.А., Донченко А.А. Реализация коммуникационных протоколов цифровых систем связи, описанных на языке E-сетей, в виде объектной программы // Труды СКФ МТУСИ, Ростов-на-Дону, 2009. – С. 40-45.

6. Лонгботтом Р. Надежность вычислительных систем / Пер. с англ. – М.: Мир, 2005. – 305 с.

softline®

Софт со всего света



Анализ помех и типовых ошибок в каналах связи при приеме сообщений

Рассмотрены помехи в канале связи и ошибки, возникающие при приеме сообщений. Приведена классификация помех и их различные модели. Построена модель ошибок в дискретном канале связи.

Ключевые слова: помехи, модель помех, канал связи, дискретный канал, модель ошибок.

Белинский Д.В.,
Северо-Кавказский филиал
Московского технического
университета связи и информатики

The analysis of noises and standard errors in communication links in case of reception of messages

Belinski D.V.,
North-Caucasian branch
of the Moscow technical university
relationship and informatics

Abstract

Considered interference in the communication channel, and errors that occur when receiving messages. At-vedena classification of interference and their various models. A model of error in a discrete communication channel.

Keywords: noise, model noise, communication channel, the discrete channel model errors.

Ошибки, возникающие при приеме сообщений, в значительной мере определяются видом и интенсивностью помех, действующих в канале. В зависимости от места нахождения источника помех различают внутренние и внешние помехи. Внутренние помехи возникают в самой системе. К ним относятся шумы устройств системы передачи данных и электрические сигналы, попадающие в приемник по внутренним цепям вследствие плохого экранирования или развязки между устройствами. Последний вид помех связан с ошибками в конструкции системы передачи данных и по возможности должен быть устранен. Внутренний шум, обусловленный хаотическим движением носителей зарядов, принципиально неустраним, хотя может быть в значительной степени ослаблен применением качественных узлов и деталей, а также снижением рабочей температуры.

Различают тепловой и дробовый шумы. Тепловой шум обусловлен тепловым движением носителей заряда, приводящим к появлению случайной разности потенциалов. Он представляет собой гауссовский случайный процесс с нулевым средним и спектральной плотностью мощности: где $h = 6,66 \cdot 10^{-34}$ Дж с — постоянная Планка; $k = 1,38 \cdot 10^{-23}$ Дж/град — постоянная Больцмана; T^0 — абсолютная температура источника шума; f — частота.

Шумы различных устройств систем передачи данных (дробовые шумы) обусловлены дискретной природой носителей заряда. Статистические характеристики дробового шума такие же, как у теплового.

Внешние помехи возникают из-за различных электромагнитных процессов, происходящих в атмосфере, ионосфере, космическом пространстве, а также излучения земной по-

верхности (естественные помехи). Кроме того, они создаются различными промышленными установками, медицинской аппаратурой, электрическими двигателями и т.п.

В зависимости от диапазона частот и условий, в которых работает СПИ, преобладает тот или иной вид помех.

Атмосферные помехи возникают в результате различных электрических процессов, происходящих в земной атмосфере. Наиболее мощным источником являются электрические громовые разряды, которые приводят к излучению электромагнитной энергии.

Промышленные помехи создаются различным электрооборудованием промышленных предприятий, транспорта, линиями электропередач и другими электроустановками. В большинстве случаев они представляют собой последовательности импульсов с постоянным или переменным периодом следования.

$$N_0(f) = \frac{hf}{\exp(hf/kT^0) - 1},$$

Упрощенную физическую модель образования помех при высокой загрузке канала можно представить в виде последовательно включенных генератора белого шума и фильтра с изменяющейся во времени по случайному закону частотной характеристикой.

Спектральную плотность мощности помех $N(f, t)$ как случайный процесс можно достаточно полно охарактеризовать плотностью вероятности $w_{f,t}(N)$ и корреляционными функциями флуктуаций во временной и спектральной областях $R_N(\tau)$ и $R_N(\nu)$. Параметрами корреляционных функций является интервал корреляции во времени τ_k и интервал корреляции по частоте F_k .

Если число помех, попадающих в полосу сигнала, ограничено, то предложенная модель не всегда применима. В этом случае поступающую на вход приемной части системы передачу данных смесь приходится представлять в виде суммы полезного сигнала и ограниченного числа аддитивных помех с известными или неизвестными статистическими характеристиками: где огибающая $A_i(t)$ и фаза $\Theta_i(t)$ помехи могут быть как случайными, так и детерминированными процессами.

Рассмотрим более подробно дискретный канал и, соответственно, модель ошибок в таком канале.

$$\gamma_i(t) = A_i(t) \cos [\omega_{cp} t + \Theta_i(t)].$$

Дискретный канал имеет дискретный вход и дискретный выход. Примером такого канала является канал, образованный совокупностью технических средств между выходом кодера канала и выходом демодулятора. Для описания дискретного канала необходимо знать алфавит входных символов x_r , $r = 1, \dots, m$, их вероятности появления $p(x_r)$, скорость передачи символов на выходе канала y_j , $j = 1, \dots, n$, и значения переходных вероятностей $p(y_j/x_r)$, $j = 1, \dots, n$; $r = 1, \dots, m$, появления символа y_j при условии передачи символа x_r .

Первые две характеристики определяются свойствами источника сообщений, скорость V — полосой пропускания непрерывного канала, входящего в состав дискретного канала, объем алфавита выходных символов — алгоритмов работы решающей схемы, переходные вероятности $p(y_j/x_r)$ — характеристиками непрерывного канала.

Заметим, что в общем случае в дискретном канале объемы алфавитов входных и выходных символов не совпадают. Примером может быть канал со стиранием. Алфавит на его выходе содержит один добавочный символ по сравнению с алфавитом на входе. Этот добавочный символ (символ стирания) появляется на выходе канала тогда, когда анализируемый сигнал нельзя с большой вероятностью отождествить ни с одним из символов входного алфавита. Стирание символов при применении соответствующего помехоустойчивого кода позволяет существенно повысить помехоустойчивость.

Зная вероятности $p(x_r)$ и $p(y_j/x_r)$, $r=1,2,\dots,m$, $j=1,2,\dots,n$, можно вычислить апостериорные вероятности того, что при принятом символе y_j был передан символ x_r . Вероятности $p(x_r)$ и $p(y_j/x_r)$ позволяют определять полную вероятность ошибки в канале (или полную вероятность правильного приема) и информационные характеристики дискретного канала.

Дискретный канал называется стационарным, если переходные вероятности $p(y_j/x_r)$, $r=1,2,\dots,m$, $j=1,2,\dots,n$, не зависят от времени. Дискретный канал называется каналом без памяти, если переходные вероятности $p(y_j/x_r)$, $r=1,2,\dots,m$, $j=1,2,\dots,n$, не зависят от ранее переданных и принятых символов.

Если в стационарном дискретном канале алфавиты на входе и выходе совпадают и удовлетворяют условию:

$$\begin{cases} P_{\text{ош}} & \text{для всех } j \neq r, \\ P(y_j/x_r) = 1 - (m-1)P_{\text{ош}} & \text{для } j = r, \end{cases}$$

то такой канал называется симметричным.

Математическая модель канала должна обеспечивать возможность нахождения основных характеристик потока ошибок. К ним относятся: вероятность ошибки в приеме символа $P_{\text{ош}}$; распределение вероятностей $P_n(r)$ появления r ошибок в блоке длины n ; распределения длин интервалов между соседними ошибками; распределения длин серий ошибок и т.п.

Модель должна быть простой и удобной для проведения расчетов. В то же время она должна достаточно точно описывать реальный канал, т.е. находится в хорошем соответствии с экспериментальными данными. Наиболее простой является модель стационарного симметричного канала без памяти. В таком канале ошибки возникают независимо друг от друга, т.е. между ошибками отсутствуют статистические связи. Вероятность ошибки $P_{\text{ош}}$ при передаче любого символа одинакова и не меняется во времени.

$$p(x_r / y_j) = \frac{p(x_r)p(y_j / x_r)}{\sum_{r=1}^m p(x_r)p(y_j / x_r)},$$

$$r = 1, \dots, m,$$

$$j = 1, \dots, n,$$

Стационарный симметричный канал без памяти полностью описывается вероятностью $P_{\text{ош}}$. Распределение ошибок в нем подчиняется биномиальному закону с характеристиками: n — число символов в блоке, r — число ошибочных символов.

Зная вероятность ошибки $P_{\text{ош}}$ и используя выражение, приведенное выше, можно найти все необходимые характеристики. В частности, вероятность правильного приема блока из n символов вероятность приема блока, содержащего хотя бы одну ошибку вероятность появления в блоке l и более ошибок.

$$P_n(r) = C_n^r \cdot p_{\text{ош}}^r (1 - p_{\text{ош}})^{n-r}.$$

Большинство реальных каналов имеют "память", которая проявляется в том, что вероятность ошибки в символе зависит от того, какие символы передавались до него и как они были приняты. Первый факт обусловлен межсимвольными искажениями, являющимися результатом рассеяния сигналов в канале, а второй — изменением отношения сигнал-шум в канале или характера помех.

При рассеянии сигнала приходящая на вход приемника посылка является суммой некоторого числа предыдущих посылок с соответствующими весовыми коэффициентами. Поэтому вероятность ошибки в последующем символе будет зависеть от характера передаваемой информации за время рассеяния сигнала. Например, при чередовании посылок разных частот, ошибка будет больше, чем внутри последовательности, состоящей из посылок одной частоты. Если меняется длительность отдельных мешающих воздействий, например, в результате общих замираний сигнала или изменения уровня помех, то ошибки будут группироваться в пакеты. Вероятность ошибки при приеме символа в этом случае зависит от того, была ошибка в предыдущем символе или нет. Простой моделью двоичного симметричного канала с памятью является канал, который может находиться в одном из двух состояний: $d = 0$ и $d = 1$. В обоих состояниях возможны независимые ошибки с вероятностями p_0 и p_1 , где нижние индексы указывают на состояние канала.

Одним из распространенных методов описания дискретного канала с памятью, связанной с межсимвольными искажениями, является ис-

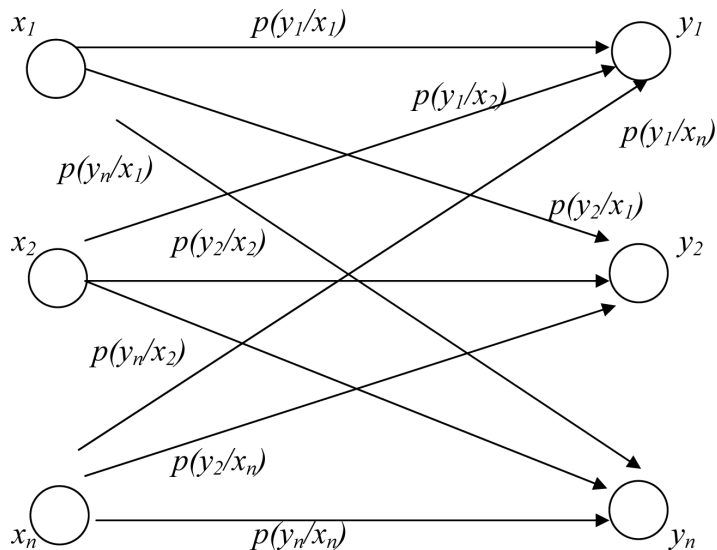


Рис.1. Модель канала с ошибками

пользование аппарата цепей Маркова (посимвольное описание). В этом случае последовательность состояний двоичного канала рассматривается как N -связная двоичная цепь Маркова, а значения символов на каждой позиции — как состояние цепи, где N — число символов, на которое распространяется память канала.

Рассмотренный дискретный канал и модель ошибок в таком канале могут быть использованы при построении моделей и синтезе устройств кодирования и передачи дискретных сигналов систем передачи данных.

Литература

1. Бертсекас Д., Галлагер Р. Сети передачи данных: Перевод с английского — М.: Мир, 1989. — 544 с.
2. Коичкина Т.П., Сидорова Т.В., Сперанский В.С. Сверхширокополосные системы телекоммуникаций. — М.: Инсвязьиздат, 2008. — 304 с.



МЕЖДУНАРОДНЫЙ КОНГРЕСС

ЭРА ГЛОНАСС

1 марта
2011

Москва
отель Ренессанс

Навигационно-информационные технологии для
повышения безопасности и комфорта на дорогах

ОСНОВНАЯ ЦЕЛЬ КОНФЕРЕНЦИИ:
информирование российской и зарубежной аудитории о статусе и планах развития «Системы экстренного реагирования при авариях «ЭРА ГЛОНАСС», о технических требованиях к терминалам, программах испытаний, создании инфраструктуры системы, дополнительных услугах в рамках проекта «ЭРА ГЛОНАСС» и зарубежном опыте по разработке и использованию подобных систем.

ЦЕЛЕВАЯ АУДИТОРИЯ

- Представители государственных организаций и ведомств, ответственные за разработку и реализацию государственной политики в области навигации и обеспечения безопасности на транспорте.
- Разработчики и производители ПО.
- Производители и разработчики телекоммуникационного оборудования.
- Автопроизводители.
- Операторы фиксированной и мобильной связи, обеспечивающие каналы информационного обмена.
- Производители и поставщики навигационного оборудования, контента, карт, картографического ПО.
- Представители СМИ.

К вопросу моделирования организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями

В соответствии с особенностями построения и условиями функционирования инфокоммуникационных сетей специального назначения (ИКС СН), с учетом требований стандартов по организации сетей управления телекоммуникациями (TMN) и организации систем сетевого управления (NMS), предлагаются различные варианты организации управляющей сети (УС) для автоматизированной системы управления (АСУ ИКС СН) на базе стандартной защищенной технологии в составе протокола IPv6, приводятся варианты математического описания УС, включающие вероятностные модели, модели массового обслуживания, приводится математическая модель передачи управляющей информации между центрами управления АСУ ИКС СН, позволяющая получить оценки вероятностно-временных характеристик УС.

Ключевые слова: управляющая сеть, система управления, инфокоммуникационная система, система управления, математическая модель.

Буренин А.Н., Легков К.Е.,
ФГУП "НИИ "Рубин"

Simulation of the information managing director of a network for modern infocommunication networks management system

Burenin A.N., Legkov K.E.,
The Federal State Unitary Enterprise
"Scientific Research Institute "Rubin"

Abstract

In article according to features of creation and operating conditions of infocommunication networks of a special purpose, taking into account requirements of standards for the organization of networks of telecommunication management (TMN) and the organization of systems of network control (NMS), different options of the organization of the controlling network (CN) for an automated control system are offered on the basis of the standard protected technology as a part of the IPv6 protocol, are brought versions of the mathematical description the CN, including probability models, waiting line models, is given a mathematical model of transmission of control data between centers automated control system, allowing to receive estimates of probable time response characteristics the CN.

Keywords: controlling network, management system, infocommunication system, management system, mathematical model.

Основой современных систем связи

различных ведомств и крупных госкорпораций являются инфокоммуникационные сети специального назначения (ИКС СН), функционирование которых осуществляется в достаточно сложных и неблагоприятных условиях обстановки [1], что требует организации достаточно четкого и устойчивого управления ими в реальном масштабе времени.

Современные ИКС СН строятся в соответствии с концепцией глобальной информационной инфраструктуры (GII) [2] на базе широкого применения современных информационных и телекоммуникационных технологий и технологий управления (рис.1).

Несмотря на сложность обеспечения функционирования ИКС СН в сложных условиях функционирования, необходимо обеспечить передачу требуемого объема информации с гарантированным качеством от индивидуальных или корпоративных пользователей в условиях возможных интенсивных воздействий на средства сети и оборудование ее узлов.

Это можно обеспечить только при наличии гибкой АСУ ИКС СН, реализующей эффективные методы управления, и при организации качественного обмена управляющей информацией между пунктами управления (ПУ). Этот обмен управляющей информацией должна обеспечить (в соответствии с рекомендациями МСЭ-Т по TMN, серия М.30**) специальная выделенная сеть управления, учитывающая специфику решения задач уп-

равления ИКС СН.

Так как архитектура современных ИКС СН, построенных в соответствии с концепцией GII, содержит три основных уровня (рис. 1), то управление ею также целесообразно декомпозировать на три уровня управления: управление инфраструктурным уровнем, управление промежуточным уровнем, управление базовым уровнем ИКС СН, на каждом из которых управление осуществляется по пяти основным задачам управления, к которым относятся задачи управления производительностью уровня, безопасностью, структурой и адресацией, ресурсами уровня и сбойными ситуациями [2].

Каждый уровень архитектуры ИКС СН [2] представляет собой сеть или совокупность сетей:

- инфраструктурный уровень представляет собой совокупность сетей услуг;
- промежуточный уровень представляет собой совокупность сетей услуг middleware (услуги безопасности, биллинга, аутентификации, поиска);
- базовый уровень — совокупностью транспортной сети, сетей доступа и сетей традиционной связи.

Значительная часть вышеперечисленных групп управления осуществляется на основе передачи соответствующих документов с использованием телекоммуникационных служб электронная почта и файловый обмен как по сети управления, так по самой управляемой ИКС СН, путем выделения специального ресурса.



Рис. 1. Архитектура современных ИКС СН

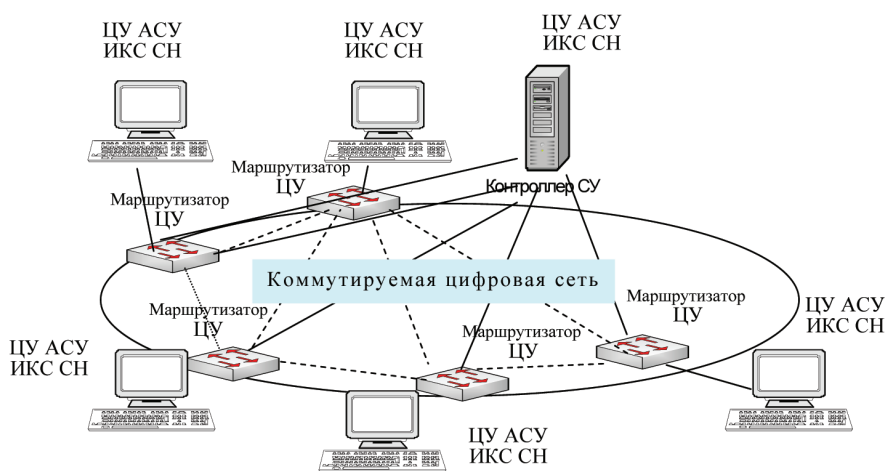


Рис.2. Топология управляющей сети АСУ ИКС СН

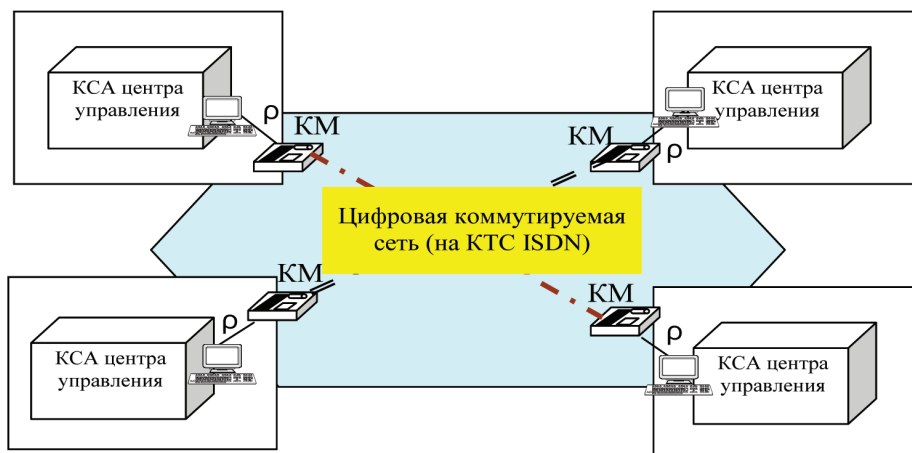


Рис. 3. Двухполюсная декомпозиция процедур обмена управляющей информацией между ПУ АСУ ИКС СН

При любом варианте управляющей сети она, как правило, организуется путем наложения защищенной IP-сети на транспортную основу с применением маршрутизаторов центров управления (рис.2).

При построении IP-сети поверх коммутируемой цифровой сети (например, сети ISDN) между слоем коммутируемых цифровых каналов и слоем IP существует цифровая сеть. Это, при соответствующей корректировке вероятностно-временных характеристик, справедливо и при организации IP-сети поверх сети FR, ATM и пр.

Каждый порт маршрутизатора центра управления сетью должен поддерживать интерфейс соответствующего канала в качестве конечного узла. После того как каналы установлены, маршрутизаторы могут пользоваться ими как физическими, посылая данные порту соседнего (по отношению к виртуальному каналу) маршрутизатора. В сети образуется сеть выделенных каналов с собственной топологией.

Подсеть коммутируемых каналов прозрачна для IP-маршрутизаторов сети управления, они ничего не знают о физических связях между портами коммутаторов сети. При этом IP-сеть является наложенной по отношению к этой сети. Сам сеанс организации того или иного соединения для повышения устойчивости управления ИКС СН осуществляется только на время обмена управляющей информацией, что существенно повышает скрытность процессов управления.

Для оценки вероятностно-временных характеристик передачи управляющей информации рассмотрим схему ее организации при наложенной сети (рис.3).

Для обеспечения защищенной передачи управляющей информации целесообразно применять криптомаршрутизатор (КМ), который реализует протокол IP-сек (защищенный подпротокол протокола IPv6) в транспортном или туннельном вариантах.

В рассматриваемом варианте для каждого цикла управления ИКС СН сеть управления может быть представлена совокупностью двухполюсных сетей между взаимодействующими центрами управления сетью.

В цифровой сети используется метод коммутации цифровых каналов, при котором информация (в виде IP-пакетов) вводится в сеть только после установления соединения, т.е. передача массива IP-пакетов возможна лишь после того, как образован сквозной канал между вызываемым и вызывающим КМ. Несомненным преимуществом такой организации является возможность немедленного (с задержкой на время установления соединения) обмена информацией между двумя КМ. В сети с коммутацией каналов прохождение срочной информации, обладающей высшим приоритетом, происходит сравнительно быстро, однако этот эффект достигается путем прерывания каналов для информации с низкой категорией приоритета. Естественно, управляющая информация обладает высшим приоритетом.

Эффективность метода коммутации каналов в цифровой коммутируемой сети существенно зависит от соотношения между средним временем передачи одного массива IP-пакетов \bar{t}_1 и временем установления соединения \bar{t}_y . В современной ISDN сети всегда выполняется условие [3]:

$$\bar{t}_{n1} > \bar{t}_y \quad (1)$$

Среднее время установления соединения \bar{t}_y на k участков равно $\bar{t}_y = k\bar{t}_{k1}$, где \bar{t}_{k1} – среднее время проключения (коммутации) цифрового канала между двумя соседними узлами ISDN. Случайное время t_{k1} в ISDN сети имеет распределение близкое к нормальному с дисперсией незначительной величины [3], которой можно пренебречь. Поэтому можно считать $t_{k1} \approx \bar{t}_{k1}$.

Случайное число транзитных участков в установленных соединениях цифровых каналов в ISDN сети, как правило, имеет распределение близкое к равномерному. Это объясняется тем фактом, что в ISDN сети применяются алгоритмы динамического управления сетью.

Поэтому можно считать, что случайное время t_y также имеет равномерное распределение со средним значением \bar{t}_y .

Тогда среднее время доставки IP-пакета в наложенной управляющей сети можно определить из выражения:

$$\bar{t}_n = \frac{Q_n}{v_{эф}} + \bar{t}_{k2} + \bar{t}_y, \quad (2)$$

где \bar{t}_y – среднее время задержки пакета в КМ; \bar{t}_{k2} – среднее время обработки заголовка IP-пакета с обращением к маршрутной таблице; Q_n и $v_{эф}$ – соответственно объем IP-пакета и эффективная скорость передачи его по установленному цифровому каналу.

Средне время задержки пакета в КМ \bar{t}_y можно определить, если описать КМ в виде системы массового обслуживания (СМО) [4, 5], предполагая, что пакеты, поступающие из центров управления сетью, образуют самоподобный поток с конечным числом источников, при этом значение \bar{t}_y определится выражением:

$$\bar{t}_y = \frac{Q_n \sum_{k=1}^m \frac{(k-1)m!\rho^k}{(m-k)!}}{v_{эф}} P_0, \quad (3)$$

где ρ – нагрузка, поступающая на КМ; m – число IP-пакетов, которое может поступить за время цикла управления (определяется объемом управляющего сообщения);

$$P_0 = \frac{1}{1 + \frac{m!\rho}{(m-1)!} + \sum_{k=2}^m \frac{m!\rho^k}{(m-k)!}}$$

– вероятность того, что КМ незагружен.

Тогда среднее время доведения управляющего сообщения для каждой пары взаимодействующих комплексов средств автоматизации ЦУ АСУ ИКС СН составит:

$$\bar{t}_{звс} = \bar{t}_y + m \left[\bar{t}_{k2} + \frac{Q_n}{v_{эф}} \left(1 + \frac{\sum_{k=1}^m \frac{(k-1)m!\rho^k}{(m-k)!}}{1 + \frac{m!\rho}{(m-1)!} + \sum_{k=2}^m \frac{m!\rho^k}{(m-k)!}} \right) \right] \quad (4)$$

Отметим важное обстоятельство, что для рассматриваемой модели (одноканальной СМО), приведенные выражения справедливы в состоянии установившегося стохастического равновесия для любых законов распределения времени обслуживания [4].

Полный ряд распределения вероятностей возможных состояний отдельного КМ можно получить, вычислив вероятности этих состояний:

$$P_k = \frac{m! \rho^k}{(m-k)!} P_0 \quad (5)$$

При этом каждое состояние КМ будет соответствовать определенному времени задержки IP-пакета, поступающего на него. С вероятностью P_0 время задержки равно 0, с вероятностью P_1 время задержки равно $\frac{Q_{п1}}{V_{эф}}$, с вероятностью P_2 время задержки составит $\frac{2Q_{п1}}{V_{эф}}$ и т.д.

С целью получения оценки вида непрерывного распределения этот ряд может быть аппроксимирован соответствующей функцией (например, взвешенной суммой экспонент).

Предложенный подход и полученные выражения могут быть использованы и при организации наложенной IP-сети на основе цифровых сетей с применением технологий FR или ATM [6], при этом изменяется только временные характеристики организации сеансов обмена управляющей информацией между ЦУ АСУ ИКС СН [7], определяемые особенностями телекоммуникационных технологий FR и ATM. Так при использовании в качестве транспортной магистральной

сети ИКС СН ATM-сети время установления виртуального цифрового соединения будет определяться задаваемым режимом передачи (ABR, VBR), а также применяемым для передачи информации АСУ ИКС СН сервисом уровня адаптации ATM (AAL1, AAL2, AAL3\4 или AAL5).

На рис. 4 приведены сравнительные характеристики вероятностно-временных параметров передачи управляющей информации АСУ ИКС СН при организации транспортной основы для наложенной IP управляющей сети с использованием соответственно технологий ISDN (кривая 1), FR (кривая 2) и ATM при AAL5 (кривая 3) в зависимости от средней интенсивности потоков управляющей информации.

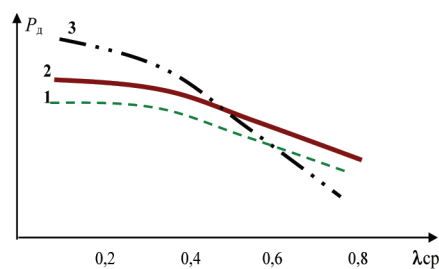


Рис. 4. Вероятность своевременной доставки управляющего сообщения в управляющей сети АСУ ИКС СН

Таким образом, предложен вариант организации управляющей сети для под-

систем управления телекоммуникационными сетями, основанный на наложении IP-сети на цифровую коммутируемую ISDN, FR или ATM сеть, получены и приведены основные вероятностно-временные характеристики процессов передачи управляющей информации, которые могут быть использованы для оценки эффективности управляющей сети.

Литература

1. Буренин А.Н., Легков К.Е. Эффективные методы управления потоками в защищенных инфокоммуникационных сетях // Научные технологии в космических исследованиях Земли, 2010. – №2. – С.29-34.
2. ITU-T Recommendation Y.101 (2000), Global Information Infrastructure terminology: Terms and definitions.
3. Боккер П. ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы / Пер. с нем. – М. Радио и связь, 1991. 304 с.
4. Клейнрок Л. Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с.
5. Саати Т.Л. Элементы теории массового обслуживания и ее приложения. – М.: Сов. Радио, 1971. – С.520.
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер. Изд. 4, 2004. – 872 с.
7. Буренин А.Н. Системно-архитектурные вопросы построения автоматизированных систем управления связью // Телекоммуникационные технологии. – СПб.: «Политехника», 1996. Вып.1. – С.97-112.

V Международная выставка современной продукции, новых технологий и услуг железнодорожного транспорта

exporail2011

16 – 18 марта
ЦВК "ЭКСПОЦЕНТР", Москва

Повышение структурной скрытности системы передачи информации с кодовым разделением каналов

Рассматривается способ формирования систем ортогональных сигналов и производится сравнительная оценка по параметру структурной скрытности предлагаемых сигналов с известными системами ортогональных сигналов, используемыми в системах передачи информации с кодовым разделением каналов.

Ключевые слова: ортогональные сигналы, система передачи информации с кодовым разделением каналов, структурная скрытность, база сигнала.

Жук А.П., Иванов А.С.,
Ставропольский государственный университет

Increase of structural reserve of an information transmission system code-division channels

Zhuk A.P., Ivanov A.S.,
Stavropol state university

Abstract

In article is considered way of the shaping the systems orthogonal signal and is produced comparative estimation on parameter of the structured secretiveness proposed signal with the known system orthogonal signal, used in system of the issue to information with code division channel.

Keywords: orthogonal signals, system of the issue to information with code division channel, structured secretiveness, base of the signal.

В последнее время в связи с бурным развитием информационной инфраструктуры нашей страны увеличилось значение систем передачи дискретной информации по каналам радиосвязи. Особое место занимают системы передачи информации с кодовым разделением каналов (СПИ КРК) на основе широкополосной технологии множественного доступа с кодовым разделением каналов.

Однако с увеличением объемов передаваемой информации в СПИ КРК, актуальной становится проблема ее защиты.

Согласно конфиденциальность передачи сообщений по радиоканалам может быть достигнута путем обеспечения:

Энергетической скрытности сигналов-переносчиков характеризуемой затратами (временными и аппаратными) на его обнаружение по энергетическим признакам без использования информации о форме, структуре и других характеристиках.

Структурной скрытности сигналов-переносчиков характеризуемой затратами (времени, средств), необходимыми для выявления состояния объекта (структуры сигнала) в котором он находится в данный момент времени с заданной достоверностью.

Информационной скрытности сообщения, которая характеризуется способностью противостоять мерам, направленным на раскрытие информации, содержащейся в сигнале (шифрование данных).

Однако в условиях массового применения СПИ с КРК секретность паролей и кодов доступа не обеспечивает необходимой защиты, поэтому требуется создать условия, при которых затраты времени и технических средств на их самый высокоскоростной поиск были бы столь

велики, что такие задачи стали бы трудно достижимыми. В связи с этим важнейшее значение на сегодняшний день приобретают вопросы, связанные с обеспечением структурной скрытности сигналов переносчиков.

Целью статьи является, повышение структурной скрытности систем передачи информации основанных на технологии широкополосного доступа с кодовым разделением каналов.

В настоящее время предложен ряд способов передачи информации в СПИ КРК с повышенным уровнем структурной скрытности, а именно:

1. Способ многостанционного доступа с кодовым разделением каналов, где расширение спектра частот осуществляется на основе использования 64 видов последовательностей, сформированных по закону функций Уолша.

2. Способ многостанционного доступа с кодовым разделением каналов, включающий операцию одновременной передачи сложных широкополосных сигналов на основе нелинейных последовательностей де Брейна со сменой формы последовательности в процессе передачи сообщения от одного информационного символа к другому.

3. Способ передачи информации с кодовым разделением каналов, в которой используются ортогональные сигналы, формируемые на основе производных ортогональных систем сигналов.

Однако все перечисленные выше способы имеют общий недостаток — количество структур дискретных ортогональных сигналов, формируемых предложенными способами, конечно, что приводит с ростом объема информации, к увеличению вероятности раскрытия структуры сигналов-переносчиков.

В статье предлагается вариант повышения структурной скрытности системы передачи информации основанной на технологии широкополосного доступа с кодовым разделением каналов, который, заключается в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать сформированные стохастическим образом ортогональные системы сигналов, описываемые собственными векторами диагональных положительно определенных симметрических матриц размерностью N . При этом используется свойство ортогональности собственных векторов, заключающееся в том, что собственные векторы, соответствующие различным собственным значениям нормального оператора, попарно ортогональны.

Известно, что всякий ненулевой вектор x называется собственным вектором матрицы A , если найдется такое число λ , что будет выполняться равенство:

$$A \cdot x = \lambda \cdot x. \quad (1)$$

Это число λ называется собственным значением матрицы A , соответствующим собственному вектору x .

Если в пространстве выбран определенный базис, то уравнение (1) для собственных векторов и собственных значений линейного преобразования можно записать в матричной форме:

$$A \cdot X = \lambda \cdot X. \quad (2)$$

Всякий ненулевой столбец X , для которого выполняется равенство (2), называется собственным вектором матрицы A , соответствующим собственному значению λ .

Собственный вектор матрицы A — это столбец вида (3) составленный из координат собственного вектора $x = (x_1, x_2, \dots, x_N)$ линейного преобразования $y = A \cdot x$ в выбранном базисе.

Собственные векторы вещественной диагональной симметрической матрицы, отвечающие различным собственным значениям, ортогональны, т.е. их скалярное произведение равно нулю.

$$X = \begin{Bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_N \end{Bmatrix} \quad (3)$$

Из всего выше сказанного следует, что для любой вещественной диагональной симметрической матрицы A соотношение (4) существует набор собственных значений $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_N\}$ и каждому собственному значению соответствует собственный вектор X , который попарно ортогонален с любым из вектор в ансамбля

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,N} \\ \alpha_{2,1} & \alpha_{2,2} & \dots & \alpha_{2,N} \\ \dots & \dots & \dots & \dots \\ \alpha_{N,1} & \alpha_{N,2} & \dots & \alpha_{N,N} \end{bmatrix} \Rightarrow \lambda = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \dots \\ \lambda_N \end{bmatrix} \Rightarrow X = \begin{bmatrix} x_{1,1} & x_{1,2} & \dots & x_{1,N} \\ x_{2,1} & x_{2,2} & \dots & x_{2,N} \\ \dots & \dots & \dots & \dots \\ x_{N,1} & x_{N,2} & \dots & x_{N,N} \end{bmatrix}. \quad (4)$$

При этом расширение информационной последовательности происходит таким образом, что, если информационный бит, равен единице то используется ортогональный сигнал инверсной структуры, а если информационный бит, равен нулю, то используется ортогональный сигнал прямой структуры.

Нелинейность формируемых структур сигналов достигается за счет того, что на каждом такте передачи информации, расширяющая последовательность в виде одного из сигналов ортогональной системы сигналов, описываемых собственными векторами диагональных положительно определенных симметрических матриц, формируется путем стохастического задания набора диагональных коэффициентов, положительно определенной симметрической матрицы A (вида 4), генератором случайных положительных чисел.

Для оценки структурной скрытности рассматриваемых систем ортогональных сигналов в работе предлагается оценивать структурную скрытность сигналов через затраты на выявление его состояния с заданной достоверностью (вероятностью правильного решения). При

этом под структурной скрытностью понимается арсенальная скрытность, определяемая мощностью A (числом элементов) множества X возможных сменных параметров сигнала, в частности вариантов кодовых структур. Рабочие параметры передаваемого сигнала выбираются из этого множества случайно.

При этом ширина спектра такого сигнала определяется известным соотношением:

$$F = \frac{1}{T}. \quad (5)$$

$$A = \frac{\bar{F}}{F} = \bar{F}T. \quad (6)$$

$$S = -\log_2(1/A) = \log_2 A = \log_2(\bar{F}T). \quad (7)$$

При базе передатчика $\bar{V} = \bar{F}T$ возможное число не перекрывающихся по частоте или форме каналов (их арсенал) равно:

При условии того, что рабочий сигнал x_i , $i = 1, \dots, A$, выбирается из имеющегося арсенала с равными вероятностями $p_i = 1/A$ структурная скрытность сигналов определяется выражением:

В соответствии с выражением (7) были получены значения структурной скрытности предложенного способа и способа передачи информации на основе последовательностей де Брейна представлены в таблице в зависимости от базы сигнала.

На рисунке 1 представлена графическая зависимость структурной скрытности СПИ КРК на основе предлагаемого способа формирования ортогональных сигналов (кривая 1) и на основе последовательностей де Брейна (кривая 2) от базы сигнала.

Зависимость структурной скрытности СПИ КРК на основе предлагаемого способа формирования ортогональных сигналов (кривая 1) и

Результаты расчетов структурной скрытности сигналов для рассмотренных СПИ КРК

База сигнала N	Предлагаемый способ	Способ де Брейна
	Структурная скрытность S_M , диз	Структурная скрытность S_Q , диз
16	23,1613	3,5850
32	31,2608	8,1699
64	39,3313	15,0768
128	47,3716	31,4756
256	59,9322	58,9057

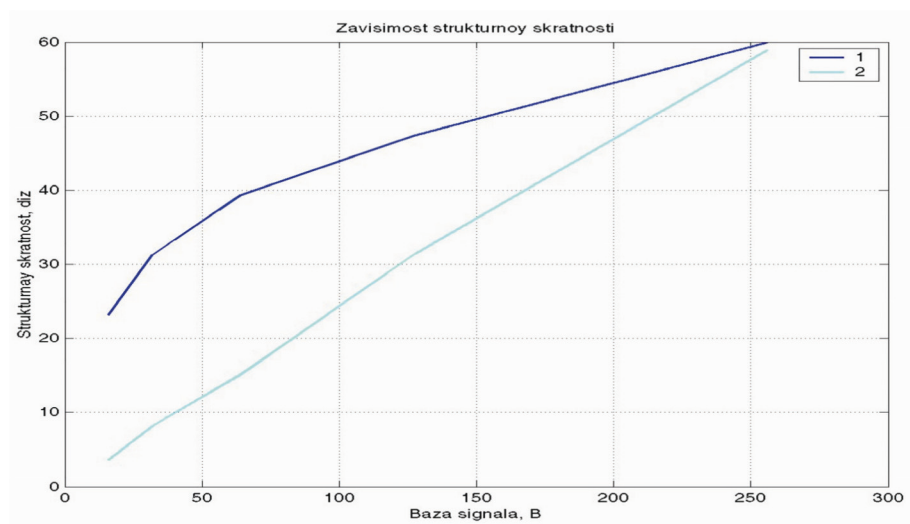


Рис. 1

на основе последовательностей де Брейна (кривая 2) от базы сигнала. Из таблицы 2 и рисунка 1 можно увидеть, что предлагаемый способ формирования систем ортогональных сигналов (кривая 1) позволяет улучшить структурную скрытность сигналов по сравнению со

способ формирования систем ортогональных сигналов на основе последовательностей де Брейна (кривая 2) при размерности базы сигнала $V = 16$ на 19,57 дБз, $V = 32$ на 23,09 дБз, $V = 64$ на 24,25 дБз, $V = 128$ на 15,89 дБз, при $V = 256$ на 1,02 дБз.

Таким образом, применение данного способа позволит повысить структурную скрытность современных системах передачи информации с кодовым разделением каналов, направленных на передачу данных различного формата (речь, факс, музыка, интернет) с различной скоростью и конфиденциальностью.

Литература

1. Варакин Л.Е. Теория систем сигналов. — М.: Советское радио, 1978. — 303 с.
2. Каневский З.М., Литвиненко В.П., Макаров Г.В., Максимов Д.А. Теория скрытности: Учеб. пособие / Под ред. З.М. Каневского. Воронеж: ВГТУ, 2006. — 211 с.
3. Громаков Ю.А. Стандарты и системы подвижной радиосвязи. — М.: АОЗТ "Эко-трендз КО", 1996.
4. Патент Российской Федерации № 2234191, кл. H04B7/216, H04L9/26 от 24.07.2001.
5. Попенко В.С. Векторный синтез ансамблей ортогональных сигналов — Ставрополь: МО, РФ, ч. II, 1993.

**III РОССИЙСКИЙ
МЕЖДУНАРОДНЫЙ КОНГРЕСС
ПО ИНТЕЛЛЕКТУАЛЬНЫМ
ТРАНСПОРТНЫМ СИСТЕМАМ**

17–20 мая 2011 года
Санкт-Петербург

Технологии MIMO в мобильных сетях нового поколения

Приведены современные беспроводные сети, стандарты связи, история их появления на рынке, роль в коммуникациях. Описаны принципы работы технологии MIMO в мобильных сетях нового поколения, основные положения, проблемы и перспективы технологии.

Ключевые слова: LTE, MRC, MIMO, мобильные сети, беспроводные цифровые коммуникации.

**Федоренко И.В., Нерсесянц А.А.,
Мясникова А.И.,**
Северо-Кавказский филиал
Московского технического
университета связи и информатики

Technology mimo in mobile networks of new generation

**Fedorenko I.V., Nersesyanc A.A.,
Myasnikova A.I.,**
North-Caucasian branch
of the Moscow technical university
relationship and informatics

Abstract

Modern wireless networks, communication standards, history of their occurrence in the market, a role in communications are resulted. Principles of work of technology MIMO in mobile networks of new generation, substantive provisions, problems and technology prospects are described.

Keywords: LTE, MRC, MIMO, mobile networks, wireless digital communications.

Беспроводные цифровые коммуникации, бурно стартовав, продолжают развиваться чрезвычайно быстро. Этому способствует неуклонный прогресс в микроэлектронике, позволяющий выпускать все более сложные (и при этом все более дешевые) средства беспроводной связи. Бум сотовой связи, сравнимый лишь с ростом производства персональных компьютеров и развитием Интернета, не замедляется уже четверть века. Мобильных телефонов во всем мире уже значительно больше, чем обычных проводных телефонных аппаратов. Быстрыми темпами развиваются персональные и локальные сети, широко внедряются беспроводные сети регионального масштаба. Низкая стоимость, быстрота развертывания, широкие функциональные возможности по передаче данных, телефонии, видеопотоков делают беспроводные сети одним из основных направлений развития телекоммуникационной индустрии.

Развитие беспроводной связи сопровождается непрерывной сменой технологий, в основе которых лежат стандарты сотовой связи GSM и CDMA, а также стандарты систем передачи данных IEEE 802. Исторически технологии беспроводной связи развивались по двум независимым направлениям — системы телефонной связи (сотовая связь) и системы передачи данных (Wi-Fi, WiMAX). Но в последнее время наблюдается явная тенденция к слиянию этих функций. Более того, объем пакетных данных в сетях сотовой связи третьего поколения (3G) уже превышает объем голосового трафика, что связано с внедрением технологий HSPA. В свою очередь, современные сети передачи информации обязательно обеспечивают заданный уровень качества услуг (QoS) для различных видов трафика. Реализуется поддержка приоритизации отдельных потоков информации, причем как на сетевом/транспортном уровнях (на уровне TCP/IP), так и на MAC-уровне (стандарты IEEE 802.16). Это позволяет использовать их для оказания услуг голосовой связи,

передачи мультимедийной информации и т.п.

В связи с этим само понятие сетей следующего, четвертого, поколения (4G) неразрывно связано (если не синонимично) с созданием универсальных мобильных мультимедийных сетей передачи информации. Сегодня две группы технологий явно нацелены на оказание универсальных услуг связи. Это WiMAX (как развитие линии IEEE 802) и технологии сотовой связи поколений "супер 3G". Причем каждая из них занимает свою нишу на обширном рынке беспроводной связи.

Технология фиксированного WiMAX (IEEE 802.16-2004) не оправдала возлагавшихся на нее надежд по быстродействию, объему зоны покрытия и ценовым характеристикам. Но операторы справедливо ожидают качественного прорыва от мобильного WiMAX (IEEE 802.16e), который уже начал активно внедряться во всех странах мира, включая Россию.

Разработка технологии LTE как стандарта официально началась в конце 2004 г. Основной целью исследований на начальном этапе был выбор технологии физического уровня, которая смогла бы обеспечить высокую скорость передачи данных. В качестве основных были предложены два варианта: развитие существующего радиointерфейса W-CDMA (используемого в HSPA) и создание нового на основе технологии OFDM. В результате проведенных исследований единственной подходящей технологией оказалась OFDM, и в мае 2006 г. в 3GPP была создана первая спецификация на радиointерфейс Evolved UMTS Terrestrial Radio Access (E-UTRA). Первые, предварительные спецификации LTE создавались в рамках так называемого 3GPP Release 7. А в декабре 2008 г. утверждена версия стандартов 3GPP (Release 8), фиксирующая архитектурные и функциональные требования к системам LTE. В середине 2009 г. ожидается выход в свет первых опытных систем на основе LTE, а в 2010 — первых коммерческих сетей.

По сравнению с ранее разработанными системами 3G, радиointерфейс LTE обеспечит улучшенные технические характеристики. В частности, в LTE ширина полосы пропускания может варьироваться от 1,4 до 20 МГц (по более ранним источникам – от 1,25 МГц), что позволит удовлетворить потребностям разных операторов связи, обладающих различными полосами пропускания. При этом оборудование LTE должно одновременно поддерживать не менее 200 активных соединений (т.е. 200 телефонных звонков) на каждую 5-МГц ячейку.

Также ожидается, что LTE улучшит эффективность использования радиочас-

тотного спектра, т.е. возрастет объем данных, передаваемых в заданном диапазоне частот. LTE позволит достичь внушительных агрегатных скоростей передачи данных – до 50 Мбит/с для восходящего соединения (от абонента до базовой станции) и до 100 Мбит/с для нисходящего соединения (от базовой станции к абоненту) (в полосе 20 МГц). При этом должна обеспечиваться поддержка соединений для абонентов, движущихся со скоростью до 350 км/ч. Зона покрытия одной БС – до 30 км в штатном режиме, но возможна работа с ячейками радиусом более 100 км. Под-

держиваются многоантенные системы MIMO.

В системах LTE на PHY уровне, как на базовой станции, так и на пользовательском терминале (UE) с целью достижения устойчивости и увеличения скорости данных в прямом канале могут применяться несколько трансиверов. Например, в случае тяжелых условий распространения при низком уровне сигнала, когда условия многолучевого распространения требуют увеличения передаваемой мощности, на приеме используется метод суммирования максимального отношения (MRC).

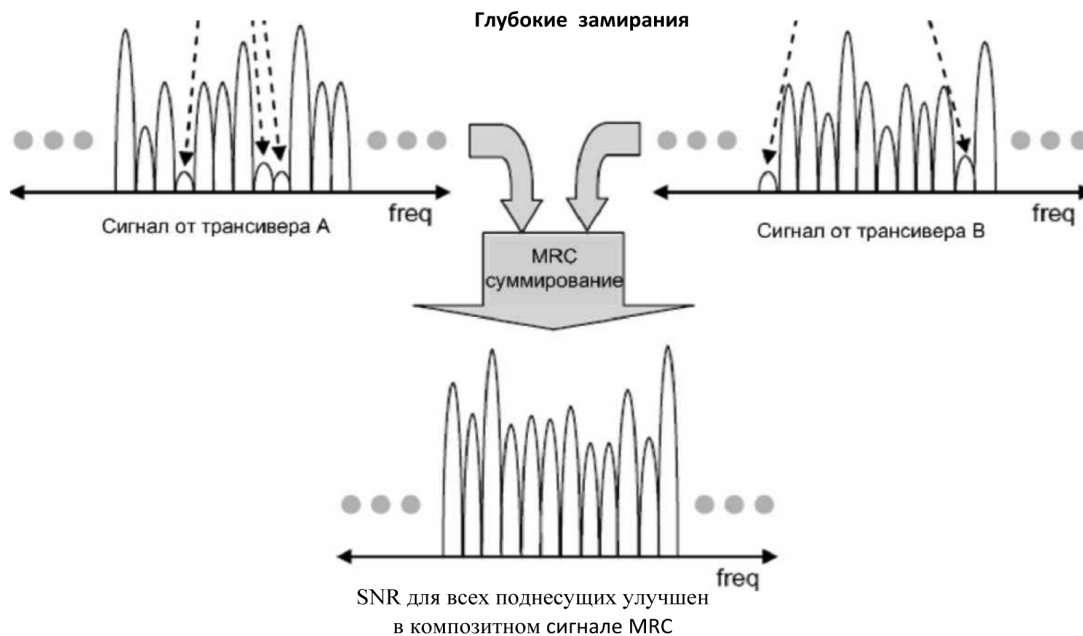


Рис. 1. Метод MRC позволяет повысить надежность в условиях AWGN и частотно-избирательных замираний

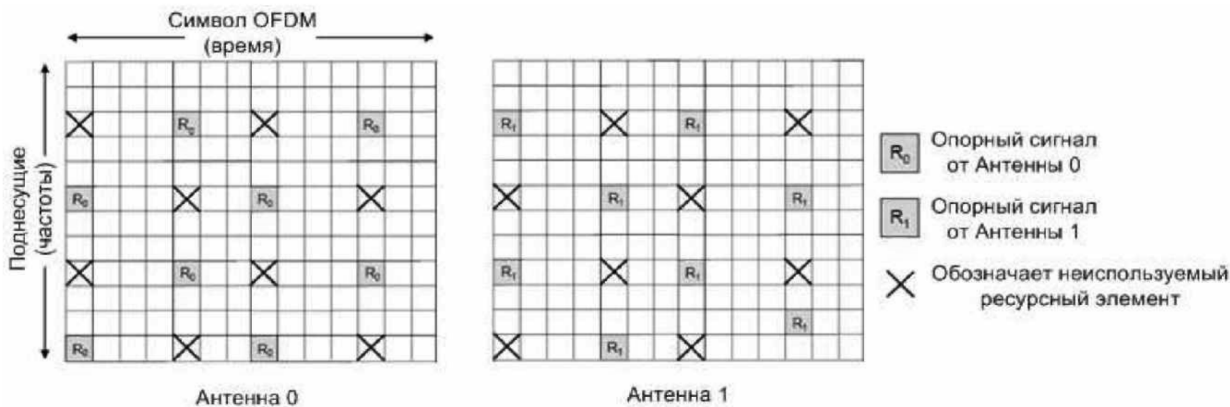


Рис. 2. Обеспечивающие работу MIMO опорные сигналы, которые передаются последовательно для вычисления характеристик каналов.

Основной же метод, который используется для увеличения системной скорости данных, – это MIMO. Для его реализации в конструкцию терминала следует добавить, по крайней мере, еще один трансивер и антенну.

В процессоре основной полосы (baseband) вводится компенсация для каждого из принимаемых сигналов, прежде чем они будут просуммированы для получения одного композитного принимаемого сигнала.

При суммировании по данному методу принимаемые сигналы складываются в процессоре основной полосы когерентно. Тепловые же шумы для каждого из трансиверов являются некоррелированными. Таким образом, линейное суммирование компенсированных по фазе и амплитуде сигналов в процессоре основной полосы приводит в двухканальном приемнике MRC в условиях ограниченного шума к увеличению SNR не менее чем на 3 дБ.

Кроме улучшения SNR за счет суммирования, приемники, работающие по методу MRC, более устойчивы к частотно-селективным федингам. Еще раз подчеркнем тот факт, что физическая раздельность приемных антенн приводит к различию импульсных характеристик их каналов приема. В присутствии частотно-избирательных замираний статистически маловероятно, что данная поднесущая будет испытывать глубокие замирания сразу в обоих каналах приема. Таким образом, вероятность глубоких частотно-избирательных федингов в суммарном сигнале существенно уменьшается.

Метод MRC улучшает степень надежности (готовности) линии связи, но не позволяет увеличить номинальную скорость данных. При использовании метода MRC данные передаются одной антенной, а принимаются двумя или большим числом приемников, поэтому MRC – это скорее метод разделенного приема, т. е. обычный метод Antenna Diversity. И наоборот, технология MIMO позволяет увеличить системную скорость данных. Такое увеличение достигается за счет использования нескольких антенн, как на стороне приема, так и на стороне передачи.

Для успешного приема сигналов по технологии MIMO, приемник должен определить импульсную характеристику

канала для каждой из передающих антенн. В системе LTE импульсная характеристика канала определяется путем последовательной передачи каждой из передающих антенн известных опорных сигналов.

Для системы 2x2 MIMO определяют одна общая или четыре отдельных канальных импульсных характеристики (C1, C2, C3 и C4). Заметим, что пока одна передающая антенна передает опорный сигнал, другая не используется. Как только импульсная характеристика канала будет определена, начнется независимая передача данных обеими антеннами. Линейная комбинация двух потоков данных на двух приемных антеннах приводит к системе из двух уравнений с двумя неизвестными, решить которую невозможно для отдельных оригинальных потоков данных.

Пусть антенные решетки в схеме CCC – MIMO, представленной на рис. 3, состоят из N передающих и M приемных элементов, связанных некоторым числом радиоканалов. На вход n-го элемента передающей AP, изолированного от остальных, подается сигнал с нормированной амплитудой напряжения U_{Π}^n . Электромагнитные волны, распространяясь в условиях неоднородного пространства по нескольким направлениям (радиоканалам), вызовут появление на m входе изолированного элемента приемной AP отраженного (по отношению к этому входу) сигнала с нормированной амплитудой напряжения U_0^m . Полная канальная матрица $H(B, A)$ образуется из элементов

$h_{mn}(b_m, a_n) = \frac{U_0^m(b_m)}{U_{\Pi}^n(a_n)}$ и имеет следующий вид:

$$H(B, A) = \begin{bmatrix} h_{11}(b_1, a_1) & \dots & h_{1N}(b_1, a_N) \\ \dots & \dots & \dots \\ h_{M1}(b_M, a_1) & \dots & h_{MN}(b_M, a_N) \end{bmatrix}, \quad (1)$$

где $A = (a_1, \dots, a_N)$, $B = (b_1, \dots, b_M)$ – некоторые сечения (входы) в фидерных линиях элементов передающей и приемной AP.

С использованием детерминистического подхода к модели распространения радиоволн и в предположении, что элементы приемной AP идеально согласованы с приемным устройством, показано, что канальная матрица $H(B, A)$ с

учетом взаимодействия элементов AP может быть выражена через аналогичную матрицу $H^{HLD}(B, A)$ без учета взаимодействия:

$$H(B, A) = (E - S_{11}^{PPM}(B)) H^{HLD}(B, A) (E - S_{11}^{PPD}(A))$$

где: $S_{11}^{PPD}(A)$ – матрица рассеяния передающей AP относительно ее входов A, связывающая между собой комплексные амплитуды напряжений падающих $U_{\Pi}(A)$ и отраженных $U_o(A)$ волн:

$$U_o(A) = S_{11}^{PPD}(A) U_{\Pi}(A); \quad (3)$$

$S_{11}^{PPM}(B)$ – матрица рассеяния приемной AP; E – единичная матрица.

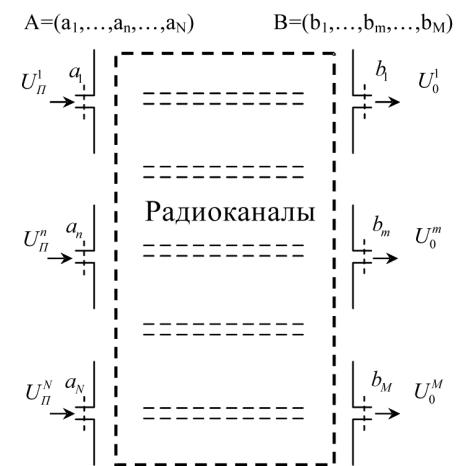


Рис. 3. Структурная схема CCC с многоканальными антенными системами

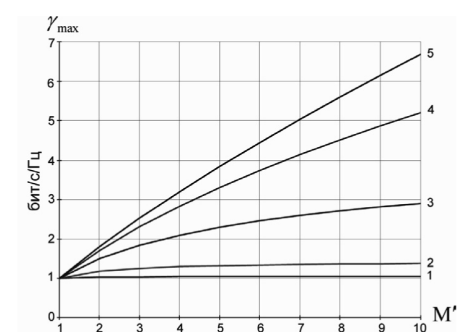


Рис. 4. Зависимость выигрыша γ_{\max} от числа каналов M' при разных значениях $\rho|\mu_1|^2$: 10дБ (1); 0дБ (2); 10дБ (3); 20дБ (4); 30дБ (5)

Из полученного выражения (2) следует, что учет эффектов взаимодействия элементов передающей и приемной AP приводит к изменению канальной матрицы $H(B, A)$.

Для определения мощности принимаемого сигнала, предполагая, что он является гармоническим, с учетом взаимодействия элементов приемной и передающей АР можно перейти к выражению для энергетической матрицы вида $W(B, A) = H_i^*(B, A)H(B, A)$, элементы которой и определяют мощность сигнала $P_c(B)$ в сечениях bt фидерных линий элементов приемной АР:

$$P_c(B) = \langle U_0^*(B)U_0(B) \rangle = \langle U_n^*(A)W(B, A)U_n(A) \rangle \quad (4)$$

Спектральное разложение энергетической матрицы по собственным векторам позволяет определить собственные значения каналов:

$$W = T \{ \mu_i \} T_i^* = T \{ |\mu_i|^2 \} T_i^* \quad (5)$$

где: T – матрица ортонормированных собственных векторов матрицы W ;

$\{ |\mu_i|^2 \}$ – диагональная матрица собственных значений $|\mu_1|^2, |\mu_2|^2, \dots, |\mu_M|^2$, определяемых из системы уравнений:

$$\begin{cases} \det(W(B, A) - |\mu|^2 E) = 0, \\ WT = \{ |\mu_i|^2 \} T. \end{cases} \quad (6)$$

Взаимодействие элементов приемной и передающей АР приводит к изменению собственных векторов и собственных значений энергетической матрицы $W(B, A)$.

На основе теоремы Шеннона для канала с «белым» шумом максимальное значение C_{\max}^1 спектральной эффективности ССС - SISO с одноканальной схемой построения может быть представлено в виде (7). В случае же организации M' независимых радиоканалов спектральная эффективность ССС – MIMO определяется выражением:

$$C_{\max}^1 = C_{\max}^{\text{SISO}} = \log_2 \left(1 + \rho |\mu_{j_{\max}}|^2 \right)$$

где: $|\mu_{j_{\max}}|^2 = \left(\frac{P_c(B)}{P_c(A)} \right)_{\max}$; $\rho = \frac{P_c(A)}{P_{\text{ш}}(B)}$. (7)

$$C_{\max}^{M'} = C_{\max}^{\text{MIMO}} = \sum_{m=1}^{M'} \log_2 \left(\frac{|\mu_m|^2}{M'} \sum_{k=1}^{M'} \frac{1}{|\mu_k|^2} + \rho \frac{|\mu_m|^2}{M'} \right) \quad (8)$$

Данное выражение получено путем спектрального разложения энергетической матрицы $W(B, A)$ и поиска максимального значения спектральной эффективности ССС – MIMO при неизменной мощности излучения ($P_c(A) = \text{const}$). Отметим, что в случае единственного канала выражение (8) переходит в выражение (7), а в случае M' каналов с равными значениями $|\mu_1| = |\mu_m|, m = 1, \dots, M'$ – в известное выражение.

$$\max(C_{\max}^{M'}) = C_{\max \max}^{M'} = M' \log_2 \left(1 + \rho \frac{|\mu_1|^2}{M'} \right) \quad (11)$$

Тогда выигрыш в спектральной эффективности ССС - MIMO при организации M' каналов с равными значениями $|\mu_i|^2$ по сравнению с ССС - SISO будет равен:

$$\gamma_{\max} = \frac{C_{\max \max}^{M'}}{C_{\max \max}^1} = \frac{M' \log_2 \left(1 + \rho \frac{|\mu_1|^2}{M'} \right)}{\log_2 \left(1 + \rho |\mu_1|^2 \right)}$$

Анализ результатов моделирования многолучевой радиотрассы позволяет сформулировать следующие основные особенности использования технологии MIMO в перспективных ССС:

– максимум спектральной эффективности ССС – MIMO достигается при равенстве собственных значений независимых каналов;

– в случае существенно неравнозначных каналов оптимальная система MIMO (по критерию максимизации СЭ) трансформируется в ФАР с адаптацией к сосредоточенным по направлению прихода помехам;

– взаимодействие элементов АР изменяет величину канального усиления и структуру собственного вектора канала;

– существует взаимное расположение элементов в приемной и передающей АР, при котором СЭ канала может быть значительно увеличена, особенно для малых значений $P_c/(P_{\text{ш}}+P_{\text{пом}})$;

– значительное повышение СЭ по сравнению с одноканальным способом передачи информации возможно только при существенном превышении $P_c/(P_{\text{ш}}+P_{\text{пом}}) \gg 1$;

– существенная неравнозначность каналов и наличие сосредоточенных по направлениям прихода помех приводит к резкому падению спектральной эффективности ССС;

– собственные значения каналов существенно и по-разному зависят от взаимного расположения базовой станции и абонентского терминала, что ограничивает возможности повышения спектральной эффективности ССС - MIMO, особенно при работе в движении и на значительные расстояния.

Литература

1. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE, технологии и архитектура. – М., 2010.
2. Легков К.Е. Методы повышения канальной скорости в каналах сетей беспроводного широкополосного доступа // Т-Comm: Телекоммуникации и транспорт, 2011. – №6. – С.39-41.
3. Легков К.Е. Беспроводные локальные сети IEEE 802.11: механизм распределения скоростей // Телекоммуникации и транспорт, 2010. – №4. – С.17-19.
4. Легков К.Е. Методы повышения производительности беспроводных mesh-сетей специального назначения // Т-Comm: Телекоммуникации и транспорт, 2010. – №6. – С.17-19.

IEEE 802.16: управление качеством информационного обмена в системах специального назначения

В настоящее время технологии беспроводного доступа городского масштаба, основанные на стандарте IEEE 802.16, нашли свое применение в системах связи специального назначения. Данный стандарт применяется для передачи большого количества трафика различного вида. Как осуществлять эффективное управление качеством информационного обмена в данных системах. Ответ на эти вопросы и раскрыт в настоящей статье.

Ключевые слова: управление услугами, услуга, широкополосный беспроводный доступ.

Мясникова А.И., Голубинцев А.В.,
Северо-Кавказский филиал
Московского технического
университета связи и информатики

IEEE 802.16: quality management information exchange in systems of special purpose

Myasnikova A.I., Golubintsev A.V.,
North-Caucasian branch of the Moscow
technical university relationship
and informatics

Abstract

Currently, wireless access citywide, based on the standard IEEE 802.16, are used in communication systems for special applications. This standard applies to transfer a large amount of traffic of various kinds. How to effectively manage the quality of information exchange in these systems. The answer to these questions and uncovered in this article.

Keywords: Service Management, service, broadband wireless access.

Проведенные эксперименты по анализу структуры трафика сетей беспроводного широкополосного доступа выявили, что исследуемый трафик имеет отчетливую структуру VBR (variable bit rate) типа, то есть интенсивность передачи информации значительно изменяется во времени, в результате чего трафик имеет высокую пачечность. Как следствие, статическое задание пропускной способности канала (методы типа шейпинга и полисинга), применяемое в современной аппаратуре специального назначения, приводит к большим потерям информации и низкой утилизации канала. Первое обстоятельство ухудшает характеристики качества обслуживания, а второе сказывается на неэффективности использования ресурсов канала.

Решением данной проблемы является использование метода разделения времени передачи пакетов, основанного на прогнозировании самоподобного сетевого трафика, который не является новым, в настоящее время существует некоторое количество работ, касающихся проблемы прогнозирования самоподобного телетрафика. Однако до настоящего времени практически не проводились исследования, посвященные изучению возможностей адаптивного распределения пропускной способности на основе прогнозирования применительно к самоподобному телетрафику беспроводных широкополосных сетей доступа специального назначения.

В качестве возможного варианта применения схемы с прогнозированием рассмотрим простой частный пример: для физического канала с потенциально достижимой пропускной способностью C_{Σ} организовано два логических (виртуальных) канала VC (virtual channels)

со статически заданными пропускными способностями C_1 и C_2 соответственно, причем $C_{\Sigma} = C_1 + C_2$ (см. рис. 1).

В первом из них передается информация реального времени, чувствительная к задержкам и потерям (для системы видеоконференц-связи, например), а во втором - второстепенная информация (данные www, ftp и другая информация, не чувствительная к задержкам и потерям).

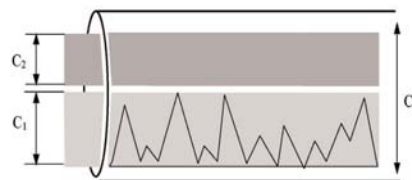


Рис. 1. Статическое распределение пропускной способности физического канала между двумя логическими

Возникает задача наиболее эффективного способа разделения общей пропускной способности C_{Σ} физического канала между двумя логическими. Поскольку в первом виртуальном канале передается критичная к потерям информация, необходимо увеличивать пропускную способность C_1 этого канала. Однако при этом уменьшается его утилизация и доступная пропускная способность для второго канала, поскольку $C_2 = C_{\Sigma} - C_1$. В результате ресурсы физического канала расходуются неэффективно. Более того, чем выше пачечность трафика в первом канале, тем ниже эффективность системы.

В этом случае может схема с прогнозированием позволяет решить эту задачу. В этом случае с помощью предсказателя система заранее получает информацию о требованиях к пропускной способности канала с приоритетной информацией (первого канала) в некоторый момент времени t в ближайшем будущем.



Рис. 2. Динамическое распределение пропускной способности физического канала между двумя логическими

Поэтому к наступлению момента времени t система выделяет для первого канала требуемый ресурс пропускной способности C_1^f , распределив при этом второму каналу всю оставшуюся доступную пропускную способность $C_2^f = C_Σ - C_1^f$. Как можно видеть из рис. 2 метод разделения времени передачи пакетов в данном примере увеличивает утилизацию в первом канале и предоставляет больше ресурсов для второго канала.

Идея предлагаемого метода состоит в модификации рассмотренных выше методов управления трафиком (полисинга и шейпинга), служащих для реализации функций обеспечения качества информационного обмена с помощью введения дополнительного модуля, прогнозирующего на некоторое время вперед необходимое значение B_c в соответствии с изменением интенсивности поступающих пакетов. При этом пропускная способность системы подстраивается под профиль трафика, уменьшая при этом потери и увеличивая использование выделенных ресурсов, а не трафик вырав-

нивается под заданный наперед профиль.

Принцип работы метода разделения времени передачи пакетов с прогнозированием, основанный на механизме «корзина маркеров», изображен на рис. 3.

Согласно данной схемы входящий поток пакетов одновременно с поступлением в систему попадает на схему агрегирования по временным интервалам. После чего n последних отсчетов получившегося временного ряда поступают на предсказатель, который выдает прогнозную оценку следующего отсчета $\hat{x}(n+1)$ агрегированного ряда x на время вперед. Исходя из требований к величине возможных потерь, оценивается пропускная способность системы $\hat{C}(n+1)$.



Рис. 3. Принцип работы метода разделения времени передачи пакетов

При этом, как показано на рис. 3, с помощью обратной связи может учитываться статистика потерянных пакетов. В результате размер буфера маркеров

устанавливается $B_c = \hat{C}(n+1)$ на время вперед.

Таким образом, значение B_c (а вместе с ним и CIR) будет меняться каждый интервал Δ , отслеживая динамику изменения интенсивности трафика. При той же самой (в среднем) пропускной способности системы, в режиме разделения времени передачи пакетов удается достичь лучших показателей потерь и использования чем в случае реализации классического полисинга.

Аналогичным образом, с помощью введения прогнозирующего модуля можно модифицировать метод шейпинга. При этом отброс пакетов из-за несовершенства предсказателя будет снижен за счет увеличения задержек. Схема функционирования такого метода фактически будет соответствовать приведенной на рис. 3, в которую дополнительно введен буфер для поступающих в систему пакетов.

Эксперимент по исследованию возможностей метода разделения времени передачи пакетов проведем с помощью следующего алгоритма (рис. 4):

в исходном дискретном временном ряде $x(k)$, соответствующем трафику выделим участок T фиксированной длины LT ;

изучая характеристики ряда на данном тренировочном участке (оценивая параметры прогностической модели), формируем прогноз $\hat{C}(i)$ (на один шаг вперед) i -го значения ряда $x(k)$, следующего за концом участка;

фиксируем получившуюся абсолютную ошибку прогноза $e(i)$;

сдвигаем участок T длины LT на один шаг вперед, считая, что к наступившему моменту времени нам уже стало известно действительное значение только, что спрогнозированного отсчета i ;

осуществляем прогноз следующего значения и т.д.

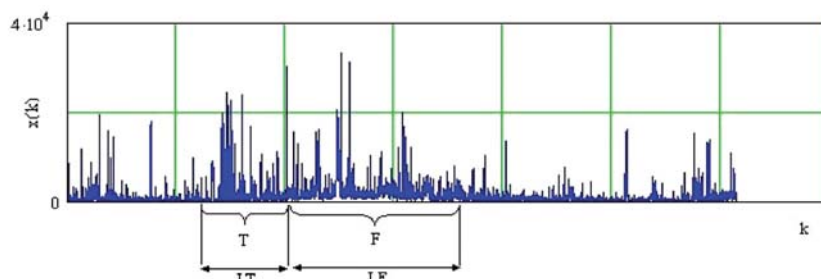


Рис. 4. Эксперимент по прогнозированию трафика

Для того чтобы оценить выигрыш от использования метода разделения времени передачи пакетов по сравнению со статическим способом, а также для выбора наиболее подходящего способа прогнозирования рассмотрим оценки улучшения качества обслуживания:

$$AdvD_{forecast}^+(i) = D_{st}^+(i) - D_{forecast}^+(i), \quad (1)$$

$$AdvD_{forecast}^-(i) = D_{st}^-(i) - D_{forecast}^-(i), \quad (2)$$

которые фактически представляют собой разности между соответствующими

оценками для статического метода распределения и выбранного метода разделения времени передачи пакетов. При этом, чем выше значения оценок (1-3), тем выше значение выигрыша в качестве обслуживания для выбранного метода разделения времени передачи пакетов по отношению к методу статического задания пропускной способности.

Заметим, что выигрыши в коэффициентах недооценки (1) и переоценки (2) для рассматриваемых методов прогно-

зирования фактически совпадают, поэтому далее будем изучать лишь одно из соотношений (1).

Все оценки выигрыша больше нуля, что означает преимущества алгоритмов динамического распределения полосы по сравнению со статическим способом. Обратим внимание на тот факт, что при увеличении bs выигрыш в использовании динамического способа уменьшается и стремится к нулю.

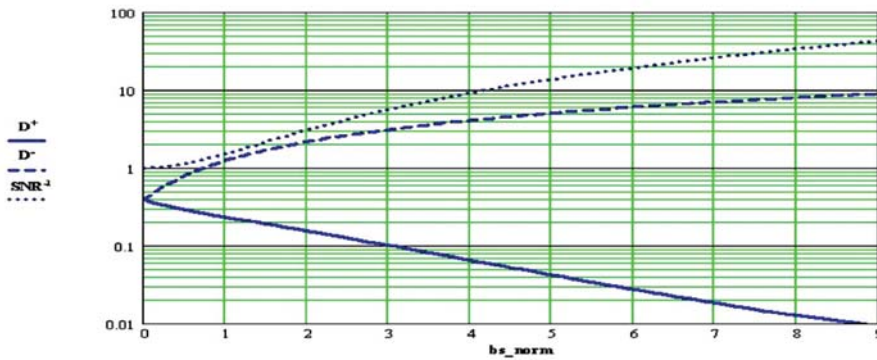


Рис. 5. Оценки статистических характеристик при статическом задании пропускной способности канала

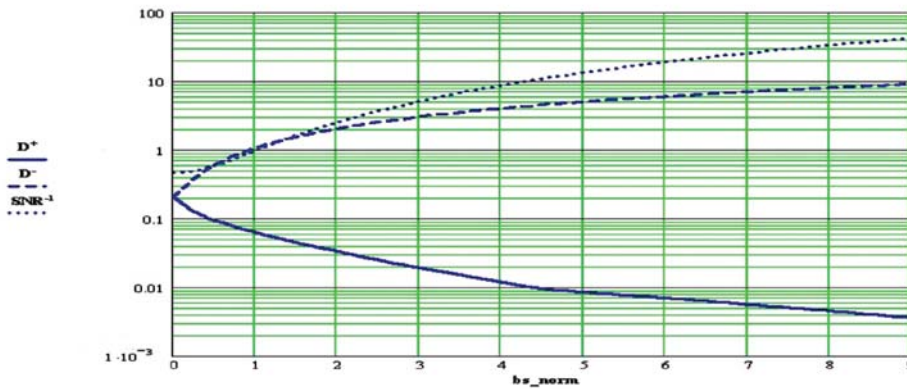


Рис. 6. Оценки статистических характеристик при динамическом задании пропускной способности канала с простым предсказателем

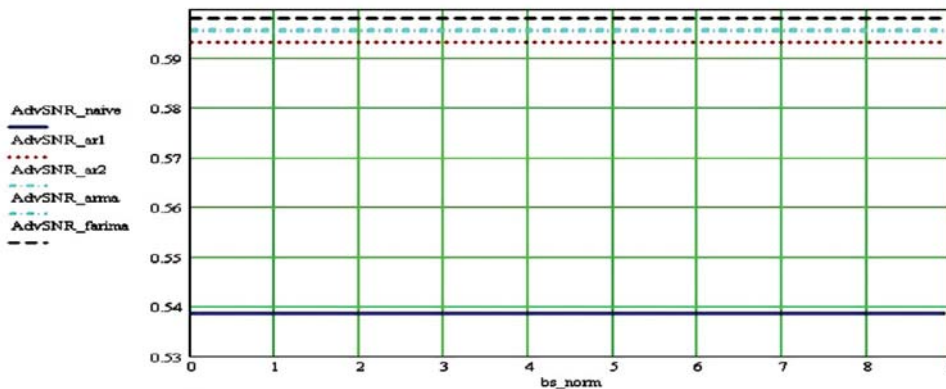


Рис. 7. Выигрыш в коэффициенте SNR^{-1} при методе разделения времени передачи пакетов с различными алгоритмами прогнозирования

С точки зрения улучшения коэффициентов $D+$ и $D-$ лучшие характеристики получаются при прогнозировании с помощью простого предсказателя, так при статическом способе задания полосы в точке $bs_norm = 1$ коэффициент недооценки $D_{st}^+ \approx 0,2433$. Это означает потерю 24.33% всей информации, переносимой трафиком $x(k)$. В то же время с помощью простого предсказателя (рис. 6) (при том же самом среднем значении полосы пропускания \hat{C} , то есть при $bs_norm=1$) потери недооценки удается уменьшить до 6.4% ($D_{naive}^+ \approx 0,064$).

Таким образом, выигрыш в $D+$ и $D-$ при использовании простого предсказателя (в точке $bs_norm=1$) составил ~18% от всего объема информации (см. рис. 6). В то же время выигрыш в показателе SNR^1 для простого предсказателя соответствует ~54%.

Оценим некоторые количественные показатели для конкретного случая. Как правило, для обеспечения удовлетворительного функционирования системы видеоконференцсвязи, например, считается, что величина потерь не должна превышать 1-2% от всего объема транслируемой информации.

По графику на рис. 6, для алгоритма с простым предсказателем с целью достижения такой величины потерь достаточно ограничить пропускную способность канала уровнем соответствующем значению $3 < bs_norm < 4.5$. Другими словами, пропускная способность канала должна быть равна среднему значению трафика (на изучаемом участке, т.е. на участке F), умноженному на коэффициент 3 - 4,5.

В то же время, для достижения такого же эффекта при использовании статического задания пропускной способности,

значение данного коэффициента возрастает значительно и соответствует 7-9 (см. рис. 5). Очевидно, данное обстоятельство увеличивает стоимость канала примерно в 2 раза.

Переходя далее к изучению рис. 6, можно сделать вывод о том, что выигрыш в статистических характеристиках $D+$ и $D-$ при использовании метода разделения времени передачи пакетов для рассмотренного случая видеоконференцсвязи (при $3 < bs_norm < 4.5$) составит от 4 до 8%.

Следует заметить, что видеоконференцсвязь является наиболее требовательным к величине потерь сервисом. В общем случае, при организации менее требовательных сервисов, величина выигрыша может быть больше ~10% (см. рис. 6).

Выигрыш в статистике SNR^1 (которая, как будет показано ниже, отвечает за джиттер) составляет ~54% (см. рис.7). С другой стороны, для более сложных моделей эта величина несколько больше и составляет ~59%.

Заметим, что применение других предсказателей и даже значительное усложнение модели дает, тем не менее, достаточно небольшое улучшение в характеристике SNR^1 (а именно, выигрыш при этом увеличивается с 54% до 59%) на фоне также незначительного ухудшения характеристик $D+$ и $D-$ [7].

Поэтому, с точки зрения простоты реализации, меньшей ресурсоемкости и требовательности предсказателя, а также лучших показателях потерь и использования ресурсов канала ($D+$ и $D-$) для использования в методе разделения времени передачи пакетов в системах распределения информации применяем простой предсказатель.

Для обеспечения требуемого качества

информационного обмена в системах беспроводного широкополосного доступа специального назначения, при изменяющихся внешних (условия распространения радиоволн, воздействие непреднамеренных и преднамеренных помех, связь в движении) и внутренних (величина и распределение трафика в сети, состав и топология сети, технические отказы и т.п.) условиях функционирования, задачи оптимизации характеристик и режимов работы отдельных элементов и системы в целом должны решаться совместно на всех уровнях ЭМВОС исходя из единого критерия.

Таким критерием может быть максимизация пропускной способности системы при заданных ограничениях на другие показатели эффективности.

В качестве такого критерия может использоваться и обеспечение требуемого качества обслуживания приоритетных пользователей при максимизации количества обслуживаемых не приоритетных абонентов и др. Впрочем, выбор критерия также может динамически изменяться в зависимости от цели и сложившихся на данный момент условий функционирования системы. А система должна распределять «усилия» по адаптации на всех уровнях для достижения требуемой цели.

Проведенные расчеты качества информационного обмена согласно разработанной ранее методики оценки с помощью программы подтверждают вывод о повышении общей эффективности системы.

Оценка качества информационного обмена при использовании методов статического задания пропускной способности и разделения времени передачи пакетов с прогнозированием в системе беспроводного широкополосного доступа представлена на рис. 8.

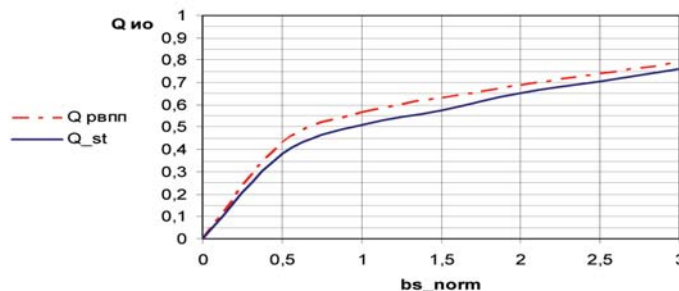


Рис. 8. Оценка качества информационного обмена при использовании методов статического задания пропускной способности и разделения времени передачи пакетов с прогнозированием

Полученные результаты подтверждают, что качество информационного обмена в системе беспроводного широкополосного доступа при применении метода разделения времени передачи пакетов с прогнозированием заметно выше (10-15 %) при том же самом объеме передаваемой в системе информации.

Применение метода разделения времени передачи пакетов ограничивается случаями, когда возможно разделить трафик на две категории: приоритетный и не приоритетный, а также когда используется техника виртуальных каналов (в отличие от статистического мультиплексирования потоков). При этом если приоритетный трафик оказывается самоподобным и обладает высоким коэффициентом пачечности, то разработанный метод также будет эффективен. В противном случае его эффективность окажется не хуже эффективности метода статического распределения пропускной способности.

Следовательно, усовершенствованный метод разделения времени передачи пакетов с применением простого предсказателя при заданных ограничениях на другие показатели качества информационного обмена и порядок его работы в системах беспроводного широкополосного доступа специального назначения могут рассматриваться как основные составляющие методики управления качеством информационного обмена, которую можно представить в виде следующей последовательности действий:

1. Оценка качества информационного обмена в системах беспроводного доступа военного назначения как интегрального показателя для всех видов предоставляемого обмена.

$$Q_z = \sum_{j=1}^n A_i \cdot K_j \quad (4)$$

где A_i – коэффициент, число значений которого определяется числом уровней КИО m , $i = m + 1$; K_i – весовой коэффициент, определяющий значимость показателей КИО; n – число показателей КИО.

2. Определение эффективности системы беспроводного доступа специального назначения:

$$W \{ Q \geq Q_{\text{тр}} \} \quad (6)$$

где $W = \frac{Q}{Q_{\text{тр}}} \geq 1$ – показатель, характеризующий возможность системы беспроводного доступа военного назначения обеспечить требуемое качество информационного обмена для всех должностных лиц системы.

3. При $W < 1$ повышение качества информационного обмена в системе беспроводного доступа специального назначения обеспечивается путем повышения пропускной способности с применением метода динамического управления с применением прогнозирования при заданных ограничениях на другие показатели эффективности.

4. При недостаточной эффективности применяемых методов, а также для дальнейшего повышения качества информационного обмена применяются ранее разработанные алгоритмы рационального распределения выделенного для системы частотного ресурса беспроводных сетей (изменение сигнально-кодовых конструкций), в зависимости от цели и сложившихся на данный момент условий функционирования сети: для не приоритетного обслуживания; согласно приоритета пользователей; формирование подканалов одинаковой ширины частотного спектра, либо обеспечение одинаковой скорости передачи в подканалах.

Таким образом, в настоящей статье проведен анализ современных методов и методик, применяемых для обеспечения качества информационного обмена, показана их неэффективность для применения в сетях беспроводного доступа специального назначения. Предложена методика управления качеством информационного обмена, которая ввиду относительной простоты и при достаточной

степени корректности может применяться в системах беспроводного широкополосного доступа специального назначения.

Литература

1. Легков К.Е., Кисляков М.А. Эксперимент по сбору трафика в сети беспроводного широкополосного доступа стандарта IEEE 802.16e // Сборник трудов СКФ МТУСИ - 2009. Ростов-на-Дону: СКФ МТУСИ, 2009. – С. 49-55.
2. Ghaderi M. On the Relevance of Self-Similarity in Network Traffic Prediction, 2003. <http://www.cs.uwaterloo.ca/cs-archive/CS-2003/28/TR-CS-2003-28.pdf>.
3. Traffic Modeling Based on FARIMA Models. Xue F., Liu J., Shu Y., Zhang L., Yang O.W.W // CCECE99 Proceed. – May 1999. – P. 162-167.
4. Chen B., Peng S., Wang K. Traffic Modeling, Prediction, and Congestion Control for High-Speed Networks: A Fuzzy AR Approach // IEEE Trans. On Fuzzy Systems Vol. 8. – 2000. – №5.
5. Chiruvolu G., Sankar R., Ranganathan N. Adaptive VBR Video Traffic Management for Higher Utilization of ATM Networks // ACM SIGCOMM, Vol. 28, Issue 3. – July 1998. – P. 27-40.
6. Легков К.Е., Донченко А.А. Анализ существующих алгоритмов распределения частотного ресурса беспроводных сетей специального назначения // Сборник трудов СКФ МТУСИ – 2009. Ростов-на-Дону: СКФ МТУСИ, 2009. – С. 50-52.
7. Донченко А.А., Легков К.Е. Анализ эффективности применения алгоритмов динамического управления пропускной способностью канала сети беспроводного широкополосного доступа // Сборник трудов СКФ МТУСИ – 2009. Ростов-на-Дону: СКФ МТУСИ, 2009. – С. 69-72.
8. Легков К.Е., Донченко М.А. Требования к показателям качества информационного обмена в сетях беспроводного широкополосного доступа // Сборник трудов СКФ МТУСИ – 2009. Ростов-на-Дону: СКФ МТУСИ, 2009. – С. 59-64.
9. Легков К.Е. Методы оценки качества информационного обмена в сетях беспроводного широкополосного доступа // Сборник трудов СКФ МТУСИ – 2009. Ростов-на-Дону: СКФ МТУСИ, 2009. – С. 64-68.

Пути защиты от угроз функционирования аппаратуры гражданских потребителей глобальных спутниковых радионавигационных систем

Проводится анализ угроз функционирования аппаратуры гражданских потребителей спутниковых радионавигационных систем и возможных путей защиты от рассматриваемых угроз.

Ключевые слова: спутниковая радионавигация, радиоэлектронное подавление, навязывание ложных сигналов.

Орёл Д.В.,
Ставропольский государственный университет

На сегодняшний день многие государства в мире в числе своих целей ставят обладание собственной спутниковой радионавигационной системой глобального или регионального характера, или спутниковой системой дифференциальной коррекции данных. В настоящее время функционируют две глобальных спутниковых радионавигационных системы (СРНС): российская Глонасс и американская Navstar GPS. Евросоюз и Китай в ближайшие годы планируют развёртывание своих глобальных спутниковых радионавигационных систем: Galileo и Compass соответственно. Кроме того, ряд государств обладает региональными спутниковыми радионавигационными системами, состоящими из двух-пяти спутников на геостационарных орбитах. Также в различных регионах мира развёрнуты спутниковые системы дифференциальной коррекции (SBAS).

Во всех рассматриваемых системах, в том числе в СРНС Глонасс, планируется использование технологии кодового разделения сигналов между спутниками. Структура сигналов с кодовым разделением каналов в рассмотренных системах достаточно схожа и имеет вид:

$$S(t) = A Q_i(t) D_i(t) \sin(2\pi L t + \phi),$$

$$i \in [1, n_{\text{ка}}] \quad (1)$$

где A — амплитуда сигнала; $Q_i(t)$ — манипулирующая функция, представляющая собой расширяющую последовательность; $D_i(t)$ — манипулирующая функция, представляющая собой передаваемые навигационные данные; L — несущая частота; ϕ — начальная фаза сигнала;

i — номер космического аппарата в системе; $n_{\text{ка}}$ — общее число космических аппаратов в системе.

Технологии координатно-временного обеспечения на основе спутниковой радионавигации с каждым годом всё более интегрируются в различные технические системы. Среди них можно выделить класс критических систем, нарушение функционирования которых зачастую может вызвать угрозу жизни и здоровью людей, экологической обстановке, экономическому благосостоянию региона. К таким критическим системам относятся, например, системы точной посадки самолётов и системы маневрирования судов в зоне морских и речных портов по сигналам СРНС. Подобные системы могут осуществлять управление судами в автоматическом и полуавтоматическом режимах, однако в настоящее время им отводится роль резервных систем информационного обеспечения по причине уязвимости аппаратуры гражданских потребителей (АГП) СРНС перед различными видами атак.

Среди видов возможных атак на АГП СРНС особо можно выделить следующие два:

- подавление навигационных радиосигналов с помощью организации радиопомех (jamming);
- навязывание ложных навигационных сигналов от псевдоспутников (spoofing).

Целью атаки подавления является блокирование навигационного сигнала, в результате которого АГП СРНС утрачивает возможность определять координаты и осуществлять синхронизацию с временной шкалой космического

Ways of protection against threats of functioning of equipment of civil customers of global satellite radio navigational systems

Oryol D.V.,
Stavropol State University

Abstract

Analysis of functioning threats for civil consumers equipment of global satellite radio navigating systems and analysis of possible ways of protection is made.

Keywords: satellite radio navigation, jamming, spoofing.

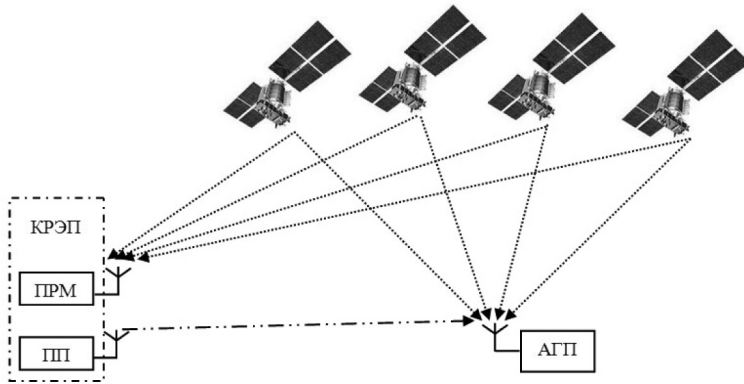


Рис. 1. Схема процесса радиоэлектронного подавления АПГ СРНС

аппарата СРНС. В случае потери сигнала от СРНС происходит переход на другую систему координатного или временного обеспечения. Если же навигационная подсистема, использующая СРНС, работает нормально, то зачастую полагаются только на её данные. В этом смысле более опасной является атака навязывания ложных навигационных сигналов, целью которой является отклонения объекта от требуемого местоположения. В данном случае навигационная задача будет решаться, и переход на резервную систему не произойдёт. Но координаты объекта будут определяться неверно, результатом чего может стать крушение судна. Навязывание ложного навигационного сигнала также можно рассматривать в качестве организации сигналоподобной радиопомехи.

Рассмотрим подробнее каждый тип атаки. Схема процесса радиоэлектронного подавления (РЭП) организованными помехами АПГ СРНС представлена на рис. 1, где АПГ — аппаратура гражданских потребителей, ПРМ — подсистема радиомониторинга, ПП — подсистема помех, КРЭП — комплекс радиоэлектронного противодействия.

Для РЭП АПГ СРНС пригодны активные организованные помехи, которые делятся на маскирующие и имитирующие. Активные маскирующие помехи создают на входе АПГ фон, который затрудняет обнаружение информационных сигналов и оценивание их параметров. Маскирующие помехи делятся на непрерывные шумовые помехи, хаотические импульсные помехи и последовательности детерминированных импульсных сигналов. Эффективность маскирующих помех зависит от соответствия временных, спектральных и статистических характеристик сигнала и помехи, а также от отно-

шения сигнал/помеха на входе АПГ. В качестве критерия эффективности помех при РЭП АПГ СРНС целесообразно использовать коэффициент подавления:

$$\eta_p = P_{SB}/P_{PD}; \quad P_{SB} = 2,5 \cdot 10^{-16} \text{ Вт} \quad (2)$$

где P_{SB} — максимальный ожидаемый уровень сигнала на входе АПГ; P_{PD} — уровень помехи $P(t)$ — на входе АПГ, достаточный для нарушения функционирования каналов первичной обработки АПГ.

Для РЭП АПГ СРНС из маскирующих помех наиболее пригодны прицельные и заградительные непрерывные шумовые помехи, которые реализуются на основе квазизелого шума (ШП) и гармонических процессов (ГП). Активные имитирующие помехи предназначены для внесения ложной информации в АПГ и перегрузки каналов первичной обработки инфор-

мации. Чтобы затруднить возможность компенсации имитирующей помехи, она должна формироваться процессом, сходным с навигационным сигналом. Имитирующие помехи, созданные генераторным методом, также называются сигналоподобными и относятся к классу "интеллектуальных" помех. Сигналоподобные помехи разделяются на прицельные, следящие и заградительные (ЗСП). К недостаткам следящей и прицельной сигналоподобных помех следует отнести сложность получения необходимых для их формирования целеуказаний. Более простой в реализации является заградительная сигналоподобная помеха, поскольку она не требует для формирования точных временных целеуказаний. Результаты исследований РЭП каналов АПГ при использовании шумовой, гармонической и заградительной сигналоподобной помех для случая штатного автономного функционирования АПГ приведены в таблице.

Из таблицы видно, что наименьшие энергетические затраты требуются для организации заградительных сигналоподобных помех, таким образом при равных показателях мощности КРЭП формируемые ЗСП будут эффективны на большем расстоянии, нежели ГП и ШП.

При подавлении радионавигационных сигналов СРНС опорные станции спутниковых систем дифференциальной коррекции могут оказаться не в состоянии сформировать дифференциальную поправку в случае нахождения в зоне действия КРЭП. Даже если дифференциальная поправка будет сформирована, её передача АПГ может оказаться невозможной в силу подавления КРЭП и этого спутникового

Показатели воздействия различных типов помех на АПГ СРНС

Канал АП	Тип помехи	Вероятность РЭП	Энергетический потенциал PnGn (дБВт)	Коэффициент подавления η_p
Канал обнаружения	ШП	$P_{P11} = 0,5$	8,5	$\eta_{p11} = 1,5 \cdot 10^{-3}$
	ГП	$P_{P11} = 0,5$	8,5	$\eta_{p12} = 1,5 \cdot 10^{-3}$
	ЗСП	$P_{P11} = 0,67$	- 9,5 -3,6	$\eta_{p13} = 5 \cdot 10^{-2}$ $\eta_{p13} = 10^{-1}$
Канал слежения за частотой	ШП	$P_{P12} = 0,32$	19,5	$\eta_{p21} = 2,5 \cdot 10^{-3}$
	ГП	$P_{P12} = 0,32$	24,4	$\eta_{p22} = 4,17 \cdot 10^{-3}$
Канал слежения за задержкой	ШП	$P_{P13} = 0,5$	10,4	$\eta_{31} \in 4,3 \cdot 10^{-6}, 10^{-3}$
	ГП	$P_{P13} = 0,5$	54	$\eta_{32} \in 4,3 \cdot 10^{-10}, 10^{-7}$
	ЗСП	$P_{P13} = 0,67$	- 9,5 -3,6	$\eta_{p33} = 5 \cdot 10^{-3}$ $\eta_{p33} = 10^{-1}$
Канал демодуляции	ШП	$P_{P14} = 0,1$	18,7	$\eta_{p41} = 8,3 \cdot 10^{-4}$
	ГП	$P_{P14} = 0,1$	18,7	$\eta_{p42} = 2,5 \cdot 10^{-5}$

сигнала. В случае успешного приёма дифференциальной поправки она окажется бесполезной при подавленных навигационных сигналах СРНС.

Возможными путями повышения защищённости АГП СРНС от воздействия ГП и ШП может служить увеличение мощности и расширение спектра навигационного сигнала. Однако реализация данных мер ограничивается международными договорённостями об использовании радиочастотного ресурса. Кроме того, данные меры будут менее эффективны в случае использования ЗСП. Возможным методом повышения защищённости АГП СРНС от ЗСП может служить повышение структурной скрытности СРНС путём стохастического использования неповторяющихся квазиортогональных кодовых последовательностей в качестве $Q_i(t)$ в (1).

Рассмотрим теперь второй тип атак на АГП СРНС — навязывание ложных навигационных сигналов от псевдоспутников. На рынке имеются устройства, позволяющие имитировать сигналы СРНС. Они способны воспроизводить точные копии сигналов, транслируемых спутниками, имитировать воздействие помех и различные виды задержек сигналов. Эти устройства применяются для тестирования навигационных приёмников в лабораторных условиях, используются в качестве псевдоспутников для обеспечения работоспособности АГП СРНС в условиях, когда распространение сигналов от спутников затруднено. Доступность подобных комплексов и квалифицированных специалистов обуславливает возможность реализации атаки типа "спуфинг".

Рассмотрим процесс решения навигационной задачи АГП СРНС методом определения псевдодальностей. Для определения местоположения в дискретный момент времени требуется решение системы уравнений вида:

$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2 = ([t_r + b-t_1]c)^2 \\ (x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2 = ([t_r + b-t_2]c)^2 \\ (x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2 = ([t_r + b-t_3]c)^2 \\ (x-x_4)^2 + (y-y_4)^2 + (z-z_4)^2 = ([t_r + b-t_4]c)^2 \end{cases} \quad (3)$$

где x, y, z — координаты приёмника; t_r — время приёмника; b и c — неопределённости, порождаемые задержкой сигналов в среде распространения; x_i, y_i, z_i, t_i — данные, передаваемые в навигационном сообщении (координаты и время спутника). Манипулирование этими данными ведёт к неверному определению местоположения и позволяет формировать ложный курс следования подвижного объекта.

При навязывании ложных навигационных сигналов СРНС системы дифференциальной коррекции могут быть подавлены организованными помехами или их сигналы также могут быть подменены ложными. Даже в случае, если работа спутниковых систем дифференциальной коррекции не будет учтена при организации атаки "спуфинг", она окажет воздействие лишь на точность определения координат в пределах одного метра, но не помешает основной цели атаки.

Одним из возможных путей защиты от навязывания ложных навигационных сигналов может быть шифрование навигационных сообщений. При этом потребуется организация режима распределения ключей среди потребителей и возможность смены ключей при их компрометации, что потребует дополнительного канала связи между АГП и сегментом управления СРНС. В силу непрерывного характера трансляции навигационного радиосигнала и доступности его приёма в любой точке существенно упрощается задача криптоанализа. Шифрование навигационных данных позволит повысить защищённость сигнала только от навязывания, в то же время не окажет влияния на возможность организации помех.

Альтернативным путём комплексной защиты АГП СРНС, как от навязывания ложных навигационных сигналов, так и от организованных радиопомех может являться повышение структурной скрытности навигационных радиосигналов. При этом существенно усложняется задачи формирования ложного навигационного сигнала и формирования ЗСП, так как возникает необходимость радиомониторинга навигационных радиосигналов СРНС в реальном времени. В случае, если алгоритм формирования манипулирующих функций $Q_i(t)$ не будет раскрыт системой радиомониторинга, а количество самих манипулирующих функций будет настолько большим, чтобы использовать их без повторения в течении времени T , то СРНС будет являться защищённой от рассмотренных типов атак в течение времени T .

www.kitel.kz

Организаторы:



Iteca Almaty:
Тел.: +7 (727) 258 34 34
Факс: +7 (727) 258 34 44
e-mail: telecoms@iteca.kz
Наталья Дмитриева



ITE Moscow LLC:
Тел.: +7 (495) 935 7350 #4123
Факс: +7 (495) 935 7351
e-mail: Kochergina@ite-expo.ru
Елена Кочергина

