МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

К защите допустить
Зав. Кафедрой ТИ
доцент А.М.Эшмурадов
«____»_____2015 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему **Анализ функционирования наложенных сетей в сетях телекоммуникации**

Выпускник	_____	Нигматов Д.И.
	подпись	ф.и.о.
Руководитель	_____	Хайтбаев А.Ф.
	подпись	ф.и.о.
Рецензент	_____	Нурушов С.И.
	подпись	ф.и.о.
Консультант по БЖД	_____	Абдуллаева С.М.
	подпись	ф.и.о.

Ташкент – 2015

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Факультет ТТ Кафедра ТИ

Направление 5311300 - Телекоммуникация

У Т В Е Р Ж Д А Ю

Зав. Кафедрой ТИ _____

«____»_____2015 г.

ЗАДАНИЕ

на выпускную квалификационную работу студента Нигматова Давронбека Исматилла угли

(фамилия, имя, отчество)

на тему Анализ функционирования наложенных сетей в сетях телекоммуникации

1. Тема утверждена приказом по университету от 25.12.2014 г.№ 1467
2. Срок сдачи законченной работы 31.05.2014г.
3. Исходные данные к работе Материалы изысканий, полученные при прохождении производственной практике.
4. Содержание расчётно-пояснительной записки (перечень подлежащих к разработке вопросов) 1. Понятия о наложенной сети 2. Синтез наложенных телекоммуникационных сетей. 3. Анализ функционирования наложенных сетей в сетях телекоммуникации 4. Безопасность жизнедеятельности.
5. Перечень графического материала Презентационные материалы.
6. Дата выдачи задания 16.01.2015 г.

Руководитель _____

подпись

Задание принял _____

подпись

7. Консультанты по отдельным разделам выпускной работы**:**

Наименование раздела	Консультант	Подпись, дата	
		Задание выдал	Задание получил
Основная часть	Хайтбаев А.Ф.	15.01.2015 г.	15.01.2015г.
БЖД	Абдуллаева С.М.	23.03.2015 г.	23.03.2015г.

8. График выполнения работы

№	Наименование раздела	Срок выполнения	Подпись руководителя (консультанта)
1.	Понятия о наложенной сети	13.02.2015 г.	
2.	Синтез наложенных телекоммуникационных сетей	24.03.2015 г.	
3.	Анализ функционирования наложенных сетей в сетях телекоммуникации	21.04.2015 г.	
4.	Безопасность жизнедеятельности	15.05.2015 г.	

Выпускник _____ « » _____ 2015 г.
подпись

Руководитель _____ « » _____ 2015 г.
подпись

Данная выпускная квалификационная работа посвящена анализа функционирования наложенных сетей в сетях телекоммуникация, благодаря которой появляется возможность определить вероятностные характеристики сетей доступа. С этой целью в работе приведен обзор наложенных сетей, предлагаются рекомендации по выбору технологий сетей доступа.

В разделе безопасности жизнедеятельности описано меры по электрической безопасности и эргономические основы безопасности жизнедеятельности человека.

Ушбу битирув малакавий иши телекоммуникация тармоқларида устма - уст тармоқнинг ишлаши таҳлил қилинган. Устма - уст тармоқнинг қурилиш усуллари кўриб чиқилган. Телекоммункация тармоқларида устма - уст тармоқда маълумотларни алмашиш абонент кириш тармоғида эҳтимоллик характеристикасини аниқлашга имкон яратади. Шу мақсадда ушбу ишда устма - уст тармоқда тармоқни самарадорлигини орттириш муқобил технология тавсия қилинган.

Шунингдек битирув ишида инсоннинг меҳнати муҳофазаси ва электрдан муҳофаза чоралари кўрилган ҳамда инсон компьютер билан ишлаганда унинг ҳаёти фаолияти хавфсизлиги масалалари кўриб чиқилган.

This final graduation work is devoted to the analysis of performance of overlay network in telecommunication network. Building principles of overlay network is considered. Analyzing overlay network in telecommunication network gives possibility to determine the probabilistic characteristics of the access networks. To this reason in this work recommended optimal technology to increase performance in overlay network.

In the life safety measures described on electrical safety, ergonomics and safety fundamentals of human life.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время известны и широко используются в городских условиях следующие средства для организации "последней мили": телефонные медные провода; волоконно-оптические кабели; телевизионные кабельные сети; радиоэфир (технология "радио-Ethernet"); каналы спутникового телевидения.

В постановлении Президента Республики Узбекистан «О государственной программе «Год благополучия и процветания» отмечается: «В 2013-2014г.г. будет проводится ускоренное формирование системы «Электронное правительство» по направлениям взаимодействия с использованием информационно-коммуникационных технологий G2G (органы государственной власти между собой), G2B (органы государственной власти с субъектами предпринимательства), G2C(органы государственной власти с гражданами), предусматривающее расширение возможностей доступа населения к интерактивным услугам за счёт развития оптических сетей широкополосного доступа по технологии FTTx.

Возможности высокоскоростной передачи данных долгие годы не распространялись на миллионы представителей мелкого бизнеса и частных абонентов, которые по понятным экономическим соображениям не могут себе позволить содержать выделенную оптико-волоконную линию. И хотя потребность этих групп абонентов в технологиях цифровой передачи постоянно росла и растет, до последнего времени им оставалось полагаться только на те средства передачи данных, которые используют линии телефонной сети общего пользования.

Рассмотрение эволюции сетей связи с точки зрения предоставляемых услуг позволяет обосновать появление сетей следующего поколения как результат конвергенции существующих сетей. Анализ принципов построения NGN (Next Generation Networks) с точки зрения функциональной архитектуры является одним из основных моментов в понимании структуры и назначения сетей следующего поколения.

Современные тенденции в сфере информационно коммуникационных технологий указывают на то, что сеть абонентского доступа получает все более широкое признание в качестве основной инфраструктуры любой современной экономики и имеет решающее значение в содействии социально-экономическому развитию. Использование в сетях абонентского доступа широкополосные технологии играют центральную роль в поддержке новейших приложений и услуг, включая приложения и услуги электронного правительства, здравоохранения, образования и т.д.

Построение сетей на базе концепции NGN не представляется целесообразным без развития инфраструктуры широкополосного доступа. При этом следует обеспечить постоянное повышение доступности данной инфраструктуры для населения, т.е. ее универсализацию. Таким образом, можно сказать, что универсализация широкополосного доступа следует рассматривать как одно из направлений, обеспечивающих развитие сетей NGN, а также как меру содействия социально-экономическому развитию страны.

Цифровизация сети доступа и увеличение ее пропускной способности с целью предоставления абонентам комплекса услуг, включая интерактивную цифровую высокоскоростную связь и услуги мультимедиа, является приоритетными задачами при развитии сетей доступа.

Во всем мире развитие сетей доступа происходит по двум основным путям:

– использование существующих кабельных линий;

– строительство новых оптических линий связи.

Использование волоконно-оптических средств на сетях доступа позволяет реализовать:

– передачу по тем же оптическим волокнам программ кабельного телевидения;

– создание цифровых сетей с интеграцией услуг, включая услуги мультимедиа.

При этом капитальные затраты на технические средства сети доступа практически не меняются для любого варианта. Может увеличиваться только стоимость терминального оборудования и оплата услуг по мере увеличения их количества и качества.

Кроме того, оптические сети доступа имеют возможность одновременного удовлетворения как потребителей, которым нужен традиционный телефонный аппарат, так и потребителей, которым требуется широкополосный канал, включая кабельное телевидение.

Таким образом, реализация системы распределения сетевого трафика на уровне наложенной сети не затрагивает работающих на нижних уровнях традиционных протоколов маршрутизации, позволяя избежать крайне нежелательной процедуры модификации существующих принципов.

Можно выделить две основные цели, достигаемые созданием наложенной сети: конструируется виртуальная топология сети, в которой может быть реализована произвольная (например, многопутевая) маршрутизация, в то время как физическая сеть продолжает управляться традиционными протоколами, использующими кратчайшие пути и организуется взаимодействие узлов сети, принимающих участие в работе децентрализованной системы управления трафиком.

1. ПОНЯТИЯ О НАЛОЖЕННОЙ СЕТИ

Наложенная сеть (от англ. Overlay Network) — общий случай логической сети, создаваемой поверх другой сети. Узлы наложенной сети могут быть связаны либо физическим соединением, либо логическим, для которого в основной сети существуют один или несколько соответствующих маршрутов из физических соединений. Примерами наложенной сети являются сети VPN и одноранговые сети, которые работают на основе интернета и представляют из себя «надстройки» над классическими сетевыми протоколами, предоставляя широкие возможности, изначально не предусмотренные разработчиками основных протоколов. Коммутируемый доступ в интернет фактически осуществляется через оверлей (например, по протоколу PPP), который работает «поверх» обычной телефонной сети.

Таким образом, реализация системы распределения сетевого трафика на уровне наложенной сети не затрагивает работающих на нижних уровнях традиционных протоколов маршрутизации, позволяя избежать крайне нежелательной процедуры модификации существующих принципов [1].

Можно выделить две основные цели, достигаемые созданием наложенной сети:

- конструируется виртуальная топология сети, в которой может быть реализована произвольная (например, многопутевая) маршрутизация, в то время как физическая сеть продолжает управляться традиционными протоколами, использующими кратчайшие пути;
- организуется взаимодействие узлов сети, принимающих участие в работе децентрализованной системы управления трафиком.

Организации передачи трафика в виртуальной топологии наложенной сети может осуществляться различными способами, среди которых стоит отметить технику создания виртуальных каналов, инкапсуляцию транзитного трафика, маршрутизацию от источника и т. п. Как уже было отмечено, основным достоинством наложенной маршрутизации является отсутствие

необходимости интеграции и вмешательства в существующие протоколы. Вторая отмеченная задача, а именно самоорганизация сети, требует специального рассмотрения.

1.1 Самоорганизующиеся наложенные сети

На сегодняшний день, как показано в работе [2], существует множество различных типов наложенных сетей, объединённых стремлением упростить взаимодействие между узлами-участниками, абстрагировавшись от реальной сложной сетевой топологии. Не каждая наложенная сеть является самоорганизующейся, однако использование принципа самоорганизации позволяет избежать необходимости вмешательства оператора, превращая первую в полностью автономную сетевую структуру, что, как уже было указано ранее, является общей тенденцией развития в пространстве Интернета Вещей. В отличие от традиционной клиент-серверной архитектуры, самоорганизующиеся наложенные сети, как правило, образованы множеством равноправных узлов, каждый из которых может выступать как в роли клиента, так и в роли сервера [3]. Ярким примером такой архитектуры являются P2P-сети (peer-to-peer) [4]. Любой узел данной сети не гарантирует своего присутствия на постоянной основе, произвольно подключаясь/отключаясь от оверлея. Реализация такого подхода позволяет значительно повысить отказоустойчивость и теоретически сохранять работоспособность сети при любом количестве и сочетании доступных узлов. Все существующие самоорганизующиеся сети можно классифицировать по следующим параметрам [5].

- Архитектура сети:
  - неструктурированные,
  - структурированные.
- Степень централизации:
  - централизованные,

- частично централизованные;
- децентрализованные.

– Топология сети:
  - одноранговые,
  - иерархические (многоуровневые).

Прогнозы роста нагрузки в сетях доступа. Каждый год исследовательский отдел компании Cisco Systems, Inc. публикует аналитические материалы, посвященные оценке текущего объема данных, передаваемых в мвсштабах глобальной сети, а также прогнозу роста на ближайшие годы. Ежегодный отчет носит название Cisco Visual Networking Index (VNI) и находится в открытом доступе. Как показывает время, прогнозы компании довольно точны и отличаются от фактических данных примерно на 2-10%. Очень интересной характеристикой с точки зрения построения сетей доступа является прогнозируемое количество пользовательского трафика. Динамика роста этого показателя, представленная в отчете [6], приведена в рис.1.1

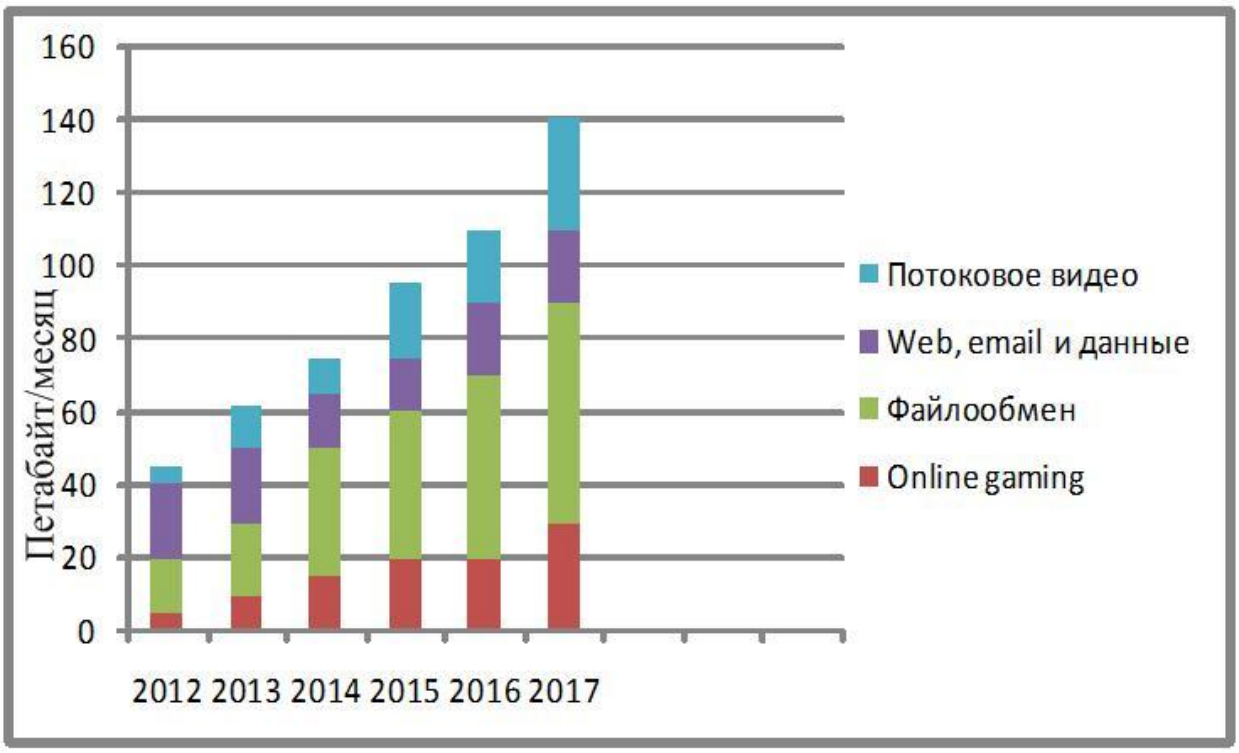


Рис. 1.1 Структура пользовательского трафика Интернета

Как можно заметить из приведенного графика, помимо общего экспоненциального роста объема передаваемых данных, в составе пользовательского трафика меняются количественные соотношения. Например, все более значительным становится вклад трафика онлайн-игр и потокового видео. Данные виды трафика отличаются большей критичностью к таким показателям качества обслуживание(QoS), как задержка и джиттер.

Помимо традиционной, хорошо прогнозируемой клиент-серверной модели организации взаимодействия, использующей для доставки контента традиционные сетевые протоколы, существует другой способ - так называемы наложенные сети. Наложенная сеть (или оверлей) в обще случае представляет собой некоторою логическую сеть, организованную поверх существующей физической инфраструктуры и являющуюся надстройкой над стандартными сетевыми протоколами. Рассмотрим подробное существующее сегодня многообразие наложенных сетей по областях их применения.

Потоковое видео. Согласно уже упомянутому прогнозу Cisco VNI, доля пользовательского видеотрафик к 2017 г. вырастет и будет согласно 69% всего пользовательского трафика (на данный момент -около 57%). Эта цифра не включает видео, полученное посредством P2P - файлообмена. Если же учесть все виды трафика видео, то к 2017 г. этот тип данных будет доминировать, составляя около 80-90% всего пользовательского трафика.

Доставка больших объемов онлайн-видео до конечных пользователей через Интернет может осуществляться с помощью технологий OTT, CDN или потоковых P2P приложений. Технология OTT (Over The Top) представляет собой разновидность IPTV, реализующую доставку легального видеоконтента по общему каналу доступа в Интернет без построения собственной сети передачи данных (ПД) или аренды ресурсов у оператора связи. Преимуществом использования P2P - технологий является возможность одновременного просмотра некоторого видеоконтента множеством пользователей. Данное свойство особенно актуально при

организации трансляций массовых мероприятий, концентров, спортивных матчей и т.п.

Каждый пользователь, просматривая некоторый видеоролик, становится одним из множества серверов, предоставляющих другим пользователям доступ к уже загруженным частям видео. Указанным способом осуществляется децентрализованное кэширование данных, значительно снижающее нагрузки на сервер-источник и магистральные сети, но вызывающее усиленное использование ресурсов сети доступа. Здесь большее число просматривающих видеоролик означает большее количество узлов наложенной сети, осуществляющих репликацию данных, благодаря чему качество доставки контента улучшается, в отличие от традиционной клиент-серверной архитектуры.

Принцип работы потоковых P2P -приложений близок к широко известным файлообменным P2P-сетям. Иногда в отдельный подвид выделяют системы P2P-TV, представляющие собой описанные потоковые P2P- приложения, предназначенные для просмотра каналов Интернет ТВ. Среди популярных P2P-сетей потокового вещания можно упомянуть BitTorrent Live, TorrentStream, PPlive, UUSee, SopCast и др. Существуют также различные P2P -реализации потоковых аудиоплееров, Интернет-радио и т.д., однако доля трафика, создаваемого такими приложениями, незначительна на фоне передачи видеопотоков.

Виртуальные операторы услуг связи. Одними из наиболее активных генераторов трафика в сетях доступа являются таким операторы услуг связы. Яркие представители таких операторов- система частично децентрализованной Интернет-телефонии Skype, различные VoIP-сервисы, такие как SIPnet, TeLme, PCTEL и мн. др. Особенность работы выртуального оператора - использование в качестве среды ПД физической инфраструктуры других операторов. При этом работа виртуального оператора никак не согласуется с возможностями конкретных сегментов сети оператора "трубы", не рассчитанных на подобную нагрузку.

1.2 Архитектура наложенной сети

Неструктурированные сети принято относить к первому поколению наложенных сетей (оверлеев), тогда как структурированные – ко второму, однако такое разделение основывается лишь на моменте появления соответствующих алгоритмов, и не является показателем их актуальности или распространенности в современных сетях [3]. Отличительной особенностью неструктурированных сетей по определению является отсутствие четкой упорядоченности архитектуры. Расположение узлов в такой сети не связано с идентификаторами первых или хранимой на них информацией, а методы поиска данных варьируются от простых лавинных рассылок до случайных блужданий (RW) и более избирательных семантического и эвристического поиска [11]. Недостатками указанных методов поиска являются избыточная нагрузка на сеть, отсутствие гарантий нахождения данных, а также плохая масштабируемость. Можно отметить некоторые характерные отличия рассматриваемых неструктурированных оверлеев [12].

- Объемы таблиц маршрутизации узлов не зависят от количества активных участников сети и являются фиксированными величинами.
- Отсутствует единая точка отказа или ей являются элементы частичной централизации, такие как серверы регистрации, трекеры и т.п.
- Трудно дать количественную оценку сложности нахождения данных.
- Подключение/отключение случайных узлов практически не влияет на функционирование остальной части сети.

В качестве примеров неструктурированных самоорганизующихся сетей можно привести файлообменные пиринговые сети, такие как Gnutella, FastTrack/KaZaa, BitTorrent, первоначальный дизайн P2P-VoIP системы Skype, P2P-систему доставки потокового трафика CoolStreaming, сенсорные сети, различные ad-hoc сети и т. д.

Самоорганизующиеся структурированные сети подчиняются строгой системе упорядочивания узлов на основе особых математических структур, таких как распределенные хэш-таблицы (DHT), кольца, сетки, многомерные координатные пространства [11] и т. п. Каждый узел получает уникальный идентификатор, однозначно указывающий на его место в сети относительно других узлов. Жесткая структура позволяет гарантировать нахождение конкретного узла по его идентификатору, при этом сложность поиска растет, как правило, не быстрее логарифма количества узлов в сети. Размер таблиц маршрутизации узлов структурированной сети чаще всего также пропорционален логарифму общего числа участников [12]. Следует отметить, что структурированные сети в силу особенностей архитектуры сильнее подвержены влиянию динамики популяции узлов. Отключение действующего узла или подключение нового вызывает выполнение ряда процедур, затрагивающих некоторую часть узлов сети и связанных с перестроением таблиц маршрутизации. Данный факт несколько ограничивает применение структурированных архитектур в условиях высокой динамики популяции [11]. Примерами структурированных сетей являются протоколы CAN, Chord, Tapestry, Pastry, Kademlia, Viceroy, распределенная система хранения данных OceanStore, исследовательский комплекс PlanetLab, масштабируемые многоадресные
CDN-системы SplitStream, Scribe и многие другие.

Помимо рассмотренных типов организации сетей существуют также гибридные варианты, совмещающие подходы структурированных и неструктурированных архитектур. Примером такой слабоструктурированной сети является сеть Freenet, поиск узла в которой осуществляется способом, близким к методу случайных блужданий, однако направление поиска задается близостью идентификаторов соседних узлов к искомому.

В отдельную группу самоорганизующихся наложенных сетей следует выделить анонимные сети [11]. Рассматривая такие сети с точки зрения генерируемого ими трафика можно выделить следующую особенность,

отличающую их от всех других наложенных сетей: для повышения безопасности анонимные сети намеренно выбирают субоптимальные маршруты при передаче данных. Это означает, что некоторый узел после нахождения требуемого ресурса, обменивается данными с последним через цепочку других узлов наложенной сети, при этом путь прохождения таких данных с точки зрения физической сети является неоптимальным. Важно подчеркнуть данный подход, как иллюстрирующий возможности организации произвольной схемы маршрутизации трафика на базе наложенной сети. Примерами самоорганизующихся анонимных сетей являются Freenet, Hordes, TOR, I2P и другие.

Степень централизации. Как уже было отмечено выше, самоорганизующиеся сети могут отличаться различной степенью централизации управления. Можно выделить три группы: централизованные, сети с частичной централизацией и полностью децентрализованные сети. Архитектура централизованной сети содержит набор серверов, обеспечивающих поиск данных в сети, а также хранящих адреса узлов-участников. Все запросы узлов обрабатываются на центральных серверах, после чего узел-инициатор получает информацию об искомых данных и адреса узлов, готовых их представить. Такая схема является наиболее простой в реализации, эффективной с точки зрения поиска ресурсов и объемов служебного трафика. Однако в то же время степень самоорганизации сети значительно снижается за счет присутствия центральных элементов, являющихся потенциальными точками отказа. Примером типичной централизованных сетей является Napster [11].

Полностью децентрализованные сети лишены недостатков, связанных с возможностью потери работоспособности в результате отказа некоторых узлов. Информация об участниках децентрализованного оверлея, данные, а также сетевой функционал распределены по всем узлам, так что отключение части узлов не отразится на работе сети, при этом наибольшей отказоустойчивостью обладают неструктурированные децентрализованные

сети [11]. В качестве примеров полностью децентрализованных сетей можно указать Gnutella, FastTrack, P-Grid и другие.

Комбинированное решение, представляющее собой децентрализованный оверлей, содержащий ряд элементов централизации (вспомогательных серверов), получило название частично децентрализованной архитектуры. Такие сети обладают не только высокой отказоустойчивостью, но также позволяют производить быстрый и эффективный поиск узлов и данных с помощью группы центральных серверов, обменивающихся актуальной информацией. Примерами частично децентрализованных сетей являются Overnet/eDonkey , BitTorrent, а также (до недавних пор) P2P-VoIP система Skype.

1.3 Топология сети

Топология самоорганизующейся сети может быть либо одноранговой (плоской), либо подразделяться на несколько логических уровней (обычно, не более двух), образуя иерархическую структуру. В одноранговой наложенной сети все узлы являются равноправными, и за счет полносвязности оверлея любая пара узлов может обмениваться данными напрямую. Примерами одноранговых сетей являются Gnutella v0.4, Freenet, CAN, Chord, Kademlia и другие.

В случае создания многоуровневой сети некоторые участники на основании объективных показателей (таких как производительность, пропускная способность и т. п.) получают особый статус «суперузла». Все остальные узлы многоуровневой сети могут обмениваться данными только через свои родительские суперузлы, выступающие в роли транзитных. При этом суперузлы, как правило, объединяются в плоскую полносвязную логическую топологию. В качестве примеров иерархических наложенных сетей можно указать FastTrack/KaZaA, Gnutella v0.6, Skype, CAP, Brocade и другие.

Оверлеи могут применяться в следующих случаях:

- Для исследования, разработки и тестирования новых протоколов связи, невозможных в традиционной инфраструктуре (например, исследование свойств IPv6 или связи «один-со-многими»);
- Для создания новых свойств сети, невозможных в традиционной инфраструктуре:
  - Маршрутизация с гарантией качества сервиса,
  - Инфраструктура, более подходящая для трансляции потоков информации (Akamai),
  - Более гибкая, эффективная и надежная маршрутизация (Resilient Overlay Networks, Chord),
  - Повышенная безопасность соединения (Secure Overlay Services, VPN),
  - Полностью распределённая инфраструктура сети (Tapestry),
  - Маршрутизация без определения целевого IP-адреса (Distributed Hash Table);
- Для создания и эксплуатации сервисов, невозможных в традиционной инфраструктуре:
  - Распределённое хранение информации, файлообмен (OceanStore),
  - Распределённые вычисления.

Основное преимущество наложенных сетей заключается в том, что они позволяют разрабатывать и эксплуатировать новые крупномасштабные распределённые сервисы без внесения каких-либо изменений в основные протоколы сети. Распространённым недостатком оверлеев являются повышенные затраты при передаче информации из-за дополнительного уровня обработки пакетов или неоптимальных маршрутов.

Распределённая хеш-таблица. DHT (англ. Distributed Hash Table — «распределённая хеш-таблица») — это класс децентрализованных распределённых систем, которые обеспечивают поисковый сервис, похожий

по принципу работы на таблицу хешей, которая имеет структуру ассоциативного массива: (ключ и значение), хранящиеся в DHT, а каждый участвующий узел может рационально искать значение, ассоциированное с данным ключом. Ответственность за поддержку связи между именем и значением распределяется между узлами, таким образом изменение набора участников является причиной минимального количества разрывов. Это позволяет легко масштабировать DHT и постоянно отслеживать добавление/удаление узлов и ошибки в их работе.

DHT — это инфраструктура, которая может быть использована для построения многих комплексных сервисов, таких как распределенные файловые системы, пиринговое распространение файлов и системы распространения контента, кооперативный web-кэш, многоадресная доставка (multicast), anycast, сервис доменных имен и система мгновенных сообщений. Основные распределенные сети, которые используют DHT, включают в себя сеть I2P, BitTorrent, eDonkey, YaCy, Tox и Coral Content Distribution Network.

Существует возможность создания поисковых машин по сети DHT. Изыскания в области DHT изначально были мотивированы в частности пиринговыми системами, такими, как I2P, Napster, Gnutella, Freenet, которые использовали распределенные в интернете ресурсы для создания одного единственного приложения. В частности они использовали широкополосный интернет и пространство на жестких дисках для предоставления сервиса распространения файлов. Эти системы различаются тем, как они находили данные пиров:

Napster имел центральный индексный сервер: каждый узел, после присоединения, должен отправить список локально хранящихся файлов на сервер, который должен произвести поиск и направить запрос к узлам, содержащим результаты. Этот центральный компонент делал систему уязвимой для атак и рисков.

Gnutella и похожие сети двинулись к модели лавинных запросов — в основном, каждый поиск привел бы к сообщению, передаваемому на любую

машину в сети. Избегая централизованного отказа, этот метод был значительно менее эффективным, чем Napster.

Freenet был также полностью распределенным, но маршрутизация работает на базе эвристического ключа, в котором каждый файл имеет ассоциированный с ним ключ, а файлы с похожими ключами имели тенденцию к объединению в кластеры на похожем наборе узлов. Запрос, скорее всего, направлялся таким кластерам без надобности опрашивать всех пиров. Однако Freenet не мог гарантировать, что данные будут найдены.
DHT используют маршрутизацию на базе более структурированного ключа, чтобы достигнуть децентрализации I2P, Gnutella и Freenet, а также эффективности и гарантируемых результатов Napster. Один из недочетов в том, что, как Freenet, DHT поддерживает только поиск по точному совпадению, а не по ключевым словам, хотя эти возможности могут наслаиваться поверх DHT.

Первые четыре DHT — CAN, Chord, Pastry и Tapestry — были введены приблизительно в 2001 году. С тех пор эта область изысканий была достаточно активна. Вне научных кругов DHT-технологию приняли как компонент BitTorrent и Coral Content Distribution Network

DHT характеризуется следующими свойствами:

- Децентрализация: форма системы коллективных узлов без координации;
- Масштабируемость: система будет одинаково эффективно функционировать при тысячах или миллионах узлов;
- Отказоустойчивость: система будет одинаково надежна (в некотором смысле) с узлами постоянно подключающимися, отключающимися и выдающими ошибки.

Ключевая методика достижения цели заключается в том, что любой узел должен скоординироваться только с несколькими узлами в системе — как правило, O (logn), где n — количество участников так, чтобы только

ограниченный объем работы был сделан для каждого изменения количества участников.

Некоторые DHT-проекты стремятся обеспечить защиту от вредоносных пользователей и позволять участникам оставаться анонимными, хотя это меньше распространено, чем во многих других P2P-системах (особенно при распространении файлов);

Наконец, DHT приходится иметь дело с более традиционными распределенными системами, такими как распределение нагрузки, целостность данных и производительность (в частности, гарантируя, что операции, такие как маршрутизация и хранение данных или поиск, завершаются быстро).

Структура. Структура DHT может быть разбита на несколько основных компонентов. Она основывается на абстрактном пространстве ключей (keyspace), таком как набор 160-битных строк (количество бит может варьироваться). Схема разбиения пространства ключей распределяет принадлежность ключей среди участвующих узлов. Затем оверлейная сеть соединяет узлы, помогая найти владельца любого ключа в пространстве ключей.

Когда все компоненты на месте, типичное использование DHT для хранения и выдачи информации происходит следующим образом: Предположим, keyspace составляет 160-битные строки. Чтобы сохранить файл с данным именем и информацией в DHT, находится SHA1 хеш от имени файла, из которого формируется 160-битный ключ k, после чего формируется сообщение put(k, data) и посылается любому участвующему узлу в DHT. Послание идёт от одного узла к другому через оверлейную сеть до тех пор, пока оно не достигнет единственного узла, ответственного за ключ k, в соответствии со схемой разбиения keyspace, где и будет храниться пара (k, data). Любой другой клиент может получить содержание файла сделав ключ (k), т.е. получив хеш имени файла, для того, чтобы найти данные, связанные с ключом, послав сообщение get(k). Сообщение снова

пройдёт через оверлей к узлу, ответственному за ключ, который ответит, что нужные данные есть в наличии.

Компоненты разбиения пространства ключей и оверлейной сети описаны ниже с целью представления основных идей обычных для большинства DHT систем. Многие разработки отличаются в деталях.

DHT и BitTorrent. DHT и PEX фактически выполняют основную функцию BitTorrent-трекера — помогают участникам файлообмена узнать друг о друге. Они могут: Помочь участникам быстрее найти друг друга. Например, на раздаче есть пир X с недоступным портом. К раздаче подключается пир Z, который не может сам начать соединение с X и вынужден ждать, пока X о нём узнает. X только что обращался к трекеру и в следующий раз собирается это сделать через час. Но вот пир Y в очередной раз обращается к трекеру и узнаёт про нового пира Z. При этом Y сам давно уже соединён и занимается файлообменом с X, поэтому он через PEX сообщает X адрес этого нового пира. Теперь X может начать соединение с Z.

Снизить нагрузку на трекер. Получая адреса пиров через DHT или PEX, клиенты реже обращаются к трекеру, тем самым снижая нагрузку.

Поддержать раздачу в периоды недоступности трекера. Если трекер является единственным источником информации о пирах, то при его неработоспособности раздача постепенно остановится. Используя PEX, клиенты могут обмениваться друг с другом информацией о пирах, с которыми у них были сеансы связи, тем самым замедляя процесс остановки раздачи. DHT же позволяет полностью заменить трекер.

DHT позволяет раздавать без трекера. Такая раздача называется trackerless. Торрент для неё создаётся без адреса трекера и клиенты находят друг друга через DHT. Правда при этом, начавший раздачу должен иметь реальный ip-адрес, доступный извне. При участии в trackerless-раздачах BitTorrent-клиенты приобретают определённое сходство с eMule, использующим сеть Kad.

Private key. В публичных (открытых) трекерах, где каждый желающий может скачать торрент и участвовать в раздаче, DHT и PEX служат на благо всех участников.

Частным (закрытым) трекерам в первую очередь важно, чтобы в раздачах могли участвовать только зарегистрированные пользователи и чтобы они соблюдали определённые правила. При первом обращении клиента частный трекер имеет возможность не допустить его к раздаче, просто не сообщая ему адреса других клиентов-участников. Поэтому для закрытого трекера важно, чтобы клиенты не получали эти адреса через DHT/PEX.

DHT и PEX появились в клиентах Azureus и BitComet примерно летом 2005 года. Администраторы многих частных трекеров были недовольны такой новой функциональностью и поэтому стали запрещать на трекере эти новые версии клиентов. Тогда разработчики клиентов предложили новый ключ внутри торрент-файла: private. Если он равен 1, то клиент обязан для этого торрента автоматически отключать DHT/PEX независимо от желания пользователя. Такой торрент называют Secure Torrent.

Практически все современные частные трекеры сами принудительно вставляют private:1 во все торренты, выкладываемые на трекере, а также запрещают несколько устаревших версий клиентов, поддерживающих DHT или PEX, но ещё не знающих про private key. Считается, что пользователи трекера просто не могут на раздачах использовать DHT/PEX, и проблемы нет. На самом же деле для того, чтобы не учитывался рейтинг, достаточно заменить свой passkey на любой другой. И даже не надо его воровать. Достаточно зарегистрировать ещё одну учётную запись, чтобы взять из неё passkey.

DHT и статистика. Этот раздел касается только закрытых трекеров, на которых private key в торренты принудительно не вставляется, и на некоторых раздачах (в зависимости от того, вставил ли раздающий сам в торрент private key) можно использовать DHT и PEX.

Часто встречается мнение, что включённый в клиенте DHT влияет на учёт статистики клиента трекером, например «раздавал через DHT, значит статистика шла мимо трекера». Это неверно. Во-первых, DHT/PEX используется только для получения адресов пиров. Ни файлообмена, ни какого-либо учёта статистики по ним не ведётся. Клиент рапортует статистику скачанного и отданного только на трекер.

1.4 Основные тенденции эволюции наложенных сетей

Начало XXI века о характеризовано значительным подъёмом в области инфокоммуникаций. Данное явление может объясняться совокупностью причин, в числе которых либерализация соответствующего законодательства, приводящая к появлению рыночной конкуренции в мировом масштабе, рост производительности и одновременное удешевление повсеместно используемых микропроцессоров, а также технологические успехи, стимулирующие развитие систем передачи данных. Заметный рост инфраструктуры существующих сетей и связи и необходимость унификации услуг привели к необходимости создания универсальных концепций, позволяющих очертить русло, в котором будет происходить дальнейшее развитие.

На данный момент происходит очередная смена парадигм в вопросах построения сетей связи общего пользования (ССОП). Принято считать, что переход существующих ССОП к концепции сетей связи следующего поколения (Next Generation Networks, NGN) в настоящее время в значительной степени завершён. Основной отличительной чертой данной концепции является эволюция и конвергенция всех сетей, независимо от их назначения, приводящие их к единому знаменателю – принципу построения на базе коммутации пакетов. Действительно, как показывает практика, в подавляющем большинстве случаев современные сети строятся на пакетных технологиях, таких как Ethernet, MPLS, IP. Переход к концепции NGN

привел к формированию двух классов операторов: собственно операторов связи, предоставляющих возможность передачи данных, и поставщиков услуг, являющихся в свою очередь клиентами первых. Данный подход значительно отличается от принятого ранее, когда предоставление услуги (например, телефонии) и её доставка обеспечивались единой технологией. В то же время такое разделение ускорило конвергенцию в сетях связи, добиваясь, с одной стороны, доступности услуг любому пользователю, а с другой, приводя к созданию единой транспортной сети [13]. За полученным видом сетей закрепилось название мультисервисных, отражающее их способность с равным успехом передавать трафик различных типов: данные, мультимедиа, телефонию.

Дальнейшее развитие сетей связи приводит к необходимости следования новой универсальной концепции Интернета Вещей (Internet of Things, IoT), в рамках которой любой конечный пользователь – человек, устройство или даже приложение – рассматривается в качестве абстрактной «интернет-вещи». Особенностью предлагаемой концепции IoT является способность новой глобальной сети функционировать в условиях количества пользователей, значительно превышающего текущее. Согласно прогнозам международного исследовательского форума [14] количество вещей в глобальной сети достигнет 7 триллионов единиц к 2020 году, другие исследователи [15] дают оценку верхней границы насыщения IoT в 100 триллионов, причем до 2025-2030 годов рост сети будет близок к экспоненциальному. Другой отличительной особенностью можно назвать изменение подхода к построению сетей: новая глобальная сеть базируется на принципах самоорганизации [16]. В данном случае самоорганизация является необходимостью в условиях гетерогенной среды, динамично меняющей свое поведение. Скопления мобильных устройств, сенсоров, разнообразных датчиков генерируют плохо предсказуемый трафик, делая нецелесообразным, а зачастую и невозможным, планирование и централизованное управление такими сетями.

Развитие сетей связи в рамках обозначенных концепций неизбежно отражается на объёмах и структуре трафика. Согласно опубликованным результатам исследований [12] суммарный трафик глобальной сети показывает устойчивый экспоненциальный рост со второй половины 90-х годов XX века. В настоящее время эта тенденция сохраняется, что подтверждают прогнозы развития сетей на ближайшее время [17] (см. рис. 1.2).

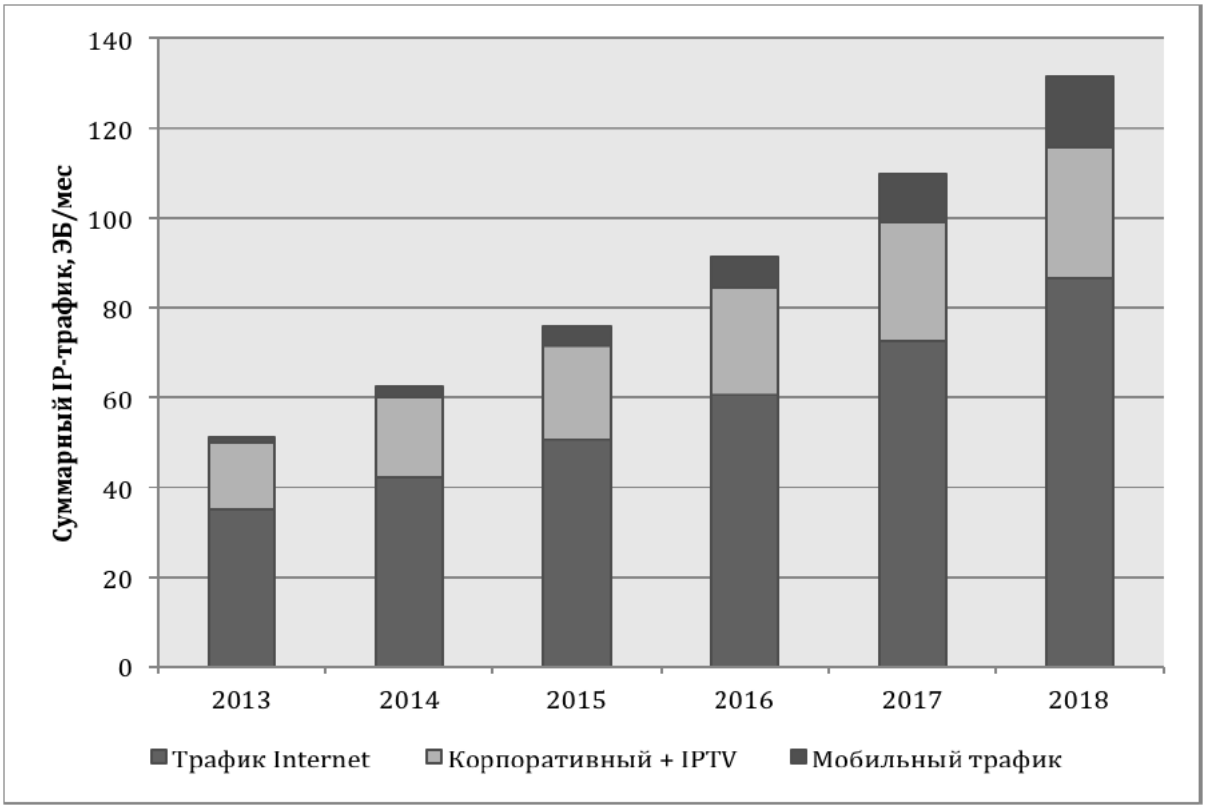


Рис. 1.2 – Прогноз интенсивности передаваемого IP-трафика

Структурный состав передаваемого трафика также будет претерпевать дальнейшие изменения (см. рис. 1.3). Если на начальных этапах перехода к концепции NGN доминировал трафик данных, то теперь наиболее значительную нагрузку создает видео-трафик, доля которого согласно прогнозам должна вырасти до 76% от общего количества передаваемого IP-трафика к 2018 году. Также отмечается тенденция роста доли интернет-трафика, доставляемого пользователям системами CDN (Content Delivery Networks). При этом интенсивность локального трафика, передаваемого в

рамках городских сетей (Metro-only) в два раза превышает таковую для магистрального трафика (Long-Haul), а в дальнейшем этот разрыв будет увеличиваться. Таким образом, можно дополнительно отметить тенденцию к локализации сетевого трафика.

Наряду с указанными тенденциями, все более значительной становится нестационарность передаваемой нагрузки. Наблюдается корреляция между временем суток, возрастом, интернет-грамотностью, кругом интересов пользователей с одной стороны и интенсивностью генерируемого ими трафика с другой [18].

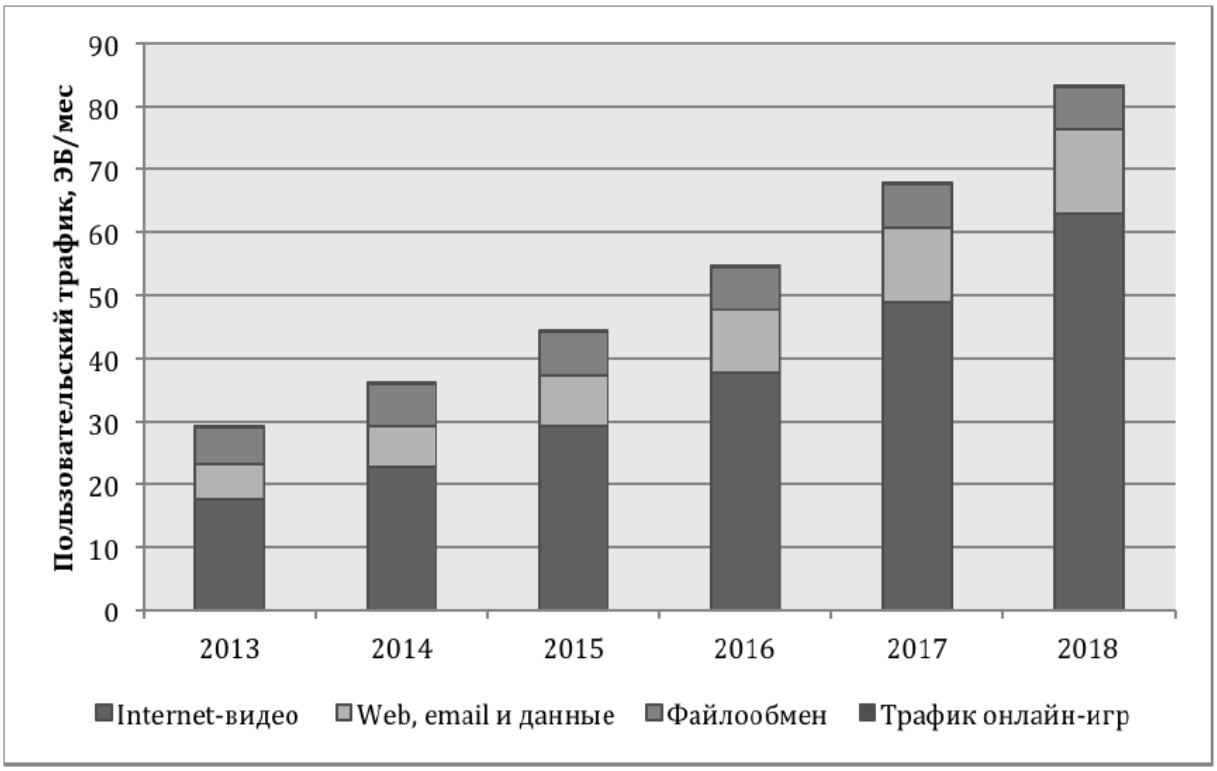


Рис. 1.3 – Прогноз структуры пользовательского трафика

Одним из примеров такой нестационарности может служить известный эффект flash-crowd, возникающий при вирусном распространении информации о некотором популярном ресурсе/контенте. Результатом этого эффекта является временный и практически непредсказуемый всплеск интенсивности передаваемого сетевого трафика. Схожие результаты дают запуск онлайн-трансляций, выход крупного обновления популярного программного продукта, широкое использование P2P-сервисов и многие

другие подобные примеры скоординированных действий большого количества участников сетевого обмена. Подобная координация вызывает резкий рост интенсивности передаваемого трафика и может быть как стихийной, например, в случае вирусного распространения информации в социальных сетях или перераспределения BGP-маршрутов, так и прогнозируемой, примерами которой могут служить просмотр онлайн-трансляций спортивных соревнований, массовое срабатывание множества узлов сенсорной сети при регистрации некоторого природного явления и т. п. На тенденцию увеличения неравномерности нагрузки также указывают прогнозы [19]: интенсивность трафика передаваемого в час наибольшей нагрузки (ЧНН) будет расти относительно средней интенсивности.

Отмеченные тенденции в изменении состава глобального трафика делают такие эффекты все более ощутимыми для транспортной инфраструктуры сети, что в совокупности с экспоненциальным ростом объемов передаваемого трафика приводит к необходимости переосмысления старых подходов к построению сетей. Как известно, традиционные протоколы маршрутизации выбирают путь прохождения данных по сети, оптимальный с точки зрения минимизации выбранной метрики. Такой подход позволяет передавать трафик наилучшим образом с точки зрения количества пройденных сетевых узлов, доступной полосы пропускания, задержек и т.п. Однако ему присущи определенные недостатки. Многие исследователи находят, что использование существующей сетевой инфраструктуры является крайне неоднородным. Так, проведенный в работе анализ интенсивности трафика относительно географического расположения показывает, что в глобальной сети трафик является сильно локализованным, а ранговое распределение подчиняется экспоненциально убывающему закону. На фоне постоянного экспоненциального роста объема передаваемого трафика [17] и вытекающей отсюда необходимости наращивать возможности оборудования такая ситуация выглядит как неэкономное и нерациональное использование существующей

инфраструктуры. Тогда как основная нагрузка сосредоточена на некоторых путях, остальная часть сети используется довольно слабо. Топология современной глобальной сети по результатам многочисленных исследований относится к классу small-world графов [19]. Особенностью таких графов является малая средняя длина пути в графе, а также степенное вероятностное распределение количества ребер случайной вершины. Например, для физической топологии Internet средняя длина пути составляет около 11 проходимых маршрутизаторов, а среднее количество ребер, инцидентных случайной вершине, k=2,66 . При этом некоторые исследователи отмечают тенденцию к уменьшению средней длины пути и общему повышению связности сети. Приведенные факты свидетельствуют, что в глобальной сети существует множество потенциальных маршрутов, позволяющих достигнуть пункта назначения, большинство из которых никогда не будут использованы из-за жестких условий, накладываемых маршрутизацией по кратчайшим путям. Более того, исследования показывают, что составные маршруты в Internet, получаемые на основе метрик нескольких различных протоколов, зачастую не оптимальны. Результаты работы [20] позволяют утверждать, что для 30-80% всех маршрутов, проходящих через глобальную сеть, могут быть найдены альтернативные пути, лучшие по показателям пропускной способности, задержек и потерь. Еще одной топологической особенностью современной глобальной сети является довольно высокий коэффициент кластеризации, показывающий вероятность того, что некоторый случайно выбранный узел окажется связанным с географически близким ему узлом.

Например, в исследовании [19] указан коэффициент кластеризации $c \in (0{,}2;0{,}3)$ (для случайных графов $c \approx 0{,}001$). Практически это означает, что наиболее плотно между собой связаны соседние узлы, что позволяет предполагать наличие множества путей альтернативных кратчайшему, особенно при маршрутизации в локальных сегментах. Другим важным вопросом является пропускная способность. Традиционно наименее производительным участком в сети считалась «последняя миля», однако с

увеличением возможностей сетей доступа все более актуальной становится проблема возникновения узких мест на других уровнях. В работе [21] отмечается, что 20-30% соединений, проходящих через глобальную сеть, постоянно маршрутизируются через перегруженные участки, при этом пределение конкретного канала связи, на котором происходит перегрузка, достаточно затруднительно. Также наблюдается явная корреляция перегрузки и текущего уровня использования канала, тогда как подобной зависимости в отношении пропускной способности соответствующего канала, а также использования ресурсов маршрутизатора не выявлено. Статистические исследования [22] показывают, что перегруженные каналы равномерно распределены по всей глобальной сети, при этом вероятности возникновения узкого места внутри сегмента провайдера, способного обеспечить инжиниринг трафика, и в каналах между сетями различных провайдеров, где применение таких методов практически исключено, приблизительно равны. Также отмечается, что доля каналов с недостаточной пропускной способностью зависит от положения сетевого сегмента в иерархии, увеличиваясь от 34% у провайдеров Tier-1 до 54% у провайдеров Tier-4.

На данный момент доминирующим является эмпирический подход, предполагающий экстенсивное наращивание пропускных способностей. Методики, используемые в настоящее время для расчета требуемой пропускной способности канала на уровне агрегации, основываются на статистических профилях трафика, причем для обеспечения должного качества обслуживания в условиях фрактальных эффектов пакетного трафика [23] вводится эмпирический понижающий коэффициент (≈0,3), предполагающий работу на недогруженных каналах [24]. Высоконагруженные и критичные участки сетей могут иметь избыточность, значительно превышающую указанную цифру. Так результаты исследования [25] позволяют утверждать, что при существующих методиках планирования сети, использование пропускной способности внутренних каналов

современного центра обработки данных при самом худшем сценарии не превысит 25%, тогда как загрузка каналов реальным трафиком в среднем не будет превышать 5%. Оценки создаваемых нагрузок с помощью традиционных методик характерны для расчета сетей, генерирующих предсказуемый агрегированный трафик. Такой трафик может успешно описываться с помощью статистических профилей (суточных, недельных), отклонения от которых незначительны. С учетом отмеченной растущей нестационарности пользовательского трафика подобный подход даёт неудовлетворительные результаты, заставляющие искать выход в области применения механизмов динамического управления сетями связи.

Выводы

Проведен анализ изменения объемов и структуры трафика глобальной сети, показывающий тенденции экспоненциального роста, нестационарности и стихийный характер возникновения нагрузок.

Проведен анализ механизмов балансировки сетевого трафика. Показано, что применяемые решения являются недостаточными для обеспечения эффективного использования существующей сетевой инфраструктуры в указанных условиях.

Показано, что одной из основных проблем сетей связи является непредсказуемость возникающих нагрузок, приводящая к потерям трафика. Предложено применить децентрализованные самоорганизующиеся наложенные сети балансировки трафика, способные реагировать на изменения сетевых нагрузок в режиме, близком к реальному времени.

2. СИНТЕЗ НАЛОЖЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

С учетом мировых и отечественных тенденций развития телекоммуникационных систем, одной из наиболее актуальной проблем отрасли связи Узбекистана является создание мультисервисной сети связи, которая удовлетворяла бы возрастающему передаваемому трафику и увеличивающемуся перечню телекоммуникационных услуг. Важной задачей при развертывании данных сетей является задача параметрического синтеза, которая заключается в определении параметров структурных элементов. Для решения данной задачи необходимо знать параметры потоков и характеристики процессов, протекающих в различных частях телекоммуникационной сети, а также уметь рассчитывать и оценивать характеристики потоков образуемых при агрегировании их при передаче и обработке и узлах сети. Данная задача дополнительно осложняется в условиях современных мультисервисных сетей, для которых характерен наложенный принцип построения и наличие мультисервисных потоков.

Необходимость учета наложенного принципа современных телекоммуникационных сетей продиктовано зависимостью процессов протекающих на различных его уровнях и их сильным влиянием их друг на друга. Это можно учесть за счет разделения системы на логическую и физическую сеть [26], где каждая связь в логической сети представляется потоком протекающей по физической сети. Использование данного подхода ограничивалась обычно двумя уровнями.

Дальнейшим развитием идеи разделения структуры наложенных сетей на логическую и физическую является модель многослойной сети, где каждая наложенной сеть называется слоем. Каждый слой описывается графом, при этом множество вершин графа верхнего слоя является подмножеством вершин нижнего слоя с дополнительным ограничением, что

каждый канал верхнего слоя соответствует одному или нескольким путям в нижнем слое.

Наличие строгого соответствия вершин разных слоев не позволяет применять эту модель при проектировании сетей, когда местоположение узлов наложенной сети не определено и определяется только на стадии синтеза сети.

С этой целью, в этом выпускном квалификационном работе предложена модель в виде многослойного графа, отличительной особенностью которой является наличие множества ребер между вершинами разных слоев. Это позволяет более полно описать структуру будущей телекоммуникационной системы структуру будущей телекоммуникационной системы и процессы, протекающие в ней в особенности, когда ее структуру еще не полностью определена.

Следует отметить, что согласно современным исследованиям трафика передаваемого в телекоммуникационных системах выявлено, что его статистические характеристики отличаются от тех, которые приняты в классической теории телетрафика. Использование традиционных методов расчета параметров сетей и их вероятностно-временных характеристик, согласно классической теории телетрафика, приводит к неоправданно оптимистическим результатам и недооценке нагрузки.

Работа [27] посвящена разработке методов параметрического синтеза мультисервисных телекоммуникационных сетей при известных параметрах самоподобных потоков в каналах связи, которые применимы для однослойных сетей. Однако, в этой работе не учитывают наложенную структуру современных сетей, изменение типа протокольного блока при передаче, а также не учитывают процессы параллельно происходящие на других уровнях (слоях) мультисервисной сети, такие как установка соединения, оказание информационной услуги сервером и другие.

Другим аспектом, на который следует обратить внимание, является то, что при постановке задач параметрического синтеза, для описание

информационных потоков, поступающих в сеть, обычно используется матрица требований передачи информации между конечными узлами сети. Однако при реализации инфокоммуникационной услуги абонент сети взаимодействует с некоторым множество узлов управления услугой в пределах множества наложенных сетей, что необходимо учитывать при синтезе мультисервисных наложенных сетей и которые не учитываются данным способом описания трафика в сети.

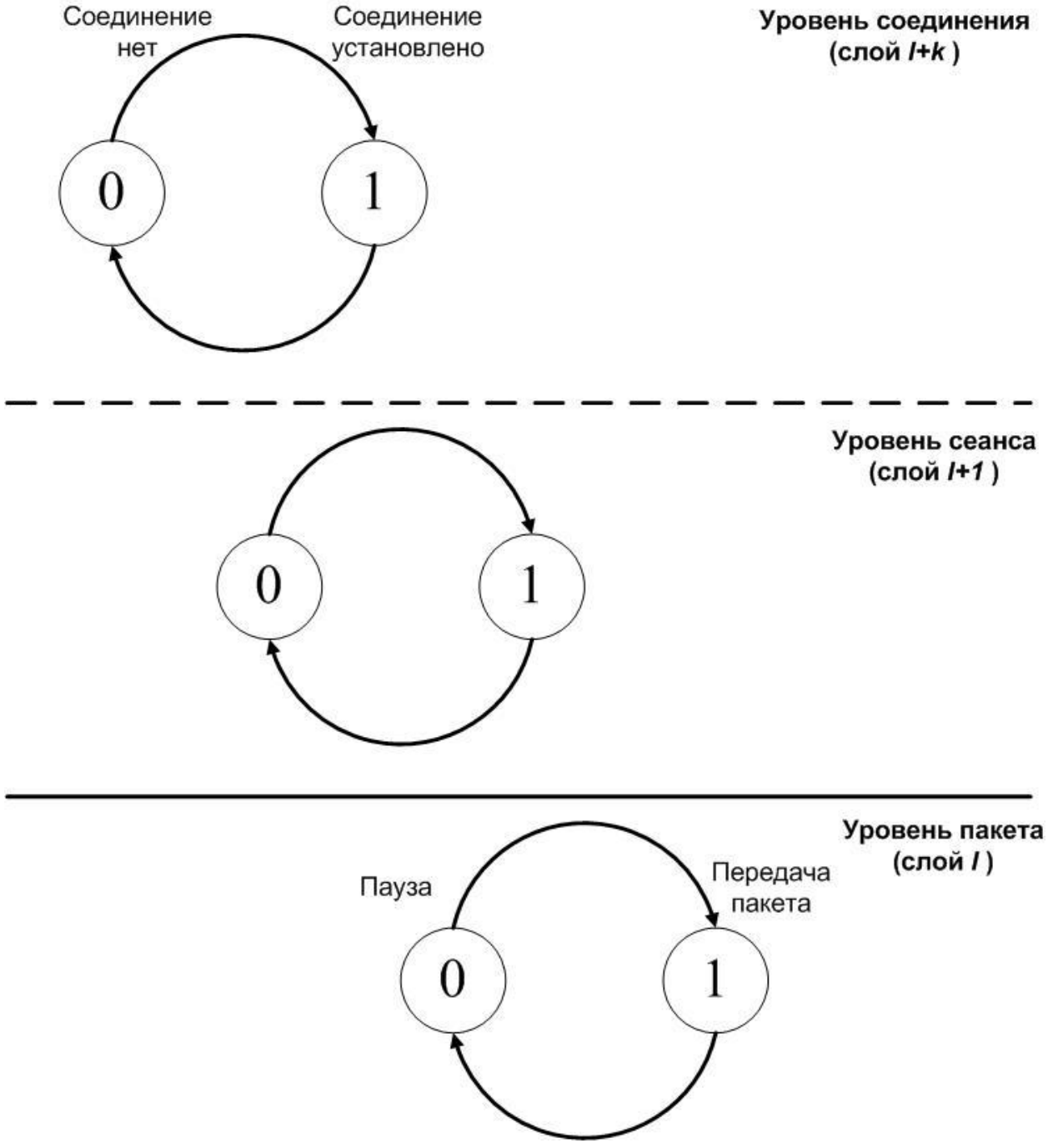


Рис. 2.1 Модель многоуровневого источника потока

Для устранения данного несоответствия, базируясь на модели, приведенной в работе [28], предлагается использовать при моделировании источников трафика в мультисервисных наложенных телекоммуникационных системах, следующую модель (рис.2.1). Модель, предлагаемая для моделирования источника трафика в мультисервисных наложенных сетях, представляет собой многоуровневый On/Off - источник.

В этом случае параметры потока в состоянии активности для наложенной сети на уровне 1 могут быть рекуррентно определены:

$$\boldsymbol{\lambda_1 = P^1_{Off}\lambda_{min} + P^1_{Off}\lambda_{I-1}} \quad \textbf{(2.1)}$$

$$\boldsymbol{\sigma^2_1 = P^1_{Off}(\lambda_{min})^2 + P^1_{On}(\lambda_{I-1})^2 - (\lambda_I)} \quad \textbf{(2.2)}$$

где (λ_I) и (λ_{I-1}) - интенсивности потока на уровне I и I-1 соответственно;

P^1_{Off} , P^1_{On} - вероятности нахождения источника в активном и пассивном состоянии соответственно;

σ^2_1 - дисперсия потока на уровне I.

Таким образом, применение предложенной выше модели многослойного источника позволяет производить оценку параметров потока от индивидуальных источников на разных уровнях наложенной сети(пакетная сеть, транспортная сеть, уровень предоставления услуг).

При параметрическом синтезе наложенных телекоммуникационных сетей необходимо определять параметры ее элементов. Для решения данной задачи рекомендуется использовать следующую методику:

1. Синтезируемая мультисервисная наложенная сеть описивается многослойным графом согласно методику [29].

2. Используя данные об абонентах, подключаемых к сети и перечне потребляемых ими телекоммуникационных услуг, производиться определение параметров потоков, создаваемых ими на каждом из уровней наложенной сети. Для решения данной задачи применяется многоуровневая

модель On/Off - источника, используемого для описания телекоммуникационной услуги, потребляемой абонентов, зависят от ее вида и ее характеристик на соответствующей уровне наложенной сети.

3. Потоки, поступающие от индивидуальных источников, агрегируются и определяются параметры группового трафика с использованием методики приведенной в работе[30].

4. Для полученной структуры сети решается задачи распределения потоков с использованием потоковой модели для многослойного графа [31]. При применении потоковой модели следует использовать ее свойство сохранения потоков [31] для значений интенсивностей потоков λ, описываемых моделями самоподобного трафика. В результате выполнения данного шага мы получим выражения для суммируемых потоков в ребрах многослойного графа.

5. С использованием расчетных выражений для параметров агрегированного самоподобного потока [30] и значений параметров, поученных на щаге 4, определяются параметры агрегированных потоков, образуемых при объединении потока протекающих по ребрам многослойного графа.

6. Найденные на предыдущем шаге выражения используется в расчетных выражениях для параметров качества обслуживания для соответствующих ребер многослойного графа.

7. Полученные в результате выполнения описанных выше шагов выражения используется при математической постановке оптимизационной задачи, решение которой позволяет определить параметры, приписанные ребрам многослойного графа и как результат - значения параметров структурных элементов мультисервисной наложенной телекоммуникационной сети.

Эффективность метода базирующего на многослойном источнике зависит от эффективности методов выбора оптимальных значений параметров элементов и адекватности методики определения характеристик потока в каналах сети. Первая составляющая при заданных характеристиках потоков хорошо себя зарекомендовала и достаточно подробно исследована в [8]. В рамках данной дипломной работе мы остановимся на исследовании

второй составляющей метода: определении параметров потоков. Эксперимент проведем с использованием средств имитационного моделирования. Для этого была разработано модель узлов, которые устанавливали между собой соединения на разных уровнях. При проведении эксперимента анализировались характеристики потоков на нижнем уровне, которые сопоставлялись с результатами расчета с использованием приведенной в этом главе. Эксперимент повторялся для разных вариантов конфигураций источников, результаты которого предоставлено в табл.2.1

Таблица 2.1

Результаты анализа параметров объединенного потока сообщений

№ эксперимента	Имитационная модель			Расчетные данные		
	λ	σ	H	λ		H
1	1057	1493	0,70	1062	1399	0,71
2	601	754	0,76	599	732	0,75
3	830	1021	0,72	832	1106	0,74
4	748	906	0,73	765	1013	0,74

Из анализа результатов, приведенных в табл. 1 видно, что экспериментальные данные сходятся с результатами расчета предложенным методам, что свидетельствует об адекватности математической модели и метода расчета. Небольшие отклонения результатов эксперимента от расчетных данных несут статистический характер связанный с ограниченным объемом выборки. Также причиной расхождения результатов могут быть переходные процессы в имитационной модели в начале и в конце эксперимента.

2.1 Механизм наложенной сети

В данной главе предлагается механизм наложенной балансировочной сети (Load Balancing Overlay, LBO) – самоорганизующейся сетевой структуры, выравнивающей нагрузку между транзитными узлами-участниками, а также позволяющей смягчить негативное влияние критичных участков (bottlenecks) сетевой топологии, имеющих пропускную способность недостаточную для передачи агрегированных потоков трафика, за счет повышения использования существующей сетевой инфраструктуры (рис. 2.2).

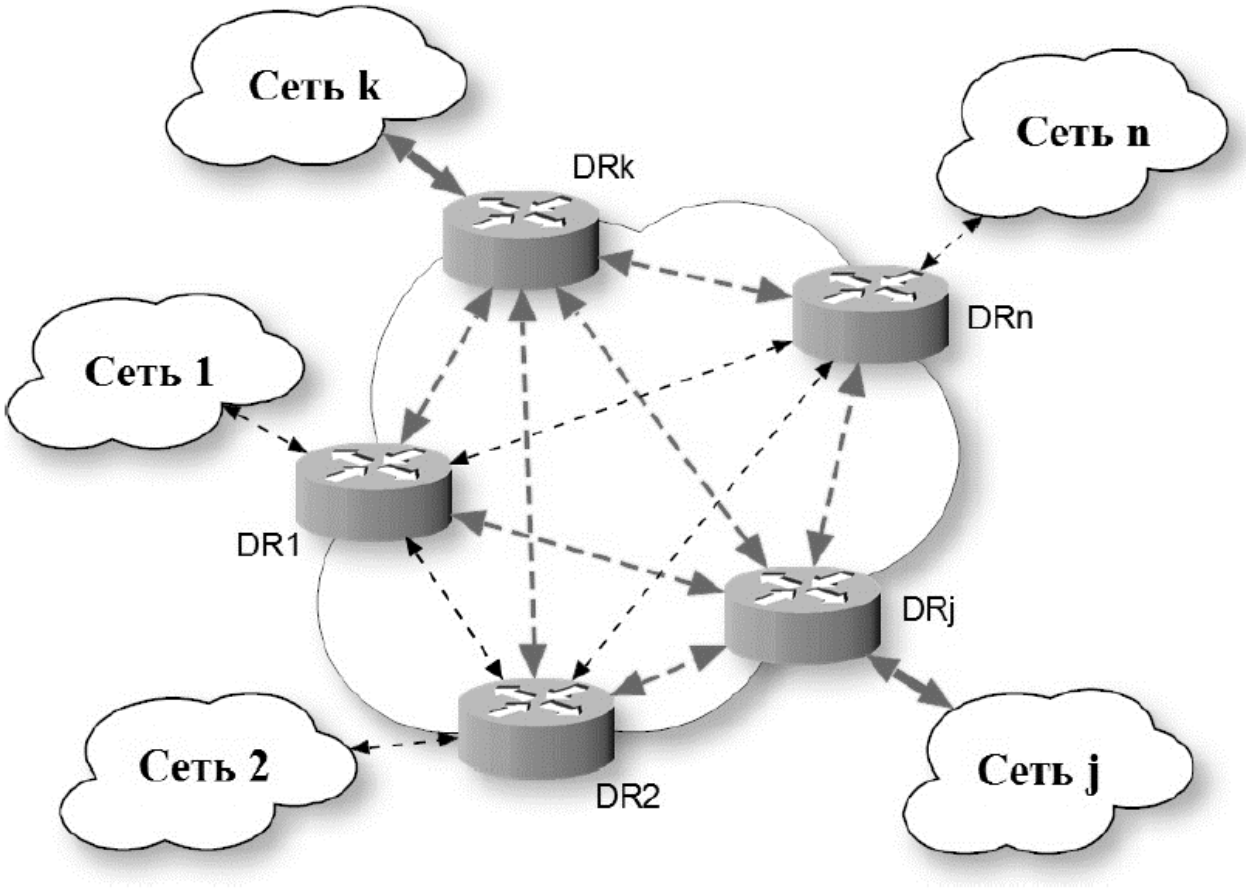


Рис. 2.2 – Модель наложенной балансировочной сети

Базовой идеей, лежащей в основе предлагаемой балансировочной сети, является возможность выбора определенных субоптимальных путей для передачи трафика, некритичного к такому показателю QoS, как сетевая задержка. К данному типу можно отнести как передачу данных (включая Web/HTTP и стремительно набирающие популярность облачные сервисы),

так и потоковый трафик (онлайн-видео, IPTV и т.п.). Перечисленные типы нагрузки являются доминирующими в общей структуре трафика глобальной сети [32]. Низкая чувствительность такого трафика к времени задержки прохождения по сети позволяет распределить нагрузку по большему количеству доступных путей, чем это возможно в рамках традиционной маршрутизации (рис. 2.3).

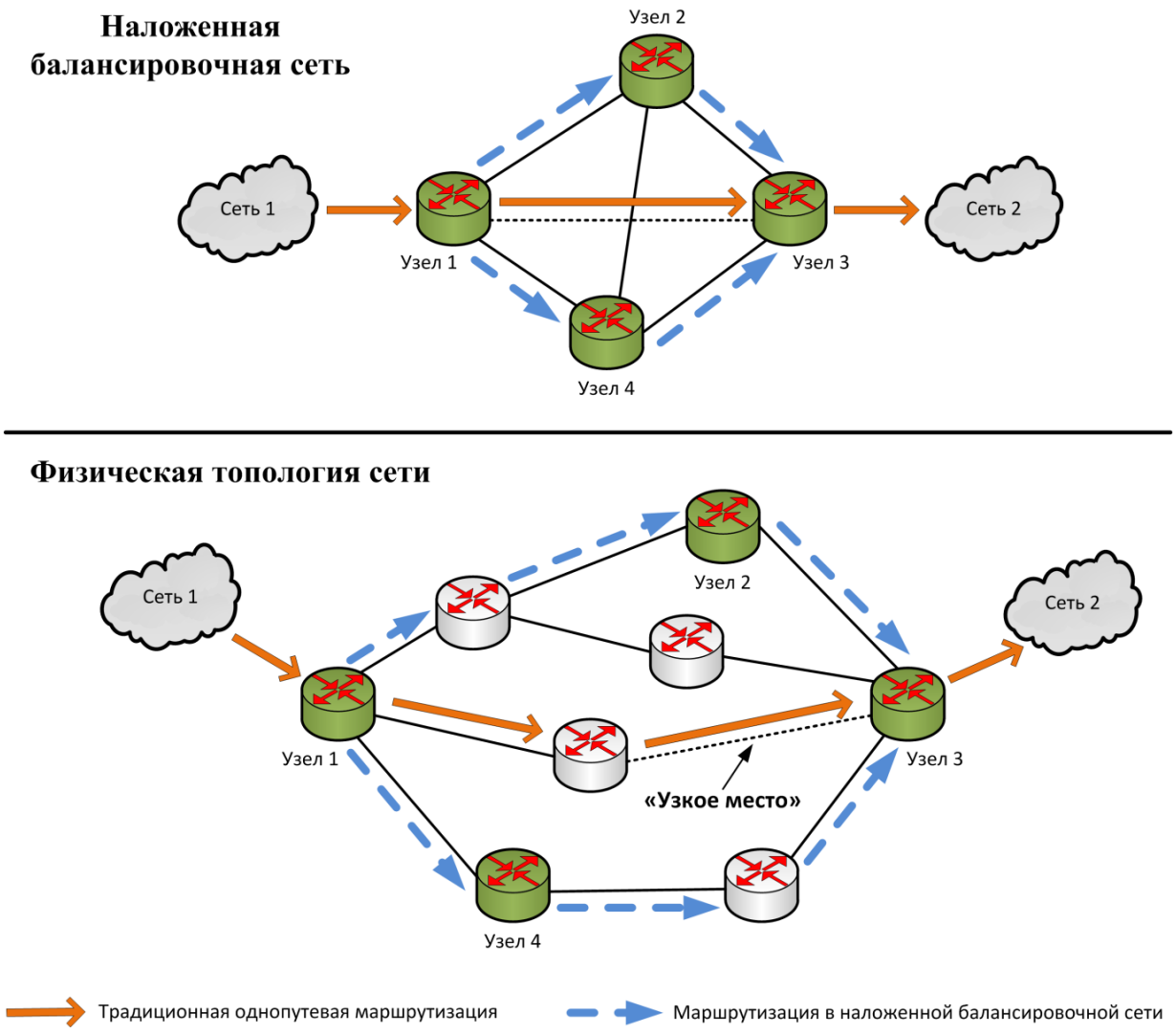


Рис. 2.3 – Распределение нагрузки наложенной балансировочной сетью в случае недостаточной пропускной способности оптимального пути.

При этом предложенный распределенный механизм способен отслеживать текущее состояние сети и реагировать на происходящие

изменения в режиме, близком к реальному времени. Условимся далее называть кратчайшие оптимальные пути между двумя узлами прямыми, а субоптимальные – обходными. Исходя из того, что наложенная сеть является виртуальной сетевой структурой, её топология предполагается полносвязной. Увеличение количества дополнительных переходов ведет к ощутимому росту, как сетевых задержек, так и вычислительной сложности задачи. В этих условиях представляется разумным ограничить множество возможных обходных путей маршрутами, проходящими через один дополнительный маршрутизатор – узел наложенной балансировочной сети. Тогда прямой путь через систему балансировки будет включать в себя два узла-маршрутизатора, а все обходные пути – три узла. Фактически предлагаемая система балансировки работает локально, внося коррективы в работу протоколов маршрутизации исключительно на участке между двумя маршрутизаторами
агрегации, входящими в наложенную сеть и оставаясь прозрачной для всех остальных участников сетевого обмена.

Всё множество узлов, участвующих в работе балансировочной сети, предлагается разбивать на группы. Балансировка потоков трафика будет осуществляться между маршрутизаторами, принадлежащими к одной группе. Узлы, состоящие в одной группе, организуются в наложенную сеть, задачей которой является координация действий по распределению транзитного трафика. Такая наложенная сеть является полностью децентрализованной самоорганизующейся одноранговой P2P-структурой, позволяющей динамически управлять группой входящих в нее узлов, а также осуществлять их подключение/отключение. Функции управления трафиком распределяются между всеми узлами-участниками наложенной сети. Основные задачи, выполняемые узлами наложенной сети, можно классифицировать следующим образом:

- Процедуры управления наложенной сетью:
  - подключение к существующей наложенной сети;

- обмен узлов сети служебной информацией;
- отключение активного узла от сети;
- обнаружение аварий узлов/каналов.

– Контроль состояния наложенной сети:
  - определение характеристик сети;
  - мониторинг текущей загрузки каналов;
  - оценка текущего количества входящих потоков.

– Управление транзитным трафиком:
  - прогнозирование входящей нагрузки;
  - контроль интенсивности входящей нагрузки;
  - расчёт распределения транзитной нагрузки/потоков;
  - перенос потоков в соответствии с рассчитанным планом.

2.2 Построение и управление наложенной сети

Наложенная балансировочная сеть представляет собой самоорганизующуюся
сетевую структуру, следовательно, первичной задачей входящих в неё узлов является организация и поддержание работоспособности такой сети. С этой точки зрения LBO построена на принципе одноранговой децентрализованной P2P-сети с равноправными узлами-участниками, не имеющей единой точки отказа.

Подключение нового узла к существующей наложенной сети. Первичная задача, возникающая перед узлом, желающим принять участие в работе наложенной балансировочной сети, является поиск таких сетей и адресов конкретных узлов, входящих в них. Как уже упоминалось в п. 2.1.2, в глобальной сети может существовать множество балансировочных оверлеев (наложенных сетевых структур), работающих автономно и независимо друг от друга. Каждому экземпляру наложенной балансировочной сети

присваивается уникальный идентификатор, единый для данной группы узлов. Элементами частичной централизации в данном случае могут служить вспомогательные дублирующие bootstrap-серверы, расположенные по общеизвестным адресам и хранящие различную информацию о существующих активных балансировочных оверлеях, включая идентификаторы сетей, адреса узлов, непосредственно входящих в них, и др. Узел, желающий подключиться к одному из оверлеев, запрашивает с помощью сообщения WHO любой известный ему bootstrap-сервер и получает информацию о существующих активных оверлеях в ответном сообщении LIST. Выбор конкретного оверлея может производиться на основании различных критериев:

- средние доступные пропускные способности каналов между узлами,
- текущее количество узлов в оверлее,
- маршрутная целесообразность (например, большое количество групп адресов назначения располагаются в тех же автономных системах, что и соответствующие узлы наложенной балансировочной сети),
- географическая/топологическая локальность узлов и т. п.

Выбор определяющих критериев в значительной степени зависит от сценария применения наложенной балансировочной сети. Возможен также вариант ручного выбора требуемого оверлея администратором на основании имеющихся у него сведений об общей сетевой топологии. Отметим, что данный вопрос требует проведения дополнительных исследований.

После того, как необходимый балансировочный оверлей выбран, и получена вся необходимая информация, узел начинает процедуру подключения. Для этого всем активным узлам, входящим в выбранный оверлей, по очереди с небольшим интервалом рассылаются уведомительное сообщение INIT, а также INFO, содержащее список диапазонов сетевых адресов, транзитный трафик к которым этот узел планирует обрабатывать и пропускать через балансировочную сеть. Здесь необходимо заметить, что не весь трафик, проходящий через узел наложенной балансировочной сети,

будет подвергаться балансировке. Пакеты, сетевые адреса которых не совпадают с указанными диапазонами, будут обрабатываться на основании обычной таблицы маршрутизации. Узел, получивший сообщение INIT, запускает кратковременную процедуру определения доступной пропускной способности каналов, между ним и узлом-инициатором, отсылает последнему сообщение INFO, после чего перестраивает собственные таблицы и уведомляет инициатора о готовности к работе сообщением READY. В данном случае временной интервал необходим для исключения возможности наложения нескольких проверочных процедур и, как следствие, искажения полученных результатов. Сообщение READY также содержит информацию о текущем времени в сети и интервале обмена сообщениями, необходимую для координации работы наложенной балансировочной сети.

После того, как все участники оверлея опрошены, узел- инициатор рассылает всем сообщение START, означающее, что с начала следующего UPDATE-периода (см. ниже) новый узел участвует в работе сети.

Помимо подключения к существующей сети узел может инициировать создание нового балансировочного оверлея, отправив bootstrap-серверу сообщение NEW с указанием необходимой информации. Сервер записывает полученные данные и возвращает идентификатор, рассчитываемый с помощью хеширования сетевого адреса узла-инициатора, что позволяет исключить появление оверлеев с одинаковыми идентификаторами. После этого начинается ожидание подключения новых участников, во время которого узел продолжает работать в режиме обычного маршрутизатора, использующего традиционные протоколы.

Обмен узлов сети служебной информацией. В процессе работы узлы, входящие в некоторую наложенную балансировочную сеть, должны обмениваться информацией о текущем состоянии сети, а точнее – остаточных канальных ресурсах, доступных для перевода на них избыточного трафика. Такая информация распространяется в сообщениях UPDATE, периодически рассылаемых между всеми узлами-участниками.

При размере сети в n активных узлов, каждые t_{UPDATE} секунд сетью будет генерироваться служебный трафик из n^2 сообщений, где t_{UPDATE} *UPDATE* – период рассылки сообщений UPDATE или UPDATE- период. Помимо обновления информации о канальных ресурсах, сообщение UPDATE также свидетельствует об активности узла-отправителя и отсутствии потери связности наложенной сети. Дополнительно в каждом сообщении UPDATE содержится вектор активности каналов между текущим узлом и остальными участниками оверлея, показывающий какие узлы доступны отправителю напрямую (в топологии наложенной сети).

Периодически один из узлов каждого балансировочного оверлея, выбираемый случайным образом, отсылает текущую информацию о своей сети и её активных участниках выбранному bootstrap-серверу, поддерживая актуальность хранящихся данных.

Отключение активного узла от сети. При плановом отключении активного узла наложенной балансировочной сети узлы-участники данного оверлея должны быть заранее проинформированы об этом событии. Узел, планирующий отключиться или перейти в неактивное состояние, рассылает сообщение SHUTDOWN всем соседям, входящим в его балансировочный оверлей, после чего в течение еще двух целых UPDATE-периодов обязан функционировать в нормальном режиме. Такая процедура дает возможность без потерь перенести все потоки, идущие по обходным путям через отключаемый узел, на новые обходные маршруты.

Обнаружение аварий узлов/каналов. В процессе работы наложенной балансировочной сети возможны ситуации потери связности между узлами, а также отказа узлов-участников. Для успешной работы балансировочной сети необходимо различать данные ситуации. Активность узлов определяется с помощью периодически рассылаемых сообщений UPDATE. В том случае, если сообщение UPDATE от некоторого узла *j* не поступает данному узлу *i* в течение более чем t_{UPDATE} секунд, узел *i* считает, что произошла авария на канале *i-j* и выставляет нулевое значение пропускной способности в

собственной таблице топологии сети (см. п. 2.3.2) и активности соответствующего канала. Если при этом в сообщениях UPDATE, получаемых от других узлов, каналы, ведущие к узлу *j*, активны – считается, что произошла потеря связности и весь трафик аварийного направления переводится на обходные маршруты. В противном случае предполагается, что произошла авария на узле с полной потерей связности, и узел j считается неактивным с последующим исключением из балансировочного оверлея.

2.3 Контроль состояния наложенной сети

Данный пункт содержит описание набора процедур, обеспечивающих получение узлами балансировочного оверлея актуальной информации о текущем состоянии сети.

Определение характеристик сети. Данная процедура запускается при подключении нового узла к существующему оверлею и служит для определения пропускных способностей виртуальных каналов, соединяющих узлы наложенной балансировочной сети. В процессе проведения процедуры оценивается время передачи некоторого тестового объема информации, на основании чего определяется пропускная способность между данной парой узлов.

Мониторинг текущей загрузки каналов. Для оценки текущей загруженности каналов наложенной балансировочной сети, каждый узел периодически рассылает тестовые запросы всем остальным участникам оверлея. По времени прохождения запроса (RTT) рассчитывается доступная пропускная способность данного виртуального канала. За интервал времени t_{UPDATE} выполняется probe k измерений, после чего результаты этих измерений усредняются, и полученное значение попадает в таблицу узла.

Оценка текущего количества входящих потоков. Для снижения сложности задачи учета и балансировки, в качестве идентификатора атомарного потока трафика принимается уникальная пара сетевых адресов:

отправителя и получателя. Согласно результатам исследований трафика крупных агрегирующих узлов, большинство потоков транспортного уровня очень незначительны, как по интенсивности, так и по времени существования. Так в исследовании [25], посвященном изучению трафика крупных центров обработки данных, указывается, что большая часть потоков транспортного уровня имеет интенсивность меньше 10 Кбит/с, а многие из этих потоков также являются короткоживущими, со временем существования порядка нескольких сотен микросекунд. Рассмотрение агрегированного потока между парой адресов сетевого уровня в качестве атомарного позволяет избежать значительной и бесполезной нагрузки на сетевое оборудование.

Балансировка транзитного трафика. Следующая базовая группа процедур, выполняемых узлами наложенной балансировочной сети, относится к вопросам управления транзитным трафиком. Как уже отмечалось ранее, данным процедурам подвергается только тот трафик, который классифицируется для дальнейшей передачи в балансировочном оверлее**.**

Прогнозирование входящей нагрузки. Каждый узел наложенной балансировочной сети в процессе работы рассчитывает возможности передачи транзитного трафика, что предполагает обладание полной информацией о текущей ситуации во всей сети. Дискретность и децентрализованность управления приводят к тому, что узлы не могут реагировать мгновенно на происходящие изменения в структуре входящего трафика, фактически влияющие на работу всей сети. Выходом из этой ситуации является применение прогнозирования поведения входящей нагрузки всеми участниками балансировочного оверлея. Каждый узел анализирует данные о загрузках каналов к соседним узлам за предыдущие периоды времени, на основании чего строится краткосрочный прогноз доступных канальных ресурсов на ближайший интервал, равный t_{UPDATE} секунд. После этого все узлы, входящие в один балансировочный оверлей, обмениваются полученными прогнозами в сообщениях UPDATE, что

позволяет каждому участнику иметь полную своевременную картину происходящего во всей сети. Вопрос выбора соответствующих методов прогнозирования подробно рассматривается в главе 3.

Контроль и ограничение интенсивности входящей нагрузки. Появление перегрузок в каналах между узлами наложенной сети крайне нежелательно, ввиду того, что неограниченный рост интенсивности входящего трафика со стороны одного из узлов в условиях применяемого подхода может привести к полной блокировке каналов между узлами наложенной сети. Во избежание этого, каждый узел рассчитывает максимально допустимую интенсивность входящего трафика на текущий период времени. При превышении данного порогового значения пакеты некоторых случайно выбранных входящих потоков будут отбрасываться узлом.

В процессе работы каждый узел наложенной балансировочной сети оценивает текущую входящую нагрузку на основании собираемой статистики об объеме переданных данных. Особенностью данной процедуры в LBO является раздельный учет интенсивности для каждого направления (т.е. нагрузки, которая должна направляться другим узлам балансировочного оверлея). Раздельная статистика обеспечивается с помощью процедуры классификации входящего трафика. Процедура классификация применяется ко всему входящему трафику и позволяет на основании адресов назначения отделить нагрузку, распределяемую в LBO, от нагрузки, обрабатываемой с помощью традиционных протоколов маршрутизации. Дополнительно процедура классификации трафика позволяет разделять приоритетный и неприоритетный типы нагрузки. После прохождения процедуры классификации каждый пакет отправляется на дальнейшую обработку требуемым процессом.

Процедура контроля входящей нагрузки может быть реализована с помощью различных алгоритмов управления очередями. При этом процессы LBO соответствующим образом заменяют традиционные AQM-алгоритмы,

прежде всего позволяя отдельно контролировать очереди входящего трафика, различающиеся сегментами назначения. В качестве эффективного механизма управления очередями можно предложить модификацию, основанную на семействе алгоритмов RED, например, вариацию FRED (Flow Random Early Drop) [91] , в которой вместо транспортных потоков будут рассматриваться потоки сетевого уровня.

Расчет распределения транзитной нагрузки/потоков. В базовом варианте концепции наложенной балансировочной сети определены два класса трафика: приоритетный и неприоритетный. Приоритетный трафик предполагается чувствительным к задержкам и их вариации, а, следовательно, не допускает передачи по обходным маршрутам. Также, при контроле интенсивности входящего трафика, безусловное предпочтение отдается потокам приоритетного трафика, пороговая интенсивность передачи которых ограничивается только пропускной способностью соответствующих каналов. Все потоки трафика в сети однозначно идентифицируются по паре значений сетевых адресов отправителя и получателя, проходя процедуру классификации.

Процедура расчета плана распределения нагрузки в наложенной балансировочной сети состоит из нескольких этапов:

- *Оценка текущих нагрузок*. Каждый узел наложенной сети определяет текущее усредненное значение интенсивности входящего трафика.
- *Определение максимально допустимой интенсивности входящего трафика.* На основании данных о предыдущих значениях усредненной интенсивности входящих потоков приоритетного трафика каждый узел строит прогноз на текущий период и рассчитывает допустимую интенсивность входящего неприоритетного трафика.
- Планирование распределения нагрузки на текущий период. Потоки трафика, попадающие в балансировочную сеть, должны быть распределены по прямым и обходным маршрутам, для чего

рассчитываются планируемые нагрузки в каждом канале пропорционально соответствующим доступным канальным ресурсам.

- Первичная оценка плана распределения потоков на текущий период. После того, как для каждого маршрута рассчитана интенсивность трафика, необходимо определить, какое количество реальных потоков будет передаваться по нему. Первичная оценка распределяет потоки пропорционально соответствующим значениям интенсивности.
- *Уточнение распределения потоков*. С целью уменьшения вероятности появления осцилляций маршрутов, применяется механизм, ограничивающий перераспределение потоков при малых изменениях. Для учета влияния механизма сглаживания осцилляций на окончательное распределение потоков по маршрутам применяется уточняющая процедура.

Перенос потоков в соответствии с рассчитанным планом. Как уже было сказано выше, процедуре переноса целесообразно подвергать только потоки неприоритетного трафика. После проведения окончательного уточнения плана распределения потоков, каждый узел приводит текущее распределение в соответствие с рассчитанным. При этом задача различения того, на какой маршрут должен быть переведен конкретный поток, опирается на процедуру классификации входящего трафика. Для переноса потока трафика на выбранные субоптимальные пути в зависимости от сценария использования наложенной балансировочной сети могут применяться различные техники:

- промежуточная инкапсуляция;
- использование свободных TE-туннелей в MPLS с указанием адреса промежуточного узла [34];
- установление постоянных VPN-туннелей между всеми узлами наложенной балансировочной сети;
- использование опции LSRR (Loose Source and Record Route) , позволяющей частично задать путь прохождения IP-пакета.

Отдельные потоки, которые будут подвергаться переносу, выбираются из общего количества неприоритетных случайным образом, причем вероятность выбора потока определяется разницей в текущем и расчётном планах распределения.

Обобщая вышеизложенные процедуры, можно представить процесс управления наложенной балансировочной сетью с точки зрения некоторого узла в виде следующей временной диаграммы (рис. 2.4).

Каждый узел с периодом t_{UPDATE} секунд рассылает всем своим соседям прогнозы остаточной пропускной способности каналов на следующий период времени. Для этого в реальной сети несколько раз за период осуществляются измерения загруженности каналов, связывающих данный узел с соседними, результаты замеров за период усредняются, и на основании истории предыдущих значений строится прогноз. Так как система децентрализована, и работа узлов не синхронизирована, узлы вынуждены обрабатывать приходящие сообщения UPDATE по мере их поступления. В течение периода времени между собственными рассылками узел принимает сообщения UPDATE от соседних узлов. Далее, на основании полученных сведений, узел рассчитывает допустимую интенсивность входящего трафика на следующий период и распределение потоков трафика. При этом, если информация от некоторого узла не была получена за данный период, используются значения предыдущего периода.

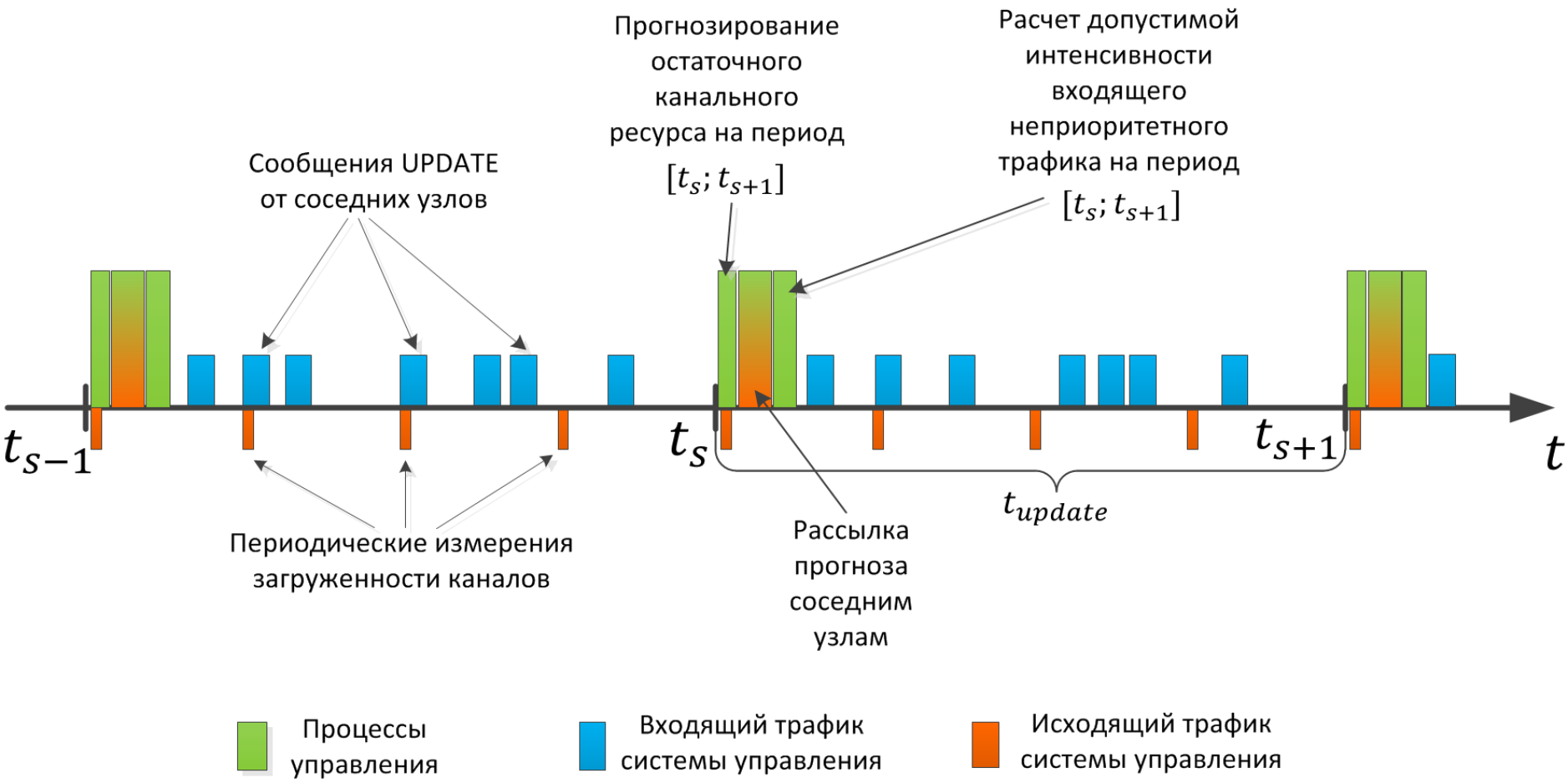


Рис. 2.4 – Временная диаграмма работы узла наложенной балансировочной сети

Отказоустойчивость наложенной балансировочной сети. Концепция наложенной балансировочной сети помимо решения задачи распределения избыточного трафика позволяет дополнительно повысить отказоустойчивость сети. Данный эффект проявляется в случае возникновения аварии на пути между некоторой парой узлов наложенной сети, отслеживаемой с помощью механизма обмена сообщениями UPDATE, и устраняется перераспределением потоков по доступным маршрутам. При этом вероятность потери соединения с некоторым активным узлом экспоненциально падает при увеличении количества узлов, входящих в оверлей.

Однако вопрос отказоустойчивости остается открытым с точки зрения передачи приоритетного трафика, т.к. наложенная балансировочная сеть в штатном режиме работы не осуществляет переноса потоков приоритетной нагрузки. Возможным решением является временное распределение потоков приоритетного трафика заблокированного направления по всем обходным путям, аналогично процедуре, проводимой над потоками неприоритетной нагрузки. При этом обнаружение аварии на канале между парой узлов дополнительно вызывает процедуру распределения приоритетной нагрузки аварийного направления, а затем снова пересчитывается доступный канальный ресурс, данные рассылаются в сообщениях UPDATE, и производится расчет величины допустимой входящей неприоритетной нагрузки и её распределение по обходным путям. Приоритетный трафик аварийного направления остается распределенным по обходным путям до тех пор, пока не будет устранена авария на прямом пути или протоколы маршрутизации физической сети не рассчитают новый маршрут. Особо стоит выделить проблему обнаружения аварии на маршруте. Известно, что наибольшую часть времени восстановления традиционных протоколов маршрутизации занимает именно обнаружение потери связности, детектируемое при срабатывании соответствующих таймеров протоколов. Для протоколов IGP-маршрутизации, таких как RIP, OSPF, IS-IS, это время

колеблется в диапазоне 30-120 секунд. Протокол BGP, де-факто единственный EGRP-протокол, связывающий разрозненные автономные системы, по результатам проведенных измерений [35] показывает возможность возникновения значительных задержек при перестроении маршрутов, достигающих нескольких минут. Забегая вперед (см. главу 4), можно отметить, что данное время сопоставимо с длительностью UPDATE-периода. Целесообразность перевода приоритетного трафика наложенной балансировочной сети на обходные пути в данном случае должна быть исследована дополнительно, т.к. дать однозначную оценку эффективности подобного перевода во всем множестве разнообразных условий организации наложенной сети, а также связности физической инфраструктуры не представляется возможным.

Ускорение обнаружения потери связности в наложенной балансировчной сети может быть достигнуто с помощью отслеживания периодических запросов, рассылаемых для мониторинга загруженности каналов. Потеря нескольких пакетов в данном случае служит индикатором возникшей аварии аналогично тому, как это реализовано в механизме BFD (Bidirectional Forwarding Detection).

Выводы

Изучена концепция децентрализованной самоорганизующейся наложенной балансировочной сети, позволяющей передавать агрегированный трафик, суммарная интенсивность которого превышает возможности передачи с помощью традиционной маршрутизации по кратчайшим путям. Определены базовые принципы организации наложенной балансировочной сети и соответствующие им процедуры.

Наложенный принцип построения является характерной чертой современных мультисервисных сетей. Проектирование подобных сетей более эффективно с применением модели в виде многослойного графа.

Использование в качестве модели источника информационного потока модели многоуровневого ON-OFF источника позволяет учесть взаимодействие элементов телекоммуникационной на различных уровнях модели ВОС. Приведены выражения позволяющие определить статистические характеристики информационного потока создаваемого пользователем на разных уровнях модели ВОС, а также характеристики потока создаваемого группой абонентов.

3. АНАЛИЗ ФУНКЦИОНИРОВАНИЯ НАЛОЖЕННЫХ СЕТЕЙ В СЕТЯХ ТЕЛЕКОММУНИКАЦИИ

На сегодняшний день качество обслуживания (Quality of Service, QoS) в территориально-распределенных мультисервисных телекоммуникационных сетях (ТКС) во многом определяется перечнем поддерживаемых средств управления трафиком – маршрутизации, резервирования ресурсов, классификации и маркировки пакетов, профилирования трафика и др. С введением новых услуг и повышением требований к качеству обслуживания соответствующие модификации должны коснуться в т.ч. протоколов и механизмов управления трафиком в ТКС. Все острее стоит проблема обеспечения гарантий качества обслуживания одновременно по нескольким показателям в условиях согласованного управления разнотипными сетевыми ресурсами (канальными, буферными ресурсами, трафиком) при реализации много путевых и динамических стратегий маршрутизации.

Как показал проведенный анализ [36], серьезным сдерживающим фактором в успешной реализации на практике ключевых концепций управления трафиком (Traffic Engineering (TE), MultiPath Routing, QoS-Based Routing, Constrained-Based Routing), является несовершенство положенных в их основу математических моделей и методов. Все попытки обеспечить согласованное решение отдельных задач управления трафиком, как правило, наталкиваются на проблему масштабируемости решений, под которой понимается свойство сети сохранять эффективность своего функционирования в заданных пределах при росте территориальной распределенности ТКС, увеличении числа контролируемых показателей QoS, количества обслу живаемых трафиков и т.д. Проблемы с масштабируемостью решений, как правило, сказываются на росте объемов циркулируемой в сети служебной информации, повышении сложности вычислительной реализации того или иного метода (модели, протокола) управления трафиком.

В ряде важных случаев выходом из создавшейся ситуации является использование иерархических (иерархическое-координационных) решений, способствующих повышению масштабируемости управления трафиком в территориально-распределенных ТКС. Однако и в рамках автономных систем (для IP-сетей) или кластеров (в ATM-сетях) проблема масштабируемости может сохранить свою актуальность, особенно при обеспечении гарантий качества обслуживания, требующего, в частности, и резервирования сетевых ресурсов. В этом случае основная трудность заключается в том, что много путевая маршрутизация, с одной стороны, способствует обеспечению более сбалансированной загруженности ТКС, но с другой, затрудняет решение задач распределения и резервирования канального ресурса (пропускной способности каналов связи) с поддержкой QoS. В этой связи в работе предлагается подход, основанный на расчете и использовании так называемых оверлейных сетей, которые определяли бы вероятный граф решения задач многопутевой маршрутизации (МПМ), на котором решения задач распределения и резервирования пропускной способности каналов связи обладали бы большей масштабируемостью.

3.1. Модель наложенных сетей с обеспечением гарантированного качества обслуживания

В работе [37] была предложена комплексная модель управления трафиком с обеспечением гарантированного качества обслуживания, в рамках которой реализуется требование мультисервисности за счет поддержки множества служб, минимизируется стоимость использования канальных ресурсов и обеспечивается согласованное решение задач МПМ, динамического распределения канальных ресурсов и гарантированного качества обслуживания по временным, скоростным показателям и показателям надежности. Данная модель является дальнейшим развитием модели, предложенной в работе [38].

Основу модели составляют ряд условий. Прежде всего, это условие сохранения потока для трафиков θ-й службы, которое может быть представлено в следующем виде:

$$\gamma_{ij}^{(\theta)} = r_{ij}^{(\theta)} + \sum_{s\epsilon M_i} \gamma_{sj}^{(\theta)} \varphi_{ji}^{s(\theta)}, \qquad \sum_{j\in M_i} \gamma_{ij}^{(\theta)} \varphi_{js}^{i(\theta)} = \alpha_{is}^{(\theta)}, \tag{3.1}$$

$$\varphi_{js}^{i(\theta)} = \begin{cases} 0, \text{если } i = j; \\ \geq 0, \text{если } i \neq j, \end{cases} \qquad \sum_{s\epsilon M_i} \varphi_{js}^{i(\theta)} = 1, \tag{3.2}$$

где $\gamma_{ij}^{(\theta)}$– интенсивность трафика -й службы в i -м узле, определяемая как сумма входного потока и потока, поступающего на i -й узел от смежных узлов для j -го узла; $\varphi_{js}^{i(\theta)}$ – маршрутная переменная, характеризующая долю потока $\gamma_{ij}^{(\theta)}$, протекающего из i -го узла по тракту $r_{ij}^{(\theta)}$ – интенсивность входного трафика θ -й службы, поступающего в сеть через i -й узел и адресованного j -му узлу; $\alpha_{is}^{(\theta)}$ – интенсивность трафика θ-й службы в тракте (i, j) ; M_i – множество узлов, смежных i -му узлу.

Выполнение условия сохранения потока для трафиков -й службы (3.1) с одновременным ограничением на маршрутные переменные (3.2) дает возможность реализовать требование, связанное с реализацией МПМ и обеспечением сбалансированной загрузки ТКС. Описать динамический характер распределения канальных ресурсов можно, дополнив условия отсутствия перегрузки каналов связи ограничением на количество используемых канальных ресурсов:

$$0 \leq \alpha_{is}^{(\theta)} \leq \varphi_{ij}^{(\theta)}, \tag{3.3}$$

$$\varphi_{ij}\, \beta_{ij}^{(\theta)} = \varphi_{ij}^{(\theta)} (0 \leq \beta_{ij}^{(\theta)} \leq 1), \tag{3.4}$$

$$\sum_{\theta=1}^{\theta} \varphi_{ij}^{(\theta)} \leq \varphi_{ij} \quad \text{или} \quad \sum_{\theta=1}^{\theta} \beta_{ij}^{(\theta)} \leq 1, \tag{3.5}$$

где $\beta_{ij}^{(\theta)}$– доля выделенного канального ресурса для трафика θ -й службы в канале (i, j) ; $\varphi_{ij}^{(\theta)}$ – выделенный объем канальных ресурсов для трафиков θ -й службы в канале (i, j) ; φ_{ij} – пропускная способность канала (i, j) .

Дополнительная группа ограничений, связанная с формулировкой достаточных условий обеспечения сквозного (end-to-end) QoS, в общем случае имеет вид:

$$\tau^{(\theta)} \le \tau_{\text{трб}}^{(\theta)}; \quad \sigma^{(\theta)} \le \sigma_{\text{трб}}^{(\theta)}; \quad \rho^{(\theta)} \le \rho_{\text{трб}}^{(\theta)}, \tag{3.6}$$

где $\tau_{\text{трб}}^{(\theta)}$, $\sigma_{\text{трб}}^{(\theta)}$, $\rho_{\text{трб}}^{(\theta)}$ – требуемые значения выбранных показателей QoS: соответственно средней задержки ($\tau^{(\theta)}$), джиттера ($\sigma^{(\theta)}$) и вероятности своевременной доставки пакетов ($\rho^{(\theta)}$) трафиков θ -й службы. В работе [7] с помощью тензорного анализа сетей эти общие условия (3.6) представлены аналитическими выражениями, т.е. в виде зависимости численных значений того или иного показателя QoS от структурных и функциональных параметров ТКС в условиях реализации многопутевой стратегии маршрутизации. Для минимизации объема используемых канальных ресурсов при обеспечении QoS в качестве критерия оптимальности получаемых решений использован стоимостной критерий:

$$D = \min_{\alpha,\varphi} \sum_{\theta=1}^{\theta} \sum_{i=1}^{m} \sum_{\substack{j=1 \\ j \neq 1}}^{m} \alpha_{ij}^{(\theta)} \varphi_{ij}^{(\theta)}, \tag{3.7}$$

где $\alpha_{ij}^{(\theta)}$– условная стоимость использования (резервирования) единицы канального ресурса для трафиков θ -й службы в канале (i, j) , т.е. фактически $\varphi_{ij}^{(\theta)}$ является метрикой данного канала.

3.2. Анализ решений по управлению трафиком в рамках рассмотренной модели

Стоит учесть, что при расчете потоков и распределении пропускных способностей каналов связи в рамках данной модели (3.1)-(3.7)

обеспечивался расчет множества путей, вдоль которых обеспечивались бы гарантии качества обслуживания одновременно по нескольким показателям QoS. При использование линейной целевой функции в ходе управления трафиком позволяет реализовать многопутевую маршрутизацию с последовательным включением путей, которая с практической точки зрения является более экономной при технологической

реализации, чем маршрутизация по всему множеству всех доступных маршрутов. Причем каждый последующий маршрут «включался», когда уже используемое множество путей не обеспечивало заданного уровня качества обслуживания.

В этой связи назовем множество рассчитанных маршрутов при заданных требованиях к качеству обслуживания графом решений, который являлся ориентированным. Вершины и дуги графа решений составляли узлы и каналы сети, входящие в рассчитанное множество рассчитанных маршрутов. В качестве примера рассмотрим сеть, структура которой представлена на рис. 3.1, а в разрывах каналов связи указаны их пропускные способности (Мбит/с). При маршрутизации трафика интенсивности 150 Мбит/с от пятого узла к десятому могут использоваться узлы 5, 6, 7, 8, 9, 10, а также соединяющие их каналы связи. Причем по пути 5-6-7-10 маршрутизировался трафик интенсивности 45 Мбит/с; по пути 5-6-10 – 35 Мбит/с; по пути 5-8-9-6-10 – 20 Мбит/с; по пути 5-8-9-10 –45 Мбит/с. Таким образом, в граф решений входят вершины (узлы сети) 5÷10 и соединяющие их дуги (каналы связи).

Граф решений задачи управления трафиком во многом определяется уровнем требований к качеству обслуживания. Так, например, при увеличении интенсивности трафика до 200 Мбит/с в дополнение к ранее полученному графу решений (рис.3.1) добавится путь 5-8-12-9-10 (рис.3.2). Такая же ситуация наблюдается и при ужесточении других показателей качества обслуживания – средней задержки, джиттера, вероятности потерь пакетов.

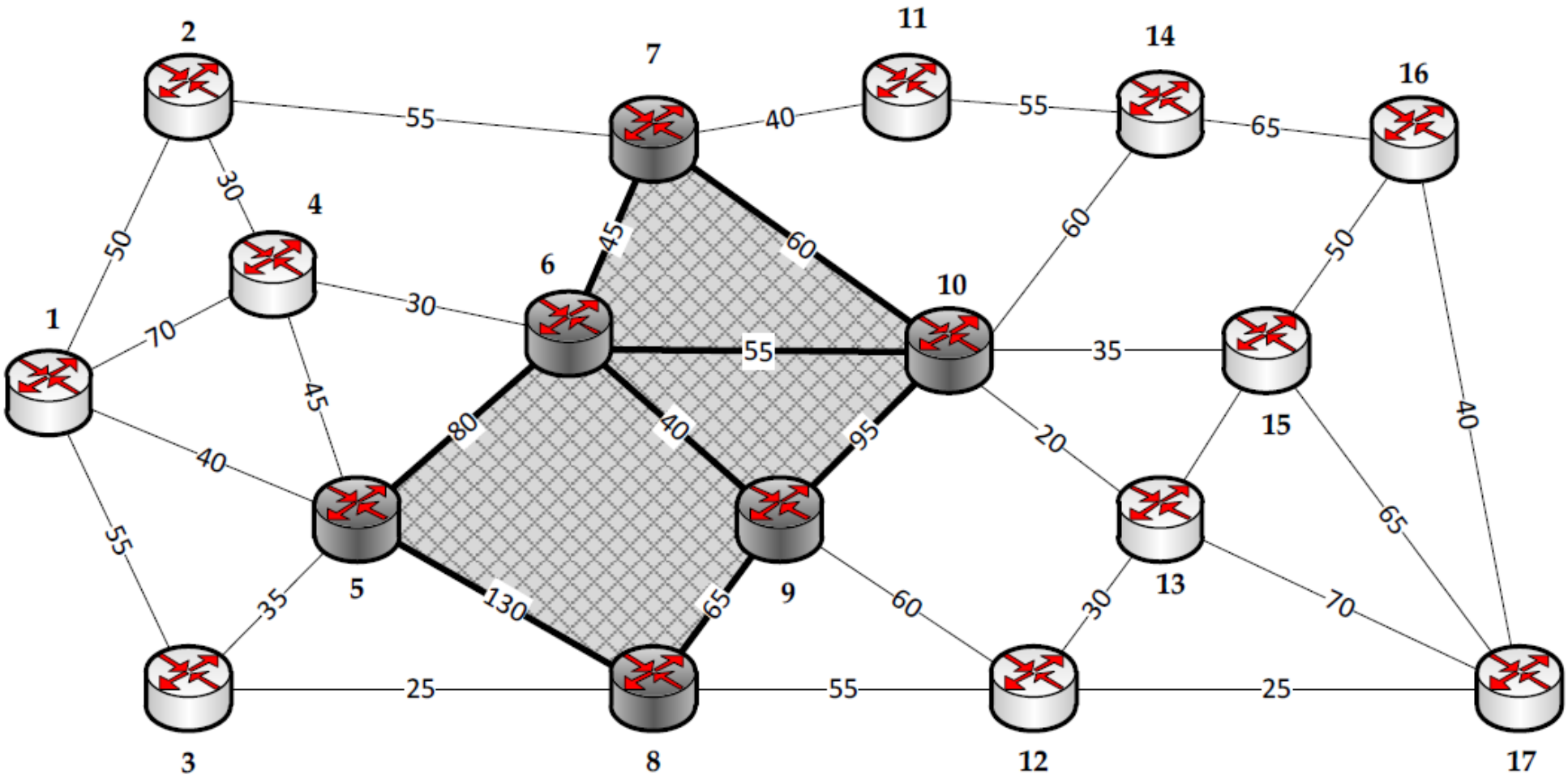


Рис. 3.1. Структура ТКС и граф решений задачи управления трафиком интенсивности 150 Мбит/с

Кроме того, важно отметить, что граф решений задачи управления трафиком может существенно отличаться от исходной структуры сети. Это связанно с тем, что в рамках предложенной модели (3.1)-(3.7) используется минимум канальных ресурсов (в т.ч. и количество каналов связи в целом) для обеспечения гарантированного QoS. Поэтому при решении задач QoS нецелесообразно использовать информацию о состоянии всей сети, необходимо ограничить поиск графа решений некоторой заранее определенной областью. А с целью повышения масштабируемости решений задач управления трафиком в рамках модели (3.1)-(3.7) расчет маршрутных переменных и переменных, отвечающих за динамическое распределение канального ресурса, целесообразно производить, основываясь не на общей структуре сети, а на структуре предварительно выбранной наложенной (оверлейной) сети, максимально совпадающей с предполагаемым графом решений. Таким образом, актуальной представляется задача, связанная с расчетом (определением) структуры подобной оверлейной сети (Overlay Network, ON). При этом структура оверлейной сети должна максимально адаптироваться к уровню QoS-требований. В предельном случае оверлейная сеть должна полностью совпадать с предполагаемым графом решений.

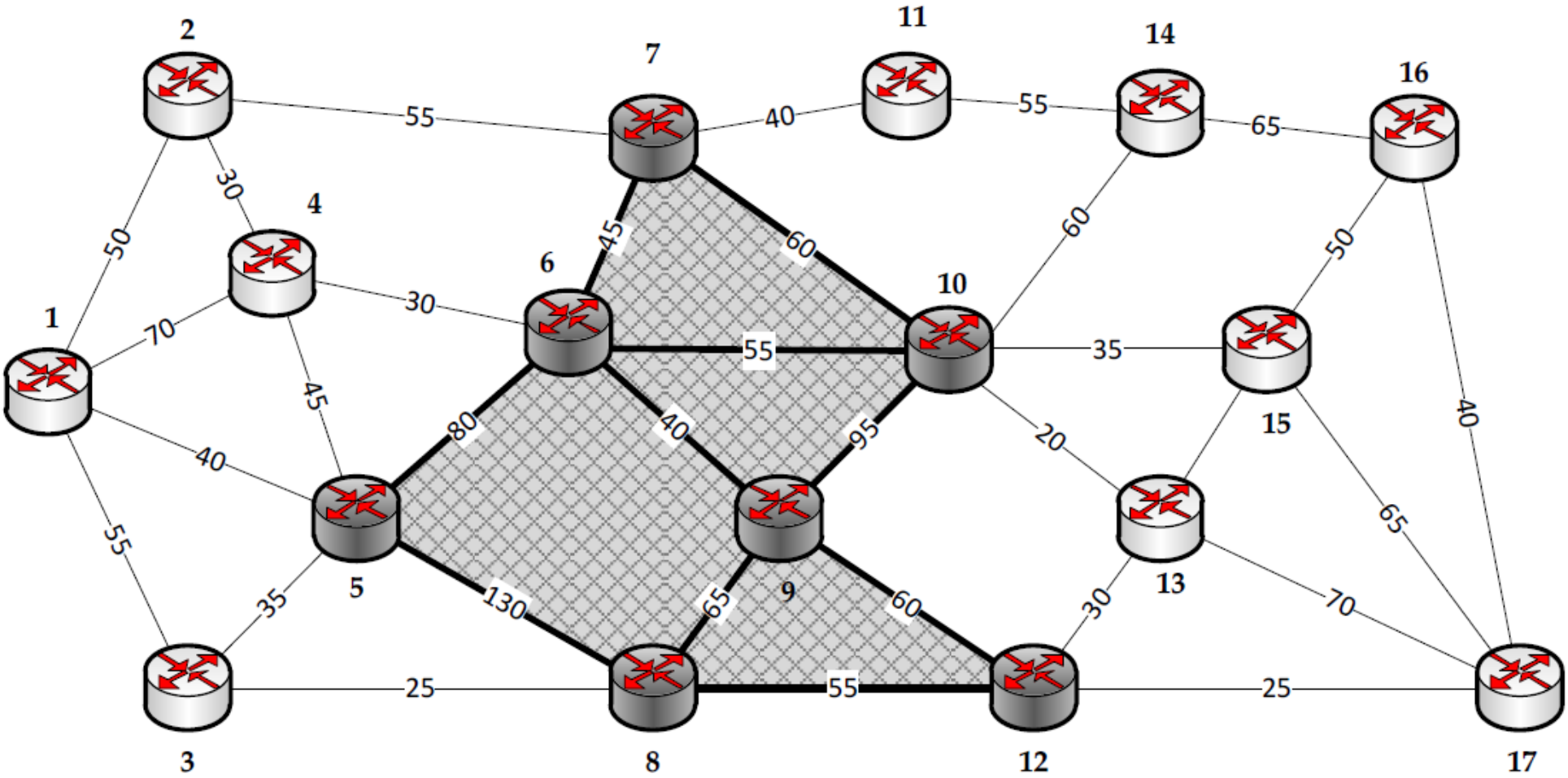


Рис. 3.2. Структура ТКС и граф решений задачи управления трафиком интенсивности 200 Мбит/с

3.3. Метод управления трафиком в территориально-распределенных мультисервисных ТКС

Обобщенная структура метода представляет собой иерархическую структуру,состоящую из 5 этапов в соответствии с решаемыми задачами.

Этап 1. Анализ исходных данных для решения задачи:

- анализ структуры ТКС (числа узлов, каналов связи, связности сети);
- анализ количества и содержания поддерживаемых служб;
- анализ требований к качеству обслуживания для трафиков каждой службы

$\tau_{\text{трб}}^{(\theta)}$, $\sigma_{\text{трб}}^{(\theta)}$, $\rho_{\text{трб}}^{(\theta)}$ в соответствии с договором на обслуживание (SLA).

Этап 2. Адаптивный выбор структуры оверлейных сетей для каждой пары узлов «отправитель-получатель».

После анализа исходных данных осуществляется выбор оверлейной структуры, по которой в дальнейшем осуществляются все расчеты. Для определения структуры ON предлагается использовать алгоритмы расчета мультипутей. Их применение основано на переходе от формализации задач нахождения кратчайшего пути в сети к описанию задач поиска некоторого множества путей – мультипутей (multipath). В результате расчетов определяется мультипуть, оптимальный в рамках выбранной метрики, который и принимался в качестве структуры оверлейной сети.

Основными алгоритмами поиска мультипутей в сети между заданной парой узлов являются [39]:

ECMP (Equal Cost Multipath) – алгоритм расчета путей равной стоимости, который может использоваться в расширениях протокола OSPF, оптимизированного под многопутевые решения;

- DASM (Diffusing Algorithm for Shortest Multipath) – алгоритм, обобщающий алгоритмы Дийкстры/Шолтена и гарантирующий отсутствие петель в рассчитываемых таблицах маршрутизации;

- ROAM (Routing On-Demand Acyclic Multipath) – алгоритм, поддерживающий многопутевой способ доставки пакетов без образования петель, он адаптирован для сетей с ограниченной мобильностью;
- MDVA (multipath distance vector algorithm) – алгоритм, который обобщает распределенный алгоритм Беллмана-Форда на случай расчета множества кратчайших путей;
- MPATH (Multipath Routing Algorithm) – алгоритм, обобщающий дерево кратчайших путей, получаемых в алгоритмах Дийкстры и Беллмана-Форда, в граф кратчайших мультипутей разной стоимости;
- MPDA (Multipath Partial Dissemination Algorithm), QMPDA (Quality Multiple Partial Dissemination Algorithm) – алгоритмы с частичным распространением информации о состоянии сети, которые обеспечивают расчет множества беспетельных путей с учетом изменения состояния сети, в т.ч. при выходе их из строя (QMPDA), также поддерживает различные классы обслуживания трафиков.

При выборе структуры ON также может использоваться, например, алгоритм двойного поиска, который находит k-кратчайших путей из некоторой фиксированной вершины ко всем остальным вершинам исходного графа. Обобщенный алгоритм Данцига и обобщенный алгоритм Флойда также находят k-первых кратчайших путей между каждой парой вершин исходного графа [40]. Суть данных алгоритмов состоит в выполнении последовательности операций сложения и сравнения на минимум. Применение первого алгоритма, как показал анализ, в вычислительном аспекте не слишком эффективно, так как часть информации, получаемой в ходе решения, не используется. В основу обобщенных алгоритмов Данцига и Флойда положены те же принципы, что и при построении исходного алгоритма. Отличие состоит в том, что в обобщенных алгоритмах используются обобщенные операции сложения и сравнения. Кроме того, в

этих алгоритмах возможно возникновение кратчайших путей, включающих контуры, привязанные к начальной и конечной вершинам рассматриваемых путей. Отличительной особенностью отмеченных алгоритмов поиска k-кратчайших путей является то, что получаемые в итоге пути, в общем случае, могут пересекаться.

Возможно несколько вариантов решения задачи выбора ON в зависимости от уровня QoS-требований и загруженности сети. На основе анализа загруженности ТКС (ρ) принимается решение об использовании того или иного алгоритма для выбора структуры оверлейных сетей для каждой пары узлов. Структурная схема метода управления трафиком с обеспечением гарантированного QoS на основе адаптивного выбора структуры ON и комплексного решения задач многопутевой маршрутизации и динамического распределения канального ресурсов.

Экспериментально установлено, что в случае, если $\rho \leq$ (0,65...0,7), выбор структуры ON лучше осуществлять с помощью графокомбинаторных алгоритмов поиска кратчайшего мультипути. В случае, если $\rho \geq$ (0,65...0,7), выбор структуры ON осуществляется с помощью алгоритмов поиска k - кратчайших путей. Применение алгоритмов поиска k -кратчайших путей возможно также и при $\rho \leq$ (0,65...0,7) , в случае высоких QoS-требований (например при передаче мультимедийной информации реального времени).

Этап 3. На выбранной структуре ON осуществляется расчет маршрутных переменных и переменных управления канальными ресурсами в рамках описанной выше комплексной модели (3.1)-(3.7).

Этап 4. Полученные решения анализируются на предмет выполнения условий обеспечения гарантированного QoS (6). В случае невыполнения условий необходимо пересмотреть выбор структуры ON (этап 2) (например, перейти от структуры с непересекающимися путями к структуре с пересекающимися путями).

Если после выбора новой структуры ON и решения комплексной задачи требования не выполняются, необходимо пересмотреть исходные

данные (этап 1) в сторону ослабления QoS-требований, если это возможно. В противном случае некоторые трафики, как правило менее приоритетные, получают отказ в обслуживании.

3.4. Анализ предложенного метода управления трафиком

В ходе исследования метода к рассмотрению принимались структуры ТКС, состоящие из 10÷50 сетевых узлов (рис. 3.3), связность ($k_{св}$) которых варьировалась в пределах от 2 до 5. Принималось, что все каналы связи образованы дуплексными каналами связи, пропускные способности варьировались от 100 до 300 Мбайт/с. Следует отметить, что использование модели (3.1)-(3.7) в рамках предложенного метода позволяет обеспечить пропорциональный рост объема используемых ресурсов в зависимости от величины внешней загрузки r0 и QoS- требований (3.6). В свою очередь, это позволило обеспечить те же значения показателей QoS, что и при использовании известных моделей маршрутизации, заложенных в протоколы RIP, IGRP, OSPF, при этом сократив объемы используемых канальных ресурсов в среднем от 15 до 30 %.

Оценка масштабируемости решений, получаемых в рамках предложенного метода, производилась по показателям временной и вычислительной сложности, а также по степени близости структур ON и графа решений. Степень идентичности (близости) структуры ON и графа решений оценивалась по коэффициенту идентичности $k_{\text{и}}$, для расчета которого использовалось следующее выражение:

$$k_{\text{и}} = n_*/n_0 \,, \qquad (3.8)$$

в котором n_0 – число каналов в структуре ON; n_* – число каналов в исходной ТКС, которые представлены одновременно и в ON, и в графе решений.

Как показали результаты анализа , с ростом загруженности ТКС практически для всех вариантов использования предложенного метода

коэффициент идентичности (3.8) с ростом r_0 также возрастал. При этом в зоне низких нагрузок (r_0 =0,1÷0,3) $k_и \approx$ 0,3÷0,5; в зоне средней нагрузки (r_0 =0,3÷0,6) $k_и \approx$ 0,7÷0,9; в зоне высокой нагрузки (r_0 =0,6÷0,9) $k_и \approx$ 0,7÷0,9;

Значение коэффициента идентичности в конечном итоге сказывалось на суммарной стоимости использования сетевых ресурсов (3.7) при решении задач обеспечения QoS. Чем выше значения $k_и$, тем меньше должно быть расхождение в стоимости использования канальных ресурсов при решении задач обеспечения QoS, основываясь на исходной (полной) структуре ТКС или только на структуре ON. Это особенно характерно для зоны высокой нагрузки , где расхождение в стоимости в среднем составляло 5-7%. Однако при больших значениях коэффициента идентичности ($k_и \approx 0.3,...,0.5$) в зоне низких нагрузок наблюдалась преимущественно ситуация, когда ON не повторяла граф решений, но практически содержала его в качестве своей подсети, что также не способствовало излишнему росту стоимости использования канальных ресурсов. Расхождения в структуре ON и графа решений в области средней нагрузки (r_0 =0,3÷0,6) приводило к повышению общей стоимости использования сетевых ресурсов в среднем до 11-15% .

В общем случае размерность оптимизационной задачи определяется количеством управляющих переменных и зависит от числа узлов, количества каналов связи и поддерживаемых сетью служб. Сложность реализации комплексной модели составляет $R = \Theta(m^2(m-1)+n)$. В рамках предложенного метода за счет применения алгоритмов выбора ON размерность задачи обеспечения QoS может быть значительно уменьшена (в среднем на 30-55%) за счет снижения количества анализируемых на сети узлов и каналов связи (рис. 3.3). При этом использование алгоритма поиска k -кратчайших путей (A1) позволило сократить число каналов связи в ON по сравнению со структурой исходной ТКС в среднем на 25-55%; использование алгоритма MPATH – в среднем на 40-60% (A2); использование алгоритма MDVA – в среднем на 40-75% (A3).

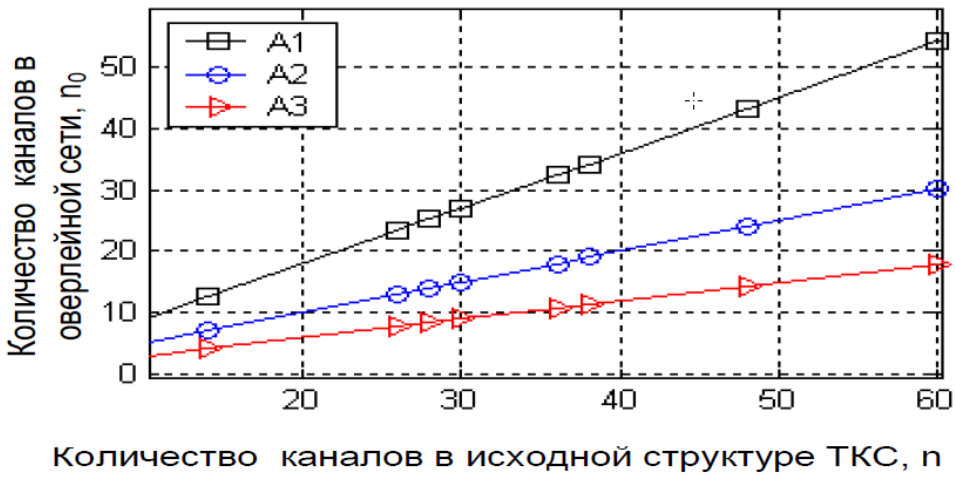
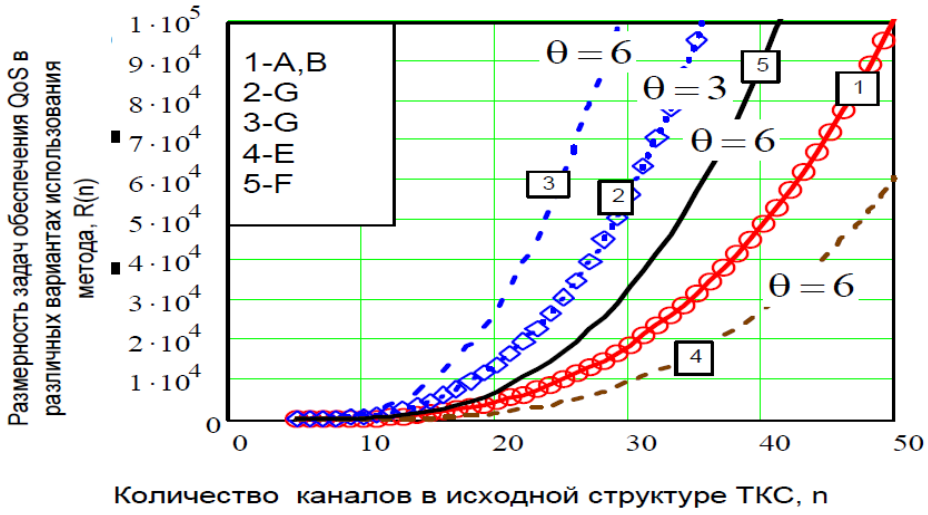
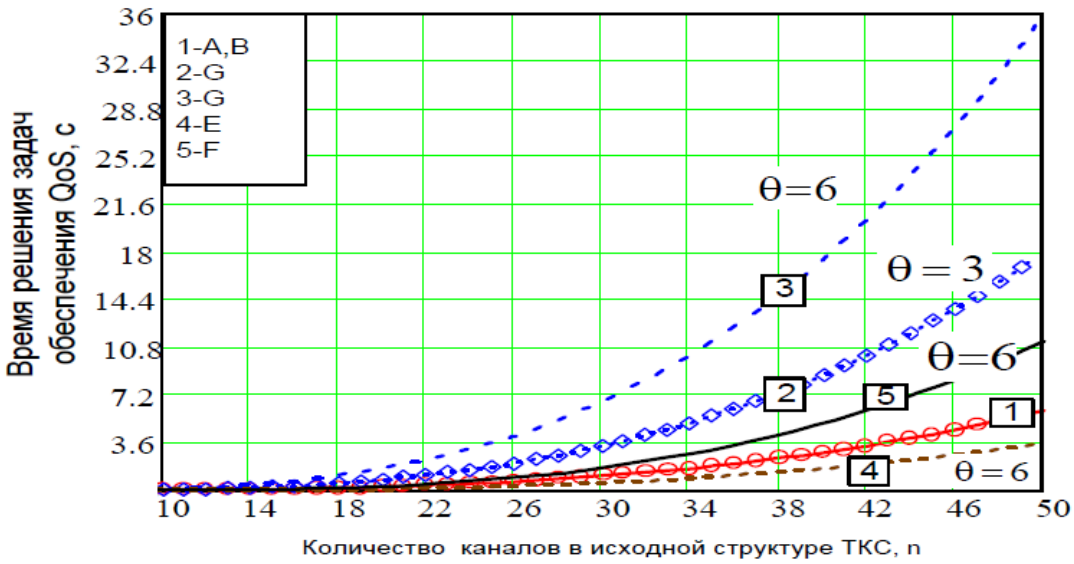


Рис. 3.3. Результаты анализа масштабируемости предложенного метода

Результаты сравнения размерности оптимизационных задач (3.7) при различных вариантах реализации метода и числа поддерживаемых служб представлены на рис.3.4 а.



а)



б)

Рис. 3.4. Результаты анализа вычислительной (а) и временной сложности (б) предложенного метода управления трафиком с обеспечением гарантированного QoS

Из полученных результатов можно сделать вывод, что использование метода управления трафиком для обеспечения QoS снижает сложность задач при одинаковом количестве служб в среднем в три-пять раз, т.к. при выборе оверлейной структуры снижается не только число анализируемых каналов связи (рис. 3.4), но и число узлов. Размерность решаемых задач непосредственно влияет на время решения, которое в целом определяет период пересчета, например, маршрутных таблиц и других управляющих воздействий. Как показали результаты моделирования (рис. 3.6 б), общее время решения задачи обеспечения QoS в рамках большинства вариантов реализации предлагаемого метода не превышало 30-35 с. Это вполне отвечает значениям таймеров (от 30 до 90 с) используемых на практике управляющих протоколов.

Выводы

Предложены модель и метод управления трафиком с обеспечением гарантированного QoS на основе адаптивного выбора структуры ON и комплексного решения задач многопутевой маршрутизации и динамического распределения канальных ресурсов. Использование в методе оверлейных сетей ориентирует на повышение масштабируемости получаемых решений, т.к. решение задач многопутевой маршрутизации и распределения канальных ресурсов в итоге осуществляется на структуре значительно меньшей размерности. Осуществлен анализ показателей эффективности, по которым оценивалось качество получаемых решений, связанных с обеспечением гарантированного качества обслуживания в мультисервисных ТКС, в рамках предложенного метода.

За счет применения алгоритмов выбора оверлейных сетей в рамках предложенного метода управления трафиком для обеспечения QoS удалось гарантировать заданные значения показателей качества обслуживания, но с существенным снижением (в три-пять раз) размерности положенной в основу данного метода оптимизационной задачи, что влечет за собой на практике пропорциональное снижение объемов циркулируемой служебной информации о загруженности каналов связи ТКС. При этом особенно ощутим выигрыш в применении разработанного метода для ТКС высокой размерности (с количеством узлов 15-20) и высокой связностью узлов (3 и выше), что характерно при построении современных территориально-распределенных мультисервисных сетей.

Предлагаемый метод отвечает требованиям современных концепций управления сетевыми ресурсами, трафиком и маршрутизацией, например Active network, Traffic Engineering, MultiPath Routing, QoS-Based Routing и Constraint-Based Routing, расширяя область применения в условиях согласованной реализации динамических стратегий многопутевой маршрутизации и распределения канальных ресурсов ТКС.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Взаимодействие человека и техносферы

Человек и окружающая его среда гармонично взаимодействуют и развиваются лишь в условиях, когда потоки энергии, вещества и информации

находятся в пределах, благоприятно воспринимаемых человеком и природной средой. Любое превышение привычных уровней потоков сопровождается негативными воздействиями на человека, техносферу.

Человек и окружающая его среда (производственная) в процессе жизнедеятельности постоянно взаимодействуют друг с другом. При этом жизнь может существовать только в процессе движения через живое тело потоков вещества, энергии и информации.

Человек и окружающая его среда гармонично взаимодействуют и развиваются лишь в условиях, когда потоки энергии, вещества и информации находятся в пределах, благоприятно воспринимаемых человеком и природной средой. Любое превышение привычных уровней потоков сопровождается негативными воздействиями на человека, техносферу и/или природную среду. В условиях техносферы негативные воздействия обусловлены элементами техносферы (машины, сооружения и т. п.) и действиями человека.

Изменяя величину любого потока от минимально значимой до максимально возможной, можно пройти ряд характерных состояний взаимодействия в системе “человек - среда обитания”:

- комфортное (оптимальное), когда потоки соответствуют оптимальным условиям взаимодействия: создают оптимальные условия деятельности и отдыха; предпосылки для проявления наивысшей работоспособности и как следствие продуктивности деятельности; гарантируют сохранение здоровья человека и целостности компонент среды обитания;

- допустимое, когда потоки, воздействуя на человека и среду обитания, не оказывают негативного влияния на здоровье, но приводят к дискомфорту, снижая эффективность деятельности человека. Соблюдение условий допустимого взаимодействия гарантирует невозможность возникновения и развития необратимых негативных процессов у человека и в среде обитания;

Из четырех характерных состояний взаимодействия человека со средой обитания лишь первые два (комфортное и допустимое) соответствуют позитивным условиям повседневной жизнедеятельности, а два других (опасное и чрезвычайно опасное) - недопустимы для процессов жизнедеятельности человека.

Взаимодействие человека со средой обитания может быть позитивным или негативным, характер взаимодействия определяют потоки веществ, энергий и информации.

Различают опасности естественного, техногенного и антропогенного происхождения. Для защиты от повседневных (холод,слабая освещенность и т. д.) опасностей человек использует жилище, одежду, системы вентиляции, отопления и кондиционирования, а также системы искусственного освещения. Обеспечение комфортных условий жизнедеятельности практически решает все проблемы защиты от повседневных опасностей.

Техногенные опасности создают элементы техносферы - машины, сооружения, вещества и т. п., а антропогенные опасности возникают в результате ошибочных или не санкционированных действий человека или групп людей.

Чем выше преобразующая деятельность человека, тем выше уровень и число опасностей - вредных и травмирующих факторов, отрицательно воздействующих на человека и окружающую его среду.

Вредный фактор - негативное воздействие на человека, которое приводит к ухудшению самочувствия или заболеванию. Травмирующий (травмоопасный) фактор - негативное воздействие на человека, которое приводит к травме или летальному исходу.

Жизнедеятельность человека потенциально опасна. Аксиома предопределяет, что все действия человека и все компоненты среды обитания, прежде всего технические средства и технологии, кроме позитивных свойств и результатов, обладают способностью генерировать травмирующие и вредные факторы. При этом любое новое позитивное

действие или результат неизбежно сопровождается возникновением новых негативных факторов.

Значительным техногенным опасностям подвергается человек при попадании в зону действуя технических систем: транспортные магистрали; зоны излучения радио- и телепередающих систем, промышленные зоны и т. п. Уровни опасного воздействия на человека в этом случае определяются характеристиками технических систем и длительностью пребывания человека в опасной зоне. Вероятно проявление опасности и при использовании человеком технических устройств на производстве и в быту: электрические сети и приборы, станки, ручной инструмент, газовые баллоны и сети, оружие и т. п. Возникновение таких опасностей связано как с наличием неисправностей в технических устройствах, так и с неправильными действиями человека при их использовании. Уровни возникающих при этом опасностей определяются энергетическими показателями технических устройств.

В настоящее время перечень реально действующих негативных факторов значителен и насчитывает более 100 видов. К наиболее - распространенным и обладающим достаточно высокими концентрациями или энергетическими уровнями относятся вредные производственные факторы: запыленность, шум, вибрации, электромагнитные поля, ионизирующие излучения, повышенные или пониженные параметры атмосферного воздуха (температуры, влажности, подвижности воздуха, давления), недостаточное и неправильное освещение, монотонность деятельности и др.

Качество освещения, особенно в условиях производства, играет важную роль в деятельности человека.

Плохо освещенные травмоопасные зоны, слепящие источники света, резкие тени от предметов и оборудования ухудшают ориентацию работающих, вследствие чего может быть травмирование.

Недостаточное или неправильное освещение рабочих мест и всего помещения вызывает преждевременное утомление организма, может быть причиной снижения производительности труда и, что очень важно, быть причиной производственного травматизма.

Неправильно выбранные при проектировании осветительные приборы и аппаратура, а также нарушения правил технической эксплуатации могут быть причиной пожара, взрыва, аварии на производстве.

Освещение производственных помещений и рабочих мест может быть как естественным так и искусственным. Последнее осуществляется с помощью источников света – ламп накаливания, люминесцентных ламп или дуговых ламп.

Основными величинами, характеризующими свет, являются световой поток, сила света, светимость, яркость, освещенность.

Наиболее распространенные источники света - это лампы накаливания и люминесцентные лампы (дневного света).

Большую роль в создании экономичного и высококачественного электрического освещения играют светильники – приборы, в которых осуществляется направленное перераспределение светового потока.

Параметрами ламп являются номинальная мощность(в цепи питания), Вт; номинальное напряжение, В; световая отдача, оцениваемая в люменах на 1 ВТ; световой поток, лм; средняя продолжительность горения, ч.

Люминесцентные лампы работают на принципе преобразования невидимого ультрафиолетового излучения газового разряда в парах ртути в видимое свечение люминофоров, которыми покрыта внутренняя поверхность стеклянной газоразрядной трубки. Такие лампы низкого давления типов ЛДЦ, ЛД, ЛХБ, ЛТБ и ЛБ широко применяются для общего освещения производственных отапливаемых помещений. Их называют лампами дневного света, поскольку они излучают свет, по своему спектру, близкий к дневному, чем обеспечивается правильная цветопередача.

Вследствие значительной яркости люминесцентных ламп открытая их установка без светильника не допускается.

4.2. Психофизиологическая нагрузка на человека

В раздел психофизиологических нагрузок наиболее важное значение занимает стресс и утомление.

Под стрессом (от англ. stress — “давление”, “напряжение”) понимают эмоциональное состояние, возникающее в ответ на всевозможные экстремальные воздействия.

При стрессе обычные эмоции сменяются беспокойством, вызывающим нарушения в физиологическом и психологическом плане. Это понятие было введено Г. Селье для обозначения неспецифической реакции организма на любое неблагоприятное воздействие. Его исследования показали, что различные неблагоприятные факторы — усталость, страх, обида, холод, боль, унижение и многое другое вызывают в организме однотипную комплексную реакцию вне зависимости от того, какой именно раздражитель действует на него в данный момент. Причем эти раздражители необязательно должны существовать в реальности. Человек реагирует не только на действительную опасность, но и на угрозу или напоминание о ней.

Поведение человека в ситуации стресса отличается от аффективного поведения. При стрессе человек, как правило, может контролировать свои эмоции, анализировать ситуацию, принимать адекватные решения.

В настоящее время в зависимости от стрессового фактора выделяют различные виды стресса, среди которых ярко выражены физиологический и психологический. Психологический стресс в свою очередь можно разделить на информационный и эмоциональный. Если человек не справляется с задачей, не успевает принимать верные решения в требуемом темпе при высокой степени ответственности, т.е., когда возникает информационная перегрузка, может развиться информационный стресс. Эмоциональный

стресс возникает в ситуациях, опасности, обиды и т.д. Г. Селье выделил в развитии стресса 3 этапа. Первый этап — реакция тревоги — фаза мобилизации защитных сил организма, повышающая устойчивость по отношению к конкретному травмирующему воздействию. При этом происходит перераспределение резервов организма: решение главной задачи происходит за счет второстепенных задач. На втором этапе — стабилизации всех параметров, выведенных из равновесия в первой фазе, закрепляются на новом уровне. Внешне поведение мало отличается от нормы, все как будто налаживается, но внутренне идет перерасход адаптационных резервов. Если стрессовая ситуация продолжает сохраняться, наступает третий этап — истощение, что может привести к значительному ухудшению самочувствия, различным заболеваниям и в некоторых случаях смерти.

Этапы развития стрессового состояния у человека:

- нарастание напряженности;
- собственно стресс;
- снижение внутренней напряженности.

По своей продолжительности первый этап строго индивидуален. Одни человек “заводится” в течение 2-3 минут, а у другого нарастание стресса может проходить в течение нескольких дней и даже недель. Но в любом случае, состояние и поведение человека, попавшего в стресс, меняется па “противоположный знак”.

Так, спокойный сдержанный человек становится суетливым и раздражительным, он может стать даже агрессивным и жестоким. А человек, в обычной жизни живой и подвижный, становится мрачным и неразговорчивым.

На первой стадии стресса у человека ослабевает самоконтроль: он постепенно теряет способность сознательно и разумно регулировать свое собственное поведение.

Второй этап развития стрессового состояния проявляется в том что у человека происходит потеря эффективного сознательного самоконтроля

(полная или частичная). “Волна” деструктивного стресса разрушительно действует на психику человека. Он может не помнить, что говорил и делал, или осознавать свои действия, довольно смутно, и не полностью. Многие потом отмечают, что в стрессовом состоянии они сделали то, что в спокойной обстановке никогда бы не сделали. Обычно все впоследствии очень жалеют об этом.

Также как и первый, второй этап по своей продолжительности строго индивидуален — от нескольких минут и часов — до нескольких дней и недель. Исчерпав свои энергетические ресурсы (достижение высшего напряжения отмечено когда человек чувствует опустошение, утомление и

Стрессовые состояния существенно влияют на деятельность человека. Люди с разными особенностями нервной системы по-разному реагируют на одинаковые психологические нагрузки. У одних людей наблюдается повышение активности, мобилизация сил, повышение эффективности деятельности. С другой стороны, стресс может вызвать дезорганизацию деятельности, резкое снижение ее эффективности, пассивность и общее торможение.

Поведение человека в стрессовой ситуации зависит от многих условий, но, прежде всего от психологической подготовки человека, включающей умение быстро оценивать обстановку, навыки мгновенной ориентировки в неожиданных обстоятельствах, волевую собранность и решительность, опыт поведения в аналогичных ситуациях.

Методы борьбы со стрессом

Стресс — это ощущение, которое испытывает человек, когда полагает, что не может эффективно справиться с возникшей ситуацией.

Если вызывающая стресс ситуация зависит от нас, необходимо более рационально сконцентрировать усилия на том, чтобы изменить ее. Если ситуация не зависит от нас, нужно смириться и менять свое восприятие, свое отношение к этой ситуации.

В большинстве ситуаций стресс проходит несколько стадий.

1. Фаза тревоги. Это мобилизация энергетических ресурсов организма. Умеренный стресс на этой стадии полезен, он ведет к повышению работоспособности.

2. Фаза сопротивления. Это сбалансированное расходование резервов организма. Внешне все выглядит нормально, человек эффективно решает встающие перед ним задачи, однако если эта стадия продолжается слишком долго и не сопровождается отдыхом, значит, организм работает на износ.

3. Фаза истощения (дистресс). Человек ощущает слабость и разбитость, снижается работоспособность, резко возрастает риск заболеваний. Непродолжительное время с этим еще можно бороться усилием воли, однако потом единственный способ восстановить силы — это основательный отдых.

Одна из наиболее часто встречающихся причин возникновения стрессов — противоречие между реальностью и представлениями человека**.**

Стрессовая реакция одинаково легко запускается как реальными событиями, так и существующими лишь в нашем воображении. В психологии это называется «закон эмоциональной реальности воображения». Как подсчитали психологи, порядка 70 % наших переживаний происходят по поводу событий, которые существуют не в реальности, а лишь в воображении.

К развитию стресса могут приводить не только отрицательные, но и положительные жизненные события. Когда что-то резко меняется в лучшую сторону, организм тоже реагирует на это стрессом.

Обычно под утомлением понимают уменьшение работоспособности, вызванное предшествующей работой, имеющее временный характер. Если оно возникает при умственной деятельности, то говорят об умственном утомлении. Состояние утомления проявляется в изменении физиологических процессов, в снижении производительности труда и технико-экономических показателей, в изменении психического статуса.

Психологи отмечают, что при развитии утомления у человека появляется особое состояние психики, которое называется утомляемостью - субъективное отражение возникающих в организме процессов, приводящих к утомлению. Оно появляется задолго до снижения производительности труда и заключается в том, что возникает переживание особого тягостного напряжения и неуверенности. Человек чувствует, что не в силах должным образом продолжать работу. При этом возникает расстройство внимания - при развитии утомления человек легко отвлекается, становится вялым, малоподвижным или, наоборот, у него появляются хаотическая подвижность, неустойчивость. Возникают расстройства в сенсорной области - при утомлении изменяется работа рецепторов, например, возникает зрительное утомление - снижается способность перерабатывать информацию, идущую через зрительный анализатор; при продолжительной ручной работе снижается тактильная и кинестетическая чувствительность. Возникают нарушения в моторной сфере: происходит замедление движений, появляются торопливость движений, расстройства ритма, ослабление точности и координированности движений, деавтоматизация движений. Наблюдаются дефекты памяти и мышления, ослабляются воля, решительность, выдержка, самоконтроль. При сильном утомлении появляется сонливость.

Выраженность изменений зависит от глубины утомления. Например, при слабом утомлении существенных изменений в психическом статусе почти нет, а при переутомлении все эти изменения крайне выражены.

В связи с изменением психического состояния ряд психофизиологов предлагает выделять 3 стадии утомления. 1-я стадия: при ней проявление чувства усталости незначительно, производительность труда не снижена. 2-я стадия - характеризуется значительным снижением производительности труда и выраженными психическими изменениями. 3-я стадия, которую некоторые исследователи расценивают как острое переутомление, сопровождается выраженным переживанием утомления.

Утомление может быть физическим (мышечным) или нервно-психическим (центральным). Обе формы утомления сочетаются при тяжелой работе, и их нельзя строго отделить одну от другой. Тяжелая физическая работа приводит в первую очередь к мышечному утомлению, а усиленная умственная или монотонная работа вызывает утомление центрального происхождения. Следует четко разграничивать утомление и усталость, обусловленную потребностью во сне.

Кроме того, определяют первичное утомление, которое развивается достаточно быстро, в начале рабочей смены и является признаком недостаточного упрочения трудовых навыков; оно преодолимо в процессе работы, в результате чего возникает "второе дыхание" - значительное повышение работоспособности. Вторичное, или медленно развивающееся утомление - собственно утомление, которое возникает примерно спустя 2,5-3 часа от начала рабочей смены, а для его снятия необходим отдых.

Переутомление, или хроническое утомление - еще один вид утомления. Оно обусловлено отсутствием надлежащего отдыха между рабочими днями, рассматривается как патологическое состояние. Проявляется общим падением производительности труда, увеличением заболеваемости, замедлением роста культурно-технического уровня и квалификации работающего; снижением творческой активности и умственной работоспособности, изменением в деятельности сердечно-сосудистой системы.

Согласно К. К. Платонову выделяют четыре степени переутомления - начинающееся, легкое, выраженное и тяжелое, каждая из которых требует соответствующих методов борьбы. Так, для снятия начинающегося переутомления достаточно регламентировать режим труда и отдыха. При легкой степени переутомления необходимо дождаться отпуска и эффективно использовать его. При выраженном переутомлении необходим срочный отдых, лучше - организованный. При тяжелой степени переутомления необходимо лечение.

4.3. Техногенное загрязнение среды

Эта глава посвящена техногенному загрязнению экосферы и среды обитания человека. Техногенное загрязнение среды является наиболее очевидной и быстродействующей негативной причинной связью в системе экосферы: «экономика, производство, техника, среда». Оно обусловливает значительную часть природоемкости техносферы и приводит к деградации экологических систем, глобальным климатическим и геохимическим изменениям, к поражениям людей. На предотвращение загрязнения природы и окружающей человека среды направлены основные усилия прикладной экологии.

Классификация техногенных воздействий, обусловленных загрязнением среды, включает такие основные категории:

1. Материально-энергетические характеристики воздействий: механические, физические (тепловые, электромагнитные, радиационные, акустические), химические, биологические факторы и агенты и их различные сочетания. В большинстве случаев в качестве таких агентов выступают эмиссии (т.е. испускания - выбросы, стоки, излучения и т.п.) различных технических источников.

2. Количественные характеристики воздействия: сила и степень опасности (интенсивность факторов и эффектов, массы, концентрации, характеристики типа «доза - эффект», токсичность, допустимость по экологическим и санитарно-гигиеническим нормам); пространственные масштабы, распространенность (локальные, региональные, глобальные).

3. Временные параметры и различия воздействий по характеру эффектов: кратковременные и длительные, стойкие и нестойкие, прямые и опосредованные, обладающие выраженными или скрытыми следовыми эффектами, обратимые и необратимые, актуальные и потенциальные; пороговость эффектов.

4. Категории объектов воздействия: различные живые реципиенты (т.е. способные воспринимать и реагировать) - люди, животные, растения; компоненты окружающей среды (среда поселений и помещений, природные ландшафты, поверхность земли, почва, водные объекты, атмосфера, околоземное пространство); изделия и сооружения.

В пределах каждой из этих категорий возможно определенное ранжирование экологической значимости факторов, характеристик и объектов. В целом по природе и масштабам актуальных воздействий наиболее существенны химические загрязнения, а самая большая потенциальная угроза связана с радиацией. Что касается объектов воздействия, то на первом месте, конечно же, стоит человек. В последнее время особую опасность представляет не только рост загрязнений, но и их суммарное влияние, часто превышающее по конечному эффекту простое суммирование последствий.

Загрязнение окружающей среды относится к непреднамеренным, хотя и очевидным, легко осознаваемым экологическим нарушениям. Они выступают на первый план не только потому, что многие из них значительны, но и потому, что они трудно контролируются и чреваты непредвиденными эффектами. Некоторые из них, например, техногенная эмиссия CO_2 или тепловое загрязнение, принципиально неизбежны, пока существует топливная энергетика.

Количественная оценка глобального загрязнения. Химизация техносферы достигла к настоящему времени таких масштабов, которые заметно влияют на геохимический облик всей экосферы. Общая масса производимых продуктов и химически активных отходов всей химической промышленности мира (вместе с сопутствующими производствами) превысила 1,5 Гт/год. Почти все это количество может быть отнесено к загрязнителям. Но дело не только в общей массе, но и в числе, разнообразии и токсичности множества производимых веществ. В мировой химической номенклатуре значится более 10^7 химических соединений; ежегодно их число

возрастает на несколько тысяч. Однако подавляющее большинство производимых и используемых веществ не оценены с точки зрения их токсичности и экологической опасности.

Источники техногенных эмиссии подразделяются на организованные и неорганизованные, стационарные и подвижные. Организованные источники оборудованы специальными устройствами для направленного вывода эмиссии (трубы, вентиляционные шахты, сбросные каналы и желоба и т.п.);

эмиссии от неорганизованных источников произвольны. Источники различаются также по геометрическим характеристикам (точечные, линейные, площадные) и по режиму работы - непрерывному, периодическому, залповому.

Выводы

Значительным техногенным опасностям подвергается человек при попадании в зону действуя технических систем: транспортные магистрали; зоны излучения радио и телепередающих систем, промышленные зоны и т. п. Уровни опасного воздействия на человека в этом случае определяются характеристиками технических систем и длительностью пребывания человека в опасной зоне. Вероятно проявление опасности и при использовании человеком технических устройств на производстве и в быту: электрические сети и приборы, станки, ручной инструмент, газовые баллоны и сети, оружие и т. п. Возникновение таких опасностей связано как с наличием неисправностей в технических устройствах, так и с неправильными действиями человека при их использовании.

ЗАКЛЮЧЕНИЕ

Проведен анализ изменения объемов и структуры трафика глобальной сети, показывающий тенденции экспоненциального роста, не стационарности и стихийный характер возникновения нагрузок.

Проведен анализ механизмов балансировки сетевого трафика. Показано, что применяемые решения являются недостаточными для обеспечения эффективного использования существующей сетевой инфраструктуры в указанных условиях.

Показано, что одной из основных проблем сетей связи является непредсказуемость возникающих нагрузок, приводящая к потерям трафика. Предложено применить децентрализованные самоорганизующиеся наложенные сети балансировки трафика, способные реагировать на изменения сетевых нагрузок в режиме, близком к реальному времени.

Изучена концепция децентрализованной самоорганизующейся наложенной балансировочной сети, позволяющей передавать агрегированный трафик, суммарная интенсивность которого превышает возможности передачи с помощью традиционной маршрутизации по кратчайшим путям. Определены базовые принципы организации наложенной балансировочной сети и соответствующие им процедуры.

Наложенный принцип построения является характерной чертой современных мультисервисных сетей. Проектирование подобных сетей более эффективно с применением модели в виде многослойного графа.

Использование в качестве модели источника информационного потока модели многоуровневого ON-OFF источника позволяет учесть взаимодействие элементов телекоммуникационной на различных уровнях модели ВОС. Приведены выражения позволяющие определить статистические характеристики информационного потока создаваемого пользователем на разных уровнях модели ВОС, а также характеристики потока создаваемого группой абонентов.

Предложены модель и метод управления трафиком с обеспечением гарантированного QoS на основе адаптивного выбора структуры ON и комплексного решения задач многопутевой маршрутизации и динамического распределения канальных ресурсов. Использование в методе оверлейных сетей ориентирует на повышение масштабируемости получаемых решений, т.к. решение задач многопутевой маршрутизации и распределения канальных ресурсов в итоге осуществляется на структуре значительно меньшей размерности.

Осуществлен анализ показателей эффективности, по которым оценивалось качество получаемых решений, связанных с обеспечением гарантированного качества обслуживания в мультисервисных ТКС, в рамках предложенного метода.

За счет применения алгоритмов выбора оверлейных сетей в рамках предложенного метода управления трафиком для обеспечения QoS удалось гарантировать заданные значения показателей качества обслуживания, но с существенным снижением (в три-пять раз) размерности положенной в основу данного метода оптимизационной задачи, что влечет за собой на практике пропорциональное снижение объемов циркулируемой служебной информации о загруженности каналов связи ТКС. При этом особенно ощутим выигрыш в применении разработанного метода для ТКС высокой

размерности (с количеством узлов 15-20) и высокой связностью узлов (3 и выше), что характерно при построении современных территориально-распределенных мультисервисных сетей.

Предлагаемый метод отвечает требованиям современных концепций управления сетевыми ресурсами, трафиком и маршрутизацией, например Active network, Traffic Engineering, MultiPath Routing, QoS-Based Routing и Constraint-Based Routing, расширяя область применения в условиях согласованной реализации динамических стратегий многопутевой маршрутизации и распределения канальных ресурсов ТКС.

СПИСОК ИСПОЛЬЗУЕМЫЕ ЛИТЕРАТУРЫ

1.Указ Президента Республики Узбекистан "О дальнейшем развитии компьютеризации и внедрении информационно-коммуникационных технологий", 2002г.

2.О государственной программе «Год благополучия и процветания». Постановление Президента Республики Узбекистан. Собрание законодательства Руз №8 ст.99, 2013г.

3. Tarkoma, S. Overlay Networks: Toward Information Networking. / S. Tarkoma. Auerbach Publications, 2010.

4. Lua, E.K. A survey and comparison of peer-to-peer overlay network schemes. / E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, S. Lim, others // IEEE Communications Surveys and Tutorials. – 2005. – Т. 7, № 1-4. – С. 72–93.

5. Wang, C. Peer-to-peer overlay networks: A survey / C. Wang, B. Li // Department of Computer Science, The Hong Kong University of Science and Technology. – 2003.

6. Cisco Visual Networking Index: Forecast and Methodology 2012-2017. Cisco Public, 2013

7. Zhi-Hui Lu, Ye Wang, and Yang Richard Yang. An Analysis and Comparison of CDN -P2P-hybrid Content Delivery System and Model //JCM. -2012 -7(3). -232-245.

8. Crowcroft J., Lua E., Pias M. A survey and Comparison of Peer-to-Peer Overlay Network Scemes. - ICST, 2004.

9. Zeidanloo H., Manaf A. Botnet Detection by Monitoring Simulation. Communication Patterns. -IJCSIS, 2010

10. Дорт-Гольц, А. А. Анализ протоколов наложенных пиринговых сетей // II МНТНПК «Актуальные проблемы инфотелекоммуникаций в науке и образовании». СПб.: СПбГУТ. – 2013. – С.113-118.

11. Shen, X. Handbook of peer-to-peer networking: Т. 1 / X. Shen, H. Yu, J. Buford, M. Akon. – Springer, 2010.

13. Яновский, Г.Г. Современные проблемы науки в области телекоммуникаций (Эволюция и конвергенция) / Г.Г. Яновский. – СПб: СПбГУТ им. МА Бонч- Бруевича, 2008.

14. Sørensen, L.T. User scenarios 2020: a worldwide wireless future / L.T. Sørensen, K.E. Skouby, D. Dietterle, A. Jhunjhunwala, X. Fu, X. Wang // WWRF Outlook. – 2009. – № 4.

15. Waldner, J.-B. Nanocomputers and swarm intelligence: Т. 12 / J.-B. Waldner. – John Wiley & Sons, 2010.

16. Кучерявый, А.Е. Интернет Вещей / А.Е. Кучерявый // Электросвязь. – 2013. – № 1.

17. Cisco visual networking index: Forecast and methodology, 2013-2018, Cisco systems, S. Jose, CA, Jun. 2014, www.cisco.com.

18. Шелухин, О.И. Фрактальные процессы в телекоммуникациях /. – М.: Радиотехника, 2003.

19. Albert, R. Statistical mechanics of complex networks / R. Albert, A.-L. Barabási // Reviews of modern physics. – 2002. – Т. 74, № 1. – С. 47.

20. Savage, S. The end-to-end effects of Internet path selection / S. Savage, A. Collins, E. Hoffman, J. Snell, T. Anderson: Т. 29. – ACM, 1999. – С. 289–299.

21. Hu, N. A measurement study of internet bottlenecks / N. Hu, L. Li, Z.M. Mao, P. Steenkiste, J. Wang: Т. 3IEEE, 2005. – С. 1689-1700.

Akella, A. An empirical evaluation of wide-area internet bottlenecks / A. Akella, S.

22. Seshan, A. Shaikh // Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement. – ACM, 2003. – С. 101–114.

23. Степанов, С.Н. Основы телетрафика мультисервисных сетей / С.Н. Степанов. – М.: Эко-трендз, 2010.
24. Семенов, Ю.В. Проектирование сетей связи следующего поколения / Ю.В. Семенов. – СПб.: Наука и техника, 2005.
25. Benson, T. Network traffic characteristics of data centers in the wild / T. Benson, A. Akella, D.A. Maltz. – ACM, 2010. – С. 267–280.
26. Haider.M. Designing of multichanel optical communication systems topologies criteria optimization. P.Dymora//Informatica - 2003, - Vol.1. -P.277-284.
27. Агеев Д.В. Моделирование современных телекоммуникационных систем многослойными графами. Проблемы телекоммуникаций-2010-№ 1(1)-С.23-24
28. Агеев Д.В. Параметрический синтез мультисервисных телекоммуникационных систем при передаче группового трафика с эффектом самоподобия Проблемы телекоммуникаций-2013-№1(10)-С.49-68.
29. Garcia A.E. Approximation to a Behavioral Model for Estimating Traffic Aggregation Scenarios. Journal of Universal Computer Science. -2008-Vol.14. Issue 5. -P.731-744.
30. Агеев Д.В. Метод проектирования телекоммуникационных систем с использованием потоковой модели для многослойного. Проблемы телекоммуникаций-2010-№2(2)-С.7-22.
31. Дорт-Гольц, А. А. Анализ протоколов наложенных пиринговых сетей // II МНТНПК «Актуальные проблемы инфотелекоммуникаций в науке и образовании». СПб.: СПбГУТ. – 2013. – С.113-118.
32. Gerber, A. Traffic types and growth in backbone networks / A. Gerber, R. Doverspike. – Optical Society of America, 2011.
33. Lin, D. Dynamics of random early detection / D. Lin, R. Morris // ACM SIGCOMM Computer Communication Review: Т. 27ACM, 1997. — С. 127–137.
34. Srinivasan, C. Multiprotocol label switching (MPLS) traffic engineering (TE) management information base (MIB) / C. Srinivasan, A. Viswanathan, T. Nadeau // Internet Engineering Task Force, RFC. – 2004. – Т. 3812.
35. Labovitz, C. Delayed Internet routing convergence / C. Labovitz, A. Ahuja, A.

Bose, F. Jahanian // ACM SIGCOMM Computer Communication Review. – 2000. – Т. 30, № 4. – С. 175–187.

36. МультисервисныеATM сети / Т.Б.Денисова, Б.Я.Лихтциндер, А.Н.Назаров и др. – М.: Эко-Трендз, 2005. –320 с.

37. Дробот О.А. Комплексная модель обеспечения гарантированного качества обслуживания с реализацией динамических стратегий распределения сетевых ресурсов // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2007. – № 148. – С.43–54.

38. Лемешко А.В., Дробот О.А. Модель многопутевой QoS-маршрутизации в мультисервисной телекоммуникационной сети // Радиотехника: Всеукр. межвед. науч.техн. сб. 2006. – Вып. 144. – С. 16–22.

39. Vutukury S., Garcia-Luna-Aceves J.J. MPATH: a loop-free multipath routing algorithm // Elsevier Journal of Microprocessors and Microsystems. – 2001. – № 24 (6). P. 319–327.

40. Jia Y., Nikoladis I., Gburzynski P. Multiple path QoS routing // Proc. Int. Conf. Communications (ICC 2001). – Helsinki, 2001. – P. 2583–2587.

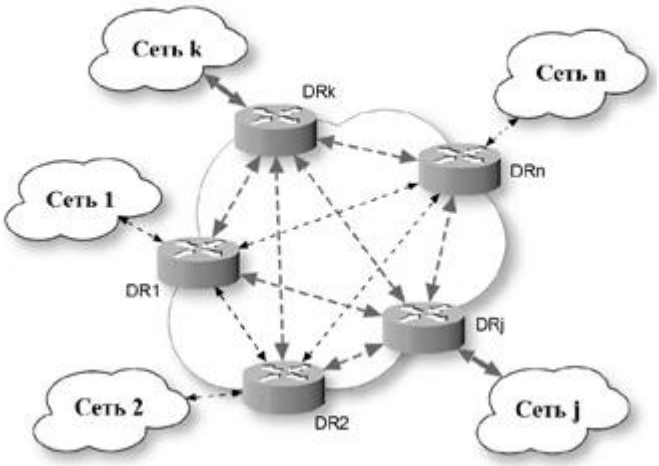
41.Экология и безопасность жизнедеятельности: Учебное пособие для студентов ВУЗов/ ред. Л. А. Муравий, 2002.

42. Белов С.В. Безопасность жизнедеятельности М.: Высшая школа. 2003.

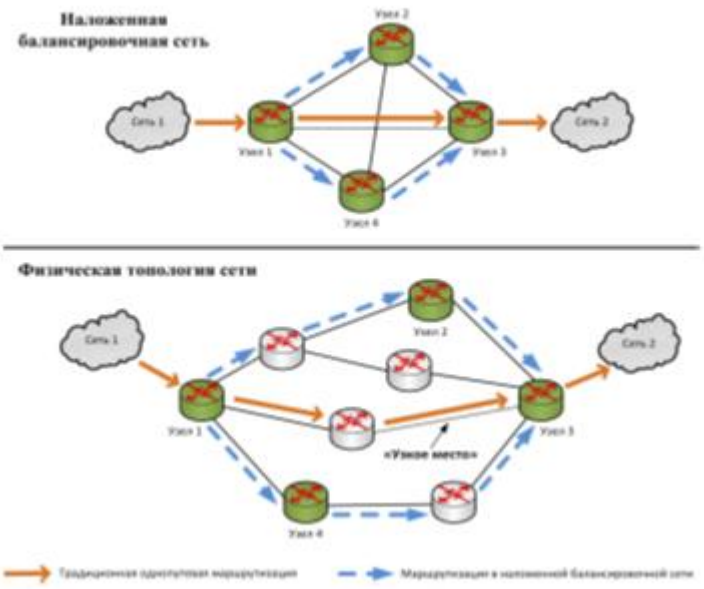
ПРИЛОЖЕНИЕ

Приведены слайд презентации

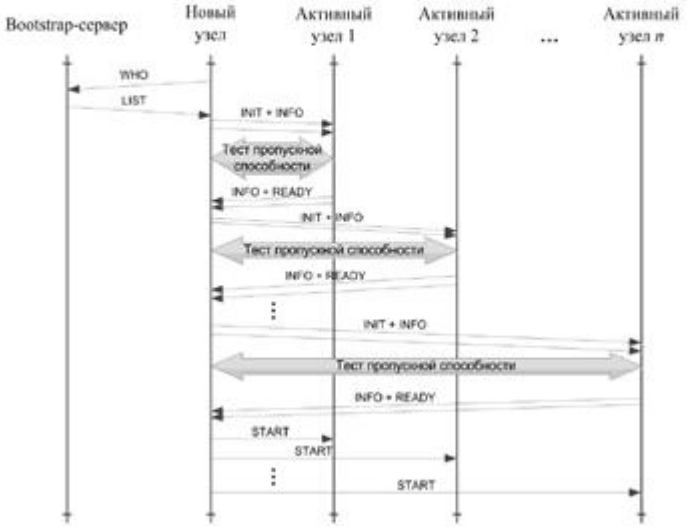
Модель наложенной балансировочной сети



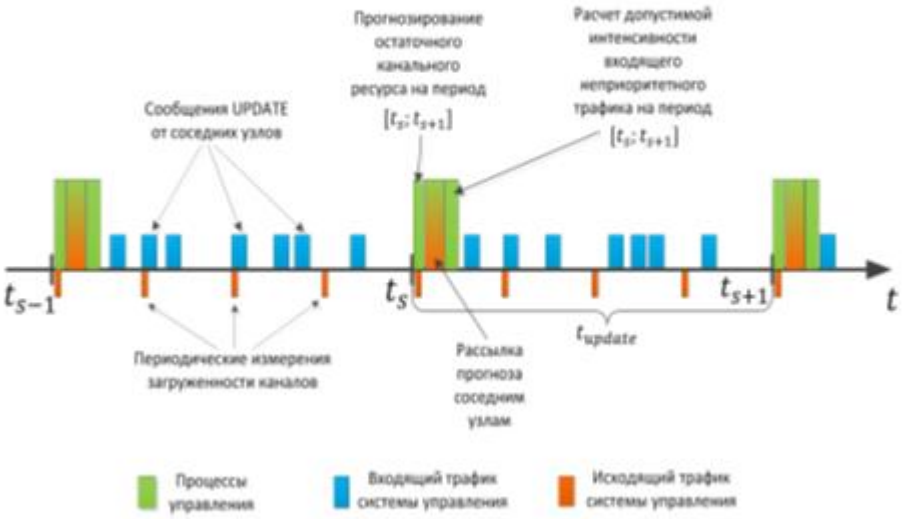
Распределение нагрузки наложенной балансировочной сетью в случае недостаточной пропускной способности оптимального пути



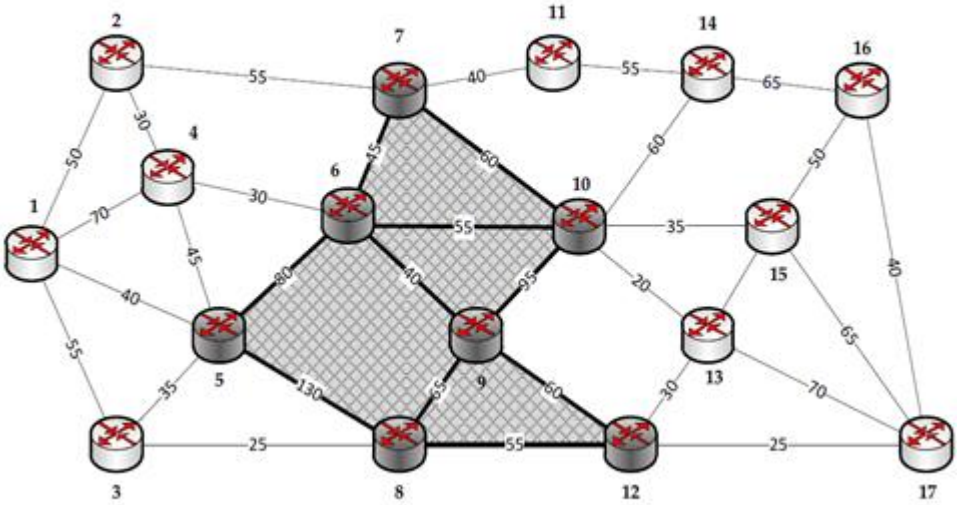
Подключение нового узла к существующей наложенной балансировочной сети



Временная диаграмма работы узла наложенной балансировочной сети



Структура ТКС и граф решений задачи управления трафиком интенсивности 200 Мбит/с



Результаты анализа качества работы алгоритмов выбора структуры наложенных сетей