Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Телекоммуникационные системы»
Специальность 6М071900 «Радиотехника, электроника и телекоммуникации»

ДОПУЩЕН К ЗАЩИТЕ
Зав. кафедрой
к.т.н., Шагиахметов Д.Р.
(ученая степень, звание, ФИО) (подпись)
«____»_____2014 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: «Анализ сравнения эффективности методов взаимодействия ОКС-7 и SIP»

Магистрант Айтбай Тимур _____ группа ИТСп-12-1
(Ф.И.О.) (подпись)
Руководитель к.т.н., доцент каф.ТКС _____ Жунусов К.Х.
(ученая степень, звание) (подпись) (Ф.И.О.)

Технический консультант _____ _____
(подпись) (Ф.И.О.)
Рецензент_____ _____ _____
(ученая степень, звание) (подпись) (Ф.И.О.)

Консультант по ВТ к.х.н., ст.преп. _____ Данько Е.Т.
(ученая степень, звание) (подпись) (Ф.И.О.)

Нормоконтроль ст.преп. _____ Абрамкина О. А.
(ученая степень, звание) (подпись) (Ф.И.О.)

Алматы, 2014

Некоммеческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Радиотехники, электроники и связи»_____
Специальность 6М071900 «Радиотехники, электроники и телекоммуникации»
Кафедра «Телекоммуникационных систем»_____

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистранту__Айтбай Тимур_____
(фамилия, имя, отчество)

Тема диссертации: «Анализ сравнения эффективноси методов взаимодействия ОКС-7 и SIP»
утверждена Ученым советом университета №142_от «_31»_октября 2013 г.___
Срок сдачи законченной диссертации «___»_____
Цель исследования состоит в анализе сравнения методов взаимодействия общеканальной сигнализации №7 и протокола установления соединения.
_____
_____
_____
_____

Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
1 Общеканальная система сигнализации №7_____
2 Протокол инициирования сеансов связи – SIP__
3 Особенности взаимодействия SIP с протоколами управления СТОП_____
4 Экспериментальное исследование методов взаимодействия _____ _5.
5 Расчет сигнального трафика протокола SIP_____

Перечень графического материала (с точным указанием обязательных чертежей)_____
Рисунок 1.2 - Взаимодействие цифровых сетей по ОКС-7_____
Рисунок 1.7 - Структура сети ОКС-7_____
Рисунок 2.4 - Структурная схема организации услуг SIP-сервера_____
Рисунок 2.5- Структура сообщений протокола SIP_____

Рекомендуемая основная литератур:
1 Гольдштейн Б.С., Сигнализации в сетях связи. М.: Радио и связь, 1997.
2 Гольдштейн Б.С., Протокол SIP. Справочник. – СПб.: БХВ – Санкт-Петербург, 2005.
2 Росляков А.В., Сети и системы связи, 2002.

Г Р А Ф И К
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1 Информационный обзор методов взаимодействия ОКС-7 и SIP	05.10.2012	
2 Основные виды технологий абонентских линий	02.02.2013	
3 Анализ основных принципов методов взаимодействия	10.03.2013	
4 Анализ работы методов взаимодействия	05.09.2013	
5 Расчет сигнального трафика протокола SIP	18.10.2013	
6 Подготовка к проведению эксперимента	10.12.2013	

Дата выдачи задания_____

Заведующий кафедрой_____(__Шагиахметов Д.Р.___)
(подпись) (Ф.И.О.)

Руководитель диссертации_____(___Жунусов К.Х.____)
(подпись) (Ф.И.О.)

Задание принял к исполнению
магистрант _____(___Айтбай Т.М.__)
(подпись) (Ф.И.О.)

Аңдатпа

Бұл диссертациялық жұмыста ОКС-7 және SIP әрекеттестігінің әдістері зерттеледі.

Бірінші бөлімде сигнализация жүйелердің жалпы дамуы келтіріледі.

Екінші бөлімде негізгі мақсаттары мен алгоритм қарастырылады.

Үшінші бөлімде әрекеттестіктің әдістері қарастырылады.

Төртінші бөлімде әрекеттестік әдістердің эксперементтік зерттеу өткізіледі.

Бесінші бөлімде SIP протоклының сигналдық трафигінің есебі өткізіледі

Аннотация

В данной диссертационной работе исследуются методы взаимодействия ОКС-7 и SIP.

В первой главе приводится общий обзор систем сигнализации.

Во второй главе рассматриваются основные принципы и алгоритмы протокола SIP.

В третьей главе рассматриваются методы взаимодействия.

В четвертой главе проводится экспериментальное исследование методов взаимодействия.

В пятой главе проводится расчет сигнального трафика протокола SIP.

Содержание

Введение

Для взаимодействия с традиционными телефонными сетями, использующими сигнализацию ОКС-7, была разработана модификация протокола SIP для телефонии – Протокол инициализации сеанса для телефонии (англ. Session Initiation Protocol for Telephones (SIP-T)[1]. Основная задача разработанной модификации протокола SIP заключается в «прозрачности» (понятности) при передаче сообщений ISUP по IP-сети. Данная задача осуществляется при инкапсуляции сигнальных единиц ОКС-7 в сообщения SIP. Сообщение ISUP содержит информацию, которую невозможно отобразить в заголовках. Поэтому информация отображается в SIP лишь частично или отбрасывается, что является недостатком данного метода.

В работе производится исследование инкапсуляции, метода взаимодействия протоколов сигнализации и установления соединения для сетей IP-телефонии. При построении алгоритма работы переадресации собрана информация, которая касается протокола SIP-T, его основных и дополнительных функций в соответствии с документами RFC комитета IETF[2]. Раскрываются функциональные возможности элементов, которые взаимодействуют по данному протоколу, также исследуются процедуры управления соединением. Приводятся примеры сценариев обмена сообщениями и их недостатки, такие как: некорректность перевода сообщения ISUP в SIP, в результате чего может произойти ошибка при установлении соединения.

В исследуемом сценарии начальной точкой является пользователь сети телекоммуникаций общего пользования, а конечной – пользователь сети SIP. Приводятся схемы организации взаимодействия для каждого сценария.

Требования к сети IP-телефонии необходимы для возможности «прозрачности» команд для организации услуг относительно сети телекоммуникаций общего пользования. Традиционные телефонные услуги и дополнительные виды обслуживания должны иметь возможность реализации с помощью системы сигнализации №7.

1 Общеканальная система сигнализации №7

Общеканальная система сигнализации №7 - это универсальная многофункциональная система межстанционной сигнализации, ориентированная на поддержку практически всех уже известных, а также будущих услуг связи. Ее огромный потенциал объясняется блочной функциональной архитектурой, где над единой транспортной подсистемой (MTP) расположены подсистемы пользователей и приложений (TUP, ISUP, MAP, TCAP, MUP и т. д.), предназначенные для обеспечения соответствующих услуг связи. Экономический эффект от внедрения ОКС-7 (общеканальной сигнализации) проявляется даже при обычной телефонной связи[3].

На протяжении последних ста лет сигнализация развивалась в рамках традиционной телефонии, причем за последние два десятилетия ее эволюция ускорилась как никогда ранее благодаря сращиванию компьютерных и коммутационных технологий. В контексте телефонии под сигнализацией понимается передача управляющей информации с целью установления/разъединения двухточечных соединений. Сигнализация бывает трех типов - абонентская, т.е. на участке между абонентским терминалом и коммутационной станцией, внутристанционная и межстанционная. Пример абонентской сигнализации приведен на рисунке 1.1, где показаны основные сигналы, передаваемые в процессе нормального установления/разъединения соединения между двумя абонентами, подключенными к одной коммутационной станции.

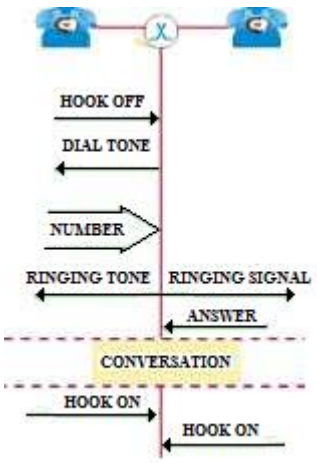

Рисунок 1.1 – Пример абонентской сигнализации

Межстанционная сигнализация в свою очередь делится на два основных типа - сигнализация по выделенному каналу CAS (Channel Associated Signalling) и сигнализация по общему каналу CCS (Common Channel Signalling). В системе использован принцип передачи управляющей информации по общему каналу сигнализации, отсюда ее сокращенное название по-русски – ОКС-7. В первом случае (CAS) сигнальная информация передается либо

непосредственно по разговорному каналу (внутриканальная сигнализация) либо по каналу, физически привязанному к нему. Во втором случае (CCS) сигнализация полностью отделена от разговорного тракта, и передача сигнальной информации осуществляется по специально выделенному высокоскоростному каналу, общему для пучка разговорных каналов[4].

На сегодняшний день известны два стандарта систем общеканальной сигнализации:

– CCITT Signalling System No. 6;

– CCITT Signalling System No. 7.

Первая из них была разработана в конце 60-х годов и по ряду причин сейчас практически не применяется. Вторая - CCITT No. 7 (SS-7) появилась в конце 70-х годов и предназначена для использования на цифровых сетях с каналами не ниже 64 Кбит/с. Основными преимуществами ОКС-7 являются:

– скорость - в большинстве случаев время установления соединения не превышает одной секунды;

– высокая производительность - один канал сигнализации способен одновременно обслужить несколько тысяч телефонных вызовов;

– кономичность - по сравнению с системами cas во много раз сокращается объем оборудования на коммутационной станции;

– надежность - достигается за счет возможности альтернативной маршрутизации в сети сигнализации;

– гибкость - система передает любые данные, не только данные телефонии.

Популярные словосочетания и аббревиатуры, такие как ISDN, сети подвижной связи, интеллектуальные сети, в действительности, остаются лишь словами на бумаге без системы сигнализации № 7 (ОКС-7) - единственного средства, обеспечивающего внедрение и функционирование современных услуг связи на сетевом уровне. Многие производители оборудования ISDN утверждают, будто их продукты обеспечивают "услуги ISDN". Однако область действия услуг, предоставляемых любым терминальным оборудованием ISDN или офисными АТС класса ISDN, ограничена пределами одной коммутационной системы, и не распространяется на абонентов других станций. Развитие сетей подвижной связи также невозможно без ОКС-7. Порой конкурирующих между собой поставщиков услуг сотовой связи объединяет лишь ОКС-7, необходимая для обеспечения автоматического обмена информацией о местонахождении абонента (роуминга). Наконец, для эффективного функционирования интеллектуальных сетей также требуется ОКС-7. Будучи разработанной для традиционной телефонии, в ОКС-7 изначально были заложены большие возможности для управления другими услугами связи. Это объясняется прежде всего бумом на рынке услуг телекоммуникаций, который продолжается с начала 80-х годов и еще не достиг своего пика. Именно в 80-х годах ОКС-7 интенсивно разрабатывалась ведущими производителями коммутационного оборудования и параллельно

утверждалось в качестве стандарта CCITT[5]. Уже сейчас ОКС-7 является обязательным элементом следующих цифровых сетей связи:

– PSTN - Public Switched Telephone Network;
– ISDN - Integrated Services Digital Network;
– PLMN - Public Land Mobile Network;
– IN - Intelligent Network.

Взаимодействие данных систем также осуществляется посредством SS №7 (см. рисунок 1.2).

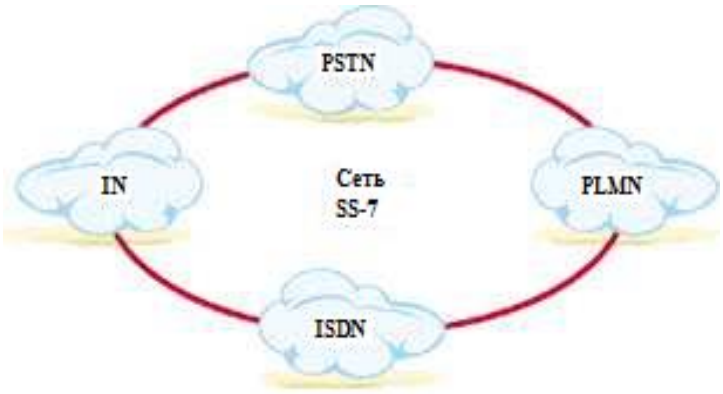

Рисунок 1.2 – Взаимодействие цифровых сетей по ОКС-7

В настоящее время практически всеми международными институтами стандартизации телекоммуникаций (ITU-T, ETSI, ANSI, ATM Forum и др.) разрабатываются стандарты SS-7 для широкополосных сетей - Broadband-ISDN, Universal Mobile Telecommunications System, Broadband-IN.

1.1 Основные понятия и элементы ОКС-7

В процессе развития сетей связи применялся и применяется до сих пор ряд систем сигнализации, причем большинство из них принято в качестве стандарта на международном уровне ITU-T (ранее CCITT). Примеры систем сигнализации CAS:

1VF (One Voice Friequency) - одночастотная сигнализация;

2VF (Two Voice Friequency) - двухчастотная сигнализация (CCITT No. 4);

MVF (Multi Friequency Pulse) - многочастотная сигнализация (CCITT No. 5).

Сами названия этих систем говорят о способе передачи сигнальной информации - тональные и/или импульсные сигналы. В системах CCS все сигнальные сообщения SM (Signalling Message) передаются по дуплексным каналам - звеньям сигнализации SL (Signalling Link) в составе пакетов данных, называемых сигнальными единицами SE (Signal Unit). Это стало возможным после появления первых коммутационных станций с программным управлением SPC (Stored Programm Control) и цифровых систем передачи с

импульсно-кодовой модуляциейPCM (Pulse-Code Modulation). Часть функций таких станций вместе с пучками звеньев сигнализации SLS (Signalling Link Set) образуют логически отделенную от базовой сети связи сеть передачи данных с коммутацией пакетов данных (сигнальных единиц), называемую сетью сигнализации SN (Signalling Network).

Пункт сигнализации - SP (Signalling Point) - это узел сети сигнализации, в котором реализованы части пользователей ОКС-7. Звено сигнализации - SL (Signalling Link) - средство передачи сигнальных единиц между двумя пунктами сигнализации. Транзитный пункт сигнализации - STP (Signalling Transfer Point) - узел сети сигнализации без функций частей пользователей, осуществляющий только функции части передачи сообщений ОКС-7[6]. Режимы сети сигнализации - связанный режим (Associated Mode) и квази-связанный режим (Quasi-Associated Mode) - пояснены на рисунке 1.3.

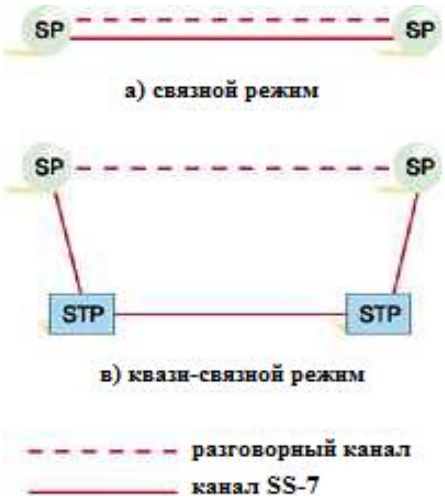

Рисунок 1.3 – Режимы сети сигнализации

Часть передачи сообщений - MTP (Message Transfer Part) является транспортной подсистемой ОКС-7, предназначенной для надежной передачи сигнальных сообщений в правильной последовательности и без ошибок. Части пользователей - UP (User Parts) функциональные блоки ОКС-7, где генерируются и обрабатываются сигнальные сообщения. Примерами частей пользователей являются:

– TUP - Telephone User Part;

– ISUP - ISDN User Part;

– MAP - Mobile Application Part.

– Базовая функциональная схема ОКС-7 приведена на рисунке 1.4. На рисунке 1.5 представлен пример обмена сигнальными сообщениями между двумя пунктами сигнализации в процессе установления/разъединения телефонного соединения:

– IAM (Initial Address Message) - содержит номерную информацию о вызываемом абоненте;

– SAM (Subsequent Address Message) - содержит дополнительную информацию, передается в случае необходимости;

– ACM (Address Complete Message) - содержит информацию о статусе вызываемого абонента (например, абонент свободен);

– ANC (Answer Charge) - определяет момент начала начисления оплаты;

– CLF (Clear Forward) - сообщение в прямом направлении о завершении вызова;

– RLG (Release Guard) - подтверждение завершения вызова в обратном направлении, разъединение соединения.

Рисунок 1.4 – Базовая функциональная схема ОКС-7

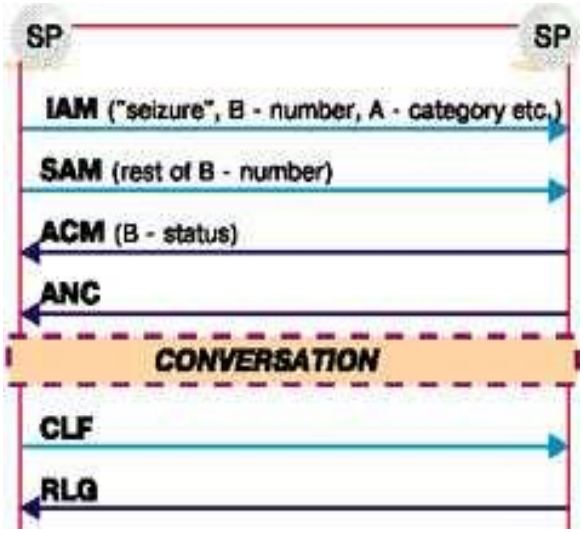

Рисунок 1.5 – Временная диаграмма установления/разъединения телефонного соединения по ОКС-7

1.1.1 Развитие телефонных сетей общего пользования

В настоящее время развитие телефонных сетей общего пользования (СТОП) связано с повсеместным внедрением системы сигнализации № 7. Сегодня, когда этот процесс становится поистине полномасштабным, вопросы тестирования ОКС-7 особенно актуальны. Процессы построения сетей ОКС-7 и передачи данных во многом схожи. В связи с этим можно утверждать, что все измерения в сетях ОКС-7 сводятся к анализу специализированного протокола передачи данных. Действительно, для внедрения технологии ОКС-7 требуется наличие сети передачи данных специального назначения - сети сигнализации.

Поэтому измерения по такой специализированной сети сводятся к логическому анализу протокола ОКС7. Измерения на физическом и канальном уровнях (в цифровых каналах и интерфейсах) не актуальны, поскольку в сетях ОКС-7 в качестве транспортной среды используются каналы вторичных сетей СТОП и ISDN. Тестировать протокол ОКС-7 на полное соответствие техническим требования следует в двух случаях: при пуске новой цифровой АТС или цифровой зоны и при вводе нового канала сигнализации.

1.2 Структура сети сигнализации

Сеть сигнализации, как и сети пакетной коммутации других типов, строится согласно следующим основным критериям:

- простота структуры сети;
- надежность;
- минимальные временные задержки;
- оптимальная стоимость.

Этим критериям лучше всего будет соответствовать сеть с достаточно симметричной топологией и функционирующая в квази-связанном режиме. Многие национальные сети ОКС-7 строятся по региональному принципу с иерархической системой транзитных пунктов сигнализации.

В рамках СТОП для ОКС-7 создается выделенная сеть сигнализации. В ней объединены несколько типовых устройств центров сигнализации), а для обмена сообщениями используются канальные интервалы сигнализации потоков E1 (TS16). Такая сеть (рисунок 1.6) включает в себя пункты передачи сигнальных сообщений (Signalling Transfer Point - STP), абонентские пункты сигнализации (Service Switching Point - SSP) и пункты предоставления дополнительных услуг (Service Control Point - SCP). С помощью STP в сети ОКС-7 выполняется маршрутизация пакетов сигнальных сообщений. SSP отводится роль терминалов сетей передачи данных, а SCP, адаптированные в соответствии с концепцией интеллектуальных сетей, работают эквивалентно хостам и коллективным базам данных этих сетей[7].

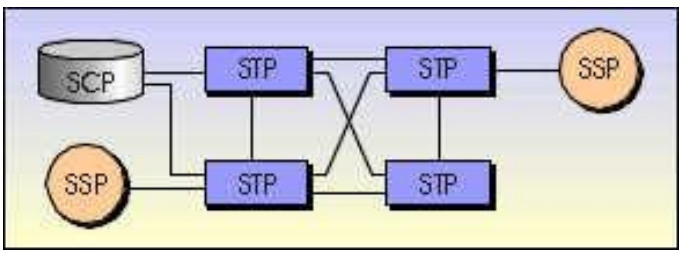

Рисунок 1.6 – Структура сети ОКС-7

1.2.1 Формат сигнальных сообщений

Формат сигнальных сообщений - сигнальная единица, в составе которой передаются сигнальные сообщения, называется значащей сигнальной

единицей MSU (Message Signal Unit) и включает ряд полей, показанных на рисунке 1.7.

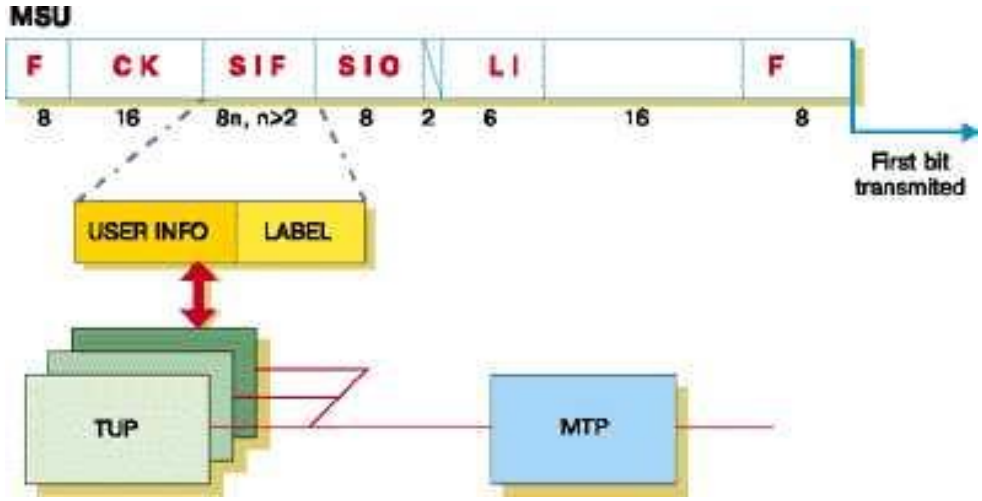

Рисунок 1.7 – Формат значащей сигнальной единицы

Формат сигнальных единиц состоит:

1. Signalling Information Field (SIF) - включает сигнальную информацию части пользователя и метку маршрутизации, которая применяется в части передачи сообщений MTP;
2. Service Information Octet (SIO) - указывет на принадлежность сигнальной информации конкретной части пользователя;
3. Length Indicator (LI) - содержит значение числа байт между полями LI и CK;
4. Check bits (CK) - проверочные биты для обнаружения ошибок передачи;
5. Error correction- состоит из четырех полей аналогичных используемым в протоколе HDLC и предназначенных для обеспечения повторных передач пакетов при обнаружении ошибок;
6. Flag (F) - обозначает начало и конец сигнальной единицы.

1.2.2 Структура протокола ОКС-7

Структура протокола ОКС-7 сложнее структуры большинства протоколов сетей передачи данных и включает в себя множество уровней и подсистем. Это связано с тем, что протокол ОКС-7 является средством для объединения различных сетей: СТОП, ISDN, подвижной радиосвязи, а также предоставляет дополнительные возможности для создания глобальных сетей персональной связи (PCS) с международным роумингом. Наличие в структуре сети ОКС-7 пунктов SCP способствует широкому внедрению интеллектуальных сетей, внося дополнительные уточнения и расширения в структуру протокола ОКС-7. Существуют рекомендации МСЭ-Т, касающиеся данной структуры и методик тестирования ее параметров. Сами рекомендации - это довольно объемные по

содержанию документы. Так, например, в рекомендацию Q.784 по тестированию функции подсистемы ISUP включены 75 тестов и на описание каждого из них отведена отдельная страница. Первая спецификация ОКС-7 была опубликована CCITT в 1980 году в рекомендациях серии Q.700 (Желтая книга). Тогда же ISO представила эталонную модель взаимодействия открытых систем (модель OSI)[8]. Соответствие архитектуры протоколов модели OSI и современного стека протоколов ОКС-7 показано на рисунке 1.8.

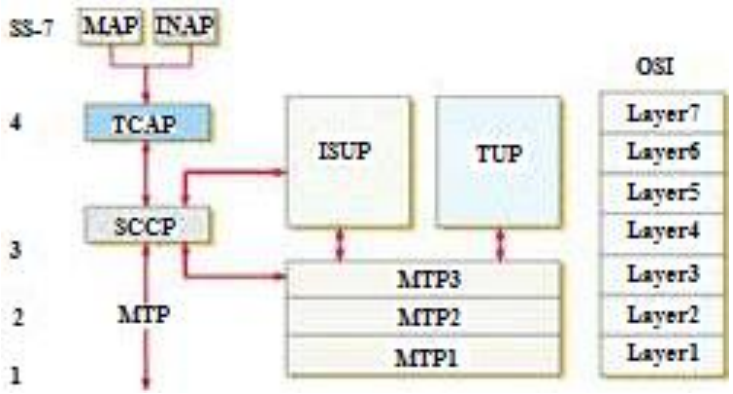

Рисунок 1.8 – Протоколы ОКС-7 и модель OSI

Архитектура протоколов ОКС-7 отражает историю ее создания. До 1984 года, когда в Красной книге CCITT была начата спецификация части транзакционных возможностей ОКС-7, стек протоколов был совместим с моделью OSI только до третьего уровня, и то не полностью. Совместимость была достигнута дополнением системы протоколами SCCP (Signalling Connection Control Part) и TCAP (Transaction Capabilities Application Part), что позволило реализовывать в ОКС-7 услуги передачи данных по тем же принципам, что и в модели OSI. На базе транзакционной части ОКС-7 позднее были специфицированы протоколы MAP (Mobile Application Part)и INAP (Intelligent Network Application Protocol), для которых существенным является обмен транзакциями между узлами сети и сетевыми базами данных.

1.3 Принципы построения сети ОКС-7

1.3.1 Компоненты сети сигнализации

Сеть связи, обслуживаемая ОКС, состоит из узлов коммутации и обработки, соединенных звеньями передачи. В контексте сигнализации узлы сети связи, использующие ОКС, рассматриваются как пункты сигнализации (Signalling Point - SP). Два пункта сигнализации, для которых существует возможность связи, т.е. которые соединены пучком разговорных каналов, называются пунктами, имеющими сигнальное отношение (Signalling Relation). А два пункта сигнализации непосредственно соединенные пучком звеньев сигнализации (сигнальных линков), называются смежными пунктами сигнализации (Adjacent SP).

1.3.2 Режимы сигнализации

Режим сигнализации - это связь между путем, по которому проходит сигнальное сообщение в сети сигнализации, и сигнальным отношением, к которому относится это сообщение.

Возможны следующие режимы сигнализации:

– связанный режим (Associated Mode) - режим, при котором сообщение, относящееся к данному сигнальному отношению между двумя SP, передается непосредственно по пучку звеньев, соединяющий эти SP. При этом режиме путь сигнального сообщения 'совпадает' с сигнальным отношением.

– несвязанный режим - режим, при котором путь сигнального сообщения не 'совпадает' с сигнальным отношением между отправителем и получателем данного сообщения, причем путь этот заранее не определен.

– квазасвязанный режим - частный случай несвязанного режима, когда путь сигнального сообщения заранее определен.

– ОКС №7 предназначен для использования при связанном и квазисвязанном режимах. Подсистема пользователя не имеет средств, позволяющих избежать нарушения последовательности поступления сообщений, которое возможно при полностью несвязанном режиме с динамической маршрутизацией сообщений.

1.3.3 Международные и национальные сети сигнализации

Международные и национальные сети сигнализации рассматриваются как независимые с точки зрения их структуры. Хотя отдельный пункт сигнализации может принадлежать и к национальной и к международной сети, коды пунктам сигнализации присваиваются в соответствии с правилами, определенными для каждой из этих сетей. Простейшая сеть сигнализации состоит из исходящего пункта и пункта назначения сигнализации, соединенных одним звеном сигнализации (связанный режим). По техническим и экономическим соображениям простая связанная сеть может быть неприемлемой. Тогда используется сеть, работающая в квазисвязанном режиме, в которой информация между исходящим пунктом и пунктом назначения может быть передана через несколько транзитных пунктов сигнализации (Signalling Transfer Point - STP)[9].

С функциональной точки зрения всемирная сеть сигнализации имеет структуру, состоящую из двух независимых уровней: международного уровня и национальных уровней.

Пункт сигнализации SP, включая транзитный пункт сигнализации STP, может входить в одну из трех категории:

– национальный пункт сигнализации (NSP), относящийся лишь к национальной сети и идентифицируемый кодом исходящего пункта (OPC) или пункта назначения (DPC) в соответствии с национальным планом нумерации пунктов сигнализации;

– международный пункт сигнализации (ISP), относящийся только к международной сети и идентифицируемый OPC и DPC в соответствии с международным планом нумерации пунктов сигнализации;

– узел, одновременно работающий как ISP и NSP (шлюз), который относится и к национальной сети и к международной сети. В каждой из сетей он идентифицируется своим OPC и DPC.

Для отличия международных кодов пунктов сигнализации от национальных используется индикатор сети. Для идентификации пунктов сигнализации используется код из 14-ти битов.

1.3.4 Структура системы ОКС-7

Система ОКС-7 может использоваться с различными структурами сети сигнализации. На выбор структуры сети сигнализации могут влиять следующие факторы:

– структура сети электросвязи, которая должна обслуживаться системой сигнализации;

– административные аспекты.

Если система сигнализации будет только на основе сигнальных отношений, то сеть будет основана главным образом на связанном режиме сигнализации и в малой степени на квазисвязанном режиме для сигнальных отношений с малой нагрузкой. В этом случае структура сети в основном определяется схемами сигнальных отношений. Примером такой реализации может международная сеть ОКС-7.

Другое решение - сеть сигнализации рассматривается как общее средство для передачи разнообразной информации по ОКС-7. В этом случае используется большая емкость звеньев сигнализации в сочетании с избыточностью, необходимой для обеспечения надежности. В такой сети в большей степени используются квазисвязанный и связанный режимы в сигнальных отношениях с большой нагрузкой.

Определяющим фактором для сети сигнализации является надежность, которая обеспечивается избыточностью. Необходимая избыточность может быть обеспечена сочетанием следующих видов избыточности:

– звеньев передачи данных сигнализации (например, специально выделенными резервными звеньями или коммутируемыми соединениями);

– оборудования оконечных устройств сигнализации (например, общей группой ОУ в оборудовании пункта сигнализации);

– звеньев сигнализации внутри пучка звеньев (работающих обычно с разделением нагрузки);

– маршрутов сигнализации для каждого пункта назначения (способных в случае необходимости работать с разделением нагрузки).

Ячеистая структура сети - это типовая структура, работающая в квазисвязанном режиме. На ее основе могут быть построены любые сети.

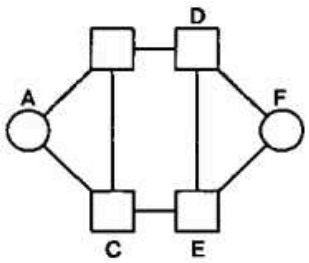

Рисунок 1.9 – Ячеистая структура сети

В ячеистой структуре каждый из пунктов сигнализации SP связан с двумя STP посредством двух пучков звеньев. Каждая пара STP соединена с другой парой четырьмя пучками звеньев сигнализации. Кроме того, между двумя STP каждой из пар имеется пучок звеньев сигнализации.

Развитые сети ОКС-7 включают в себя совокупность SP и связывающую их сеть транзитных SP, т.е. являются не иерархическими. В свою очередь, сеть транзитных пунктов сигнализации может иметь несколько уровней иерархии.

Транзитная сеть сигнализации с одним уровнем иерархии является более предпочтительной из-за максимальной простоты, минимальных временных задержек передачи сигнальных сообщений, эффективности стоимостных показателей. Однако в больших сетях с целью достижения большей надежности и доступности сети может быть построен второй уровень иерархии транзитных пунктов сигнализации.

1.3.5 Функции управления сетью

К функциям управления сетью внутри протокола ОКС-7 относятся функции подсистем MTP и SCCP по поддержанию качественных характеристик сети ОКС-7 с помощью автоматических процедур. Автоматические процедуры подсистемы MTP обеспечивают реконфигурации сети сигнализации в случае отказов и управление сигнальным трафиком при перегрузке. Функции управления сетью сигнализации подсистемы MTP включают управление сигнальным трафиком, звеньями сигнализации и маршрутом сигнализации. Эти функции используются всякий раз, когда в сети сигнализации имеет место такое событие, как отказ или восстановление ЗС (пучка ЗС)[10]. Функция управления сигнальным трафиком используется для перенаправления сигнального трафика с одного звена (маршрута) на другое звено (маршрут) или нескольких других звеньев (маршрутов), а также для временного снижения сигнального трафика в случае перегрузки в пункте сигнализации. Она включает следующие процедуры:

- переход на резервное звено сигнализации;
- возврат на исходное звено сигнализации;
- вынужденное ремаршрутизирование;
- управляемое ремаршрутизирование;
- перезапуск (рестарт) MTP;
- запрещение управлением;

– управление потоком сигнального трафика.

Функция управления звеньями сигнализации используется для восстановления отказавших ЗС, для активации (включение в работу) свободных ЗС (еще не сфазированных) и деактивации (выключение из работы) проверяемых ЗС. Она включает следующие процедуры:

– активации;
– восстановления;
– деактивации звена сигнализации;
– активации звена пучка ЗС.

Функция управления маршрутами сигнализации используется для распределения информации о состоянии сети сигнализации, для блокировки или разблокировки маршрутов сигнализации. Она содержит следующие процедуры:

– управление;
– запрещение передачи;
– разрешение передачи;
– ограничение передачи;
– тестирование пучка маршрутов сигнализации;
– тестирование перегрузки пучка маршрутов сигнализации.

Функции по управлению сетью сигнализации подсистемы SCCP включают управление стоянием пункта сигнализации и управление состоянием подсистемы.

Функция управления состоянием пункта сигнализации используется для выполнения маршрутизации с обходами на резервные пункты сигнализации и/или на резервные подсистемы. Процедуры, реализующие эту функцию:

– ПС запрещен;
– ПС разрешен;
– ПС перегружен.

Функция управления состоянием подсистемы используется для идентификации подсистем, испытаний их, маршрутизации на резервные подсистемы, информации местных пользователей о состоянии их резервных подсистем. Процедуры, реализующие эту функцию:

– подсистема запрещена;
– подсистема разрешена;
– испытания состояния подсистемы;
– координированное изменение состояния;
– местное циркулярное оповещение;
– циркулярная передача.

1.3.6 Функция управления сигнальным трафиком

Функция управления сигнальным трафиком в сети используется для переноса сигнального трафика в звеньях или маршрутах сигнализации, либо для временного сокращения его объема в случае перегрузки.

К основным процедурам управления сигнальным трафиком относятся:

– недоступность звена сигнализации (отказ, выключение из работы, блокировка или запрет) - для переноса сигнального трафика на одно или более резервных ЗС (если есть) используется процедура перехода на резерв;

– доступность звена сигнализации (восстановление, включение в работу, разблокировка или разрешение) - восстановление исходного состояния для переноса сигнального трафика на ЗС, ставшее доступным;

– недоступность маршрута звена сигнализации - вынужденное ремаршрутизирование для переноса трафика на резервный маршрут;

– доступность звена сигнализации - ремаршрутизирование для переноса сигнального трафика на маршрут, ставший доступным;

– ограничение маршрута сигнализации - управляемое ремаршрутизирование для переноса трафика на резервный маршрут.

1.3.7 Процедура перехода на резерв должна обеспечивать перенос трафика, передаваемого недоступным ЗС, на одно или несколько резервных ЗС как можно быстрее, избегая потери, дублирования или неправильного порядка следования сообщений. С этой целью в случае нормальной работы процедура перехода на резерв содержит сохранение значащих сигнальных единиц (ЗСЕ) в буферной памяти и их восстановление, которое производится перед повторным запуском резервных ЗС для перенесенного трафика. Резервные звенья могут передавать свой собственный трафик, который не прерывается процедурой перехода на резерв[11]. Сигнальный трафик, переносимый из недоступного звена сигнализации, маршрутизируется соответствующим образом.

Возможны два варианта перенесения трафика:

– на одно или несколько ЗС одного и того же типа;

– на один или несколько различных пучков звеньев.

Вследствие этого можно определить для каждого конкретного трафика три различных соотношения между новым звеном сигнализации и недоступным звеном:

– новое звено сигнализации параллельно недоступному;

– новое ЗС не принадлежит маршруту, к которому относится недоступное звено, однако этот маршрут еще проходит через пункт сигнализации на удаленном комплекте недоступного ЗС (см. рисунок 1.11);

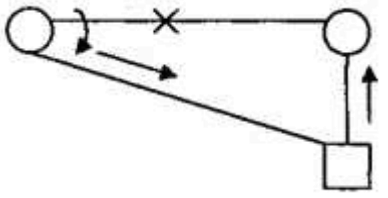

Рисунок 1.10 – Маршрут через пункт сигнализации на удаленном комплекте недоступного ЗС

– новое ЗС не входит в состав маршрута с недоступным звеном и этот сигнальный маршрут не проходит через пункт сигнализации, служащий транзитным пунктом и находящийся на удаленном комплекте недоступного звена. Только в этом случае возможно нарушение последовательности поступления сообщений (см. рисунок 1.12).

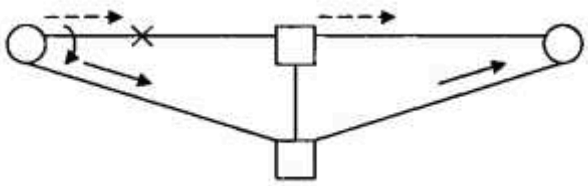

Рисунок 1.11 – Новое СЗ не входящий в состав маршрута с недоступным звеном

Переход на резерв запускается в пункте сигнализации, когда звено определяется как недоступное, и выполняются следующие условия:

– передача и прием значащих сигнальных единиц на соответствующем звене сигнализации заканчивается;

– начинается передача сигнальных единиц состояния звена или заполняющих сигнальных единиц;

– определяется одно или несколько резервных звеньев сигнализации;

– осуществляется процедура сохранения содержимого буфера повторной передачи недоступного звена сигнализации;

– сигнальный трафик направляется к одному или нескольким резервным звеньям сигнализации.

1.4 Развитие сети ОКС-7

В бывшем СССР внедрение ОКС-7 началось в середине 80-х годов, одновременно с пуском в эксплуатацию ряда междугородных квазиэлектронных станций (в Минске и Харькове) и узлов автоматической коммутации, связанных между собой этой системой сигнализации (подсистемы MTP и TUP, «Красная книга» МККТТ) по аналоговым каналам на скорости 4,8 Кбит/с. В то время широкомасштабного внедрения ОКС-7 не произошло по объективным причинам, однако работа над пилотным проектом и его последующая коммерческая эксплуатация позволили накопить некоторый опыт решения сетевых проблем и проведения испытаний, а также выявили наиболее критичные точки при организации взаимодействия системы сигнализации № 7 с существующими системами сигнализации телефонной сети общего пользования (СТОП)[12]. К 1993 г. широкомасштабное внедрение ОКС-7 в Казахстане стало не только возможным, но и необходимым. Причиной тому послужили:

– массовое внедрение цифровых систем коммутации с программным управлением и ускорение темпов цифровизации первичной сети на всех уровнях иерархии СТОП;

– создание федеральных сетей подвижной связи по стандартам GSM-900 и NMT-450;

– создание и модернизация ведомственных и коммерческих сетей связи, предоставляющих пользователям более широкий по сравнению с СТОП спектр услуг связи повышенного качества;

– начало внедрения услуг ЦСИО (ISDN) на сетях общего пользования и ведомственных сетях связи.

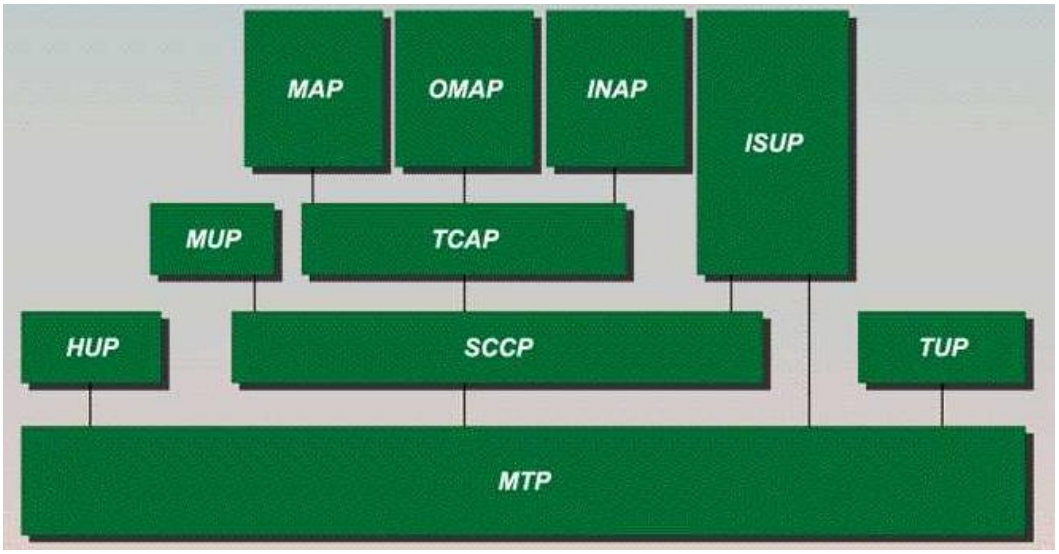

Рисунок 1.12 – Архитектура системы сигнализации

Подсистемы, приведенные на рисунке 1.12:

MTP – передачи сообщений;

SCCP – управления сквозными сигнальными соединенями;

TCAP – транзакций;

MAP – пользовательская подвижная связи (GSM);

ISUP – пользователи ЦСИО;

TUP – телефонного пользователя;

MUP – пользователя подвижной связи (NMT);

HUP – передачи сигналов управления в процессе разговора (NMT);

INAP – пользователя интеллетуальной сети (IN);

OMAP – техобслуживания и эксплуатации.

Наличие на рынке большого числа компаний - операторов и поставщиков оборудования вызвало необходимость координировать и регулировать процесс

внедрения ОКС-7 на национальной сети. Эти функции взяло на себя Министерство транспорта и коммуникации. В 1994 г. специальной рабочей группой Министерства при участии экспертов из основных фирм - производителей коммутационной техники, работающих на российском рынке, были разработаны национальные спецификации системы ОКС-7, в первую очередь для подсистем MTP, ISUP, SCCP и TCAP, которые обеспечивают функционирование телефонных и ISDN-сетей. На сегодняшний день уже разработаны и утверждены спецификации MAP, MUP, HUP, INAP и разработана (но не утверждена) спецификация OMAP[13]. В процессе работы над первыми спецификациями были приняты решения:

– рекомендовать иерархическое построение национальной сети ОКС-7 с использованием индикатора сети (NI) 10bin на федеральном уровне сети и 11bin - на местном (региональном), что, несмотря на географические и демографические особенности республики, позволило бы использовать для адресации пунктов сигнализации 14 бит;

– отказаться от применения звеньев сигнализации ОКС-7 в аналоговых каналах;

– приостановить внедрение подсистемы пользователя телефонии (TUP), что позволило интегрировать процессы внедрения ISDN и ОКС-7;

– ввести обязательную сертификацию оборудования с функциями ОКС-7 (в том числе и для сетей подвижной связи) и ISDN;

– подготовить указание Министерства транспорта и коммуникации о предпочтительном применении ОКС-7 при взаимодействии вновь вводимых коммутационных станций на всех уровнях сетевой иерархии;

– создать «Опытную зону внедрения ОКС-7, услуг ISDN и услуг сетей подвижной связи» (т. е. зону национального пилотного проекта внедрения ОКС-7 и ISDN) и в ее рамках определить систему нумерации пунктов сигнализации, отработать инженерную методику расчета сети ОКС, провести апробирование национальных технических спецификаций подсистем ОКС-7, отработать взаимодействие этих подсистем с существующими системами сигнализации и обеспечить стыковку с подвижными сетями связи различных регионов и т. д.

2 Протокол инициирования сеансов связи - SIP

2.1 Принципы протокола OSI

Протокол инициирования сеансов - Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи. Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям.

Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543. В основу протокола рабочая группа MMUSIC заложила следующие принципы:

Персональная мобильность пользователей. Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения -REGISTER - информирует о своих перемещениях сервер определения местоположения[14].

Масштабируемость сети. Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при её расширении. Серверная структура сети, построенной на базе протокола SIR в полной мере отвечает этому требованию.

Расширяемость протокола. Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

В качестве примера можно привести ситуацию, когда протокол SIP используется для установления соединения между шлюзами, взаимодействующими с ТфОП при помощи сигнализации ОКС7 или DSS1. В настоящее время SIP не поддерживает прозрачную передачу сигнальной информации телефонных систем сигнализации. Вследствие этого дополнительные услуги ISDN оказываются недоступными для пользователей IP-сетей.

Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений, которые должны быть зарегистрированы в уже упоминавшейся ранее организации IANA. При этом, если SIP-сервер принимает сообщение с неизвестными ему полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.

Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.

Интеграция в стек существующих протоколов Интернет, разработанных IETF. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF). Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVR RFC 2205), транспортный протокол реального времени (Real-Time Transport Protocol - RTP, RFC 1889), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP, RFC 2326), протокол описания параметров связи (Session Description Protocol -SDP, RFC 2327). Однако функции протокола SIP не зависят ни от одного из этих протоколов[15].

Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с протоколом H.323. Возможно также взаимодействие протокола SIP с системами сигнализации ТфОП - DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата. Кроме того, протокол SIR наравне с протоколами H.323 и ISUP/IR может применяться для синхронизации работы устройств управления шлюзами; в этом случае он должен взаимодействовать с протоколом MGCR Другой важной особенностью протокола SIP является то, что он приспособлен к организации доступа пользователей сетей IP-телефонии к услугам интеллектуальных сетей, и существует мнение, что именно этот протокол станет основным при организации связи между указанными сетями.

2.2 Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5/ATM, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDR При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и т.п.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDR но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки. В свою очередь, протокол TCP упрощает работу с межсетевыми экранами (firewall), а также гарантирует надежную доставку данных. При использовании протокола TCP разные

сообщения, относящиеся к одному вызову, либо могут передаваться по одному TCP-соединению, либо для каждого запроса и ответа на него может открываться отдельное TCP-соединение. В таблице 2.1 показано место, занимаемое протоколом SIP в стеке протоколов TCP/IP[16].

Таблица 2.1 – Протоколы SIP и уровни модели OSI

Протокол	Уровень модели OSI
Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCPи LOP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень
PPP, ATM, Ethernet	Уровень звена данных
UTP5, SDH, DDH, V.34 и др.	Физический уровень

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который следует передавать информацию. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между сторонами данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи - SDP (Session Description Protocol). Поскольку в течение сеанса связи может производиться его модификация, предусмотрена передача сообщений SIP с новыми описаниями сеанса средствами SDR[17].

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

В протоколе SIP не реализованы механизмы управления потоками информации и предоставления гарантированного качества обслуживания. Кроме того, протокол SIP не предназначен для передачи пользовательской информации, в его сообщениях может переноситься информация лишь ограниченного объема. При переносе через сеть слишком большого сообщения SIP не исключена его фрагментация на уровне IP, что может повлиять на качество передачи информации.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является

поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP.

Протокол SIP предусматривает организацию конференций трех видов:

– в режиме многоадресной рассылки (multicasting), когда информация передается на один multicast-адрес, а затем доставляется сетью конечным адресатам;

– при помощи устройства управления конференции (MCU), к которому участники конференции передают информацию в режиме точка-точка, а оно, в свою очередь, обрабатывает ее (т.е. смешивает или коммутирует) и рассылает участникам конференции;

– путем соединения каждого пользователя *с* каждым в режиме точка-точка.

Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

2.3 Архитектура сети SIP

В некотором смысле прародителем протокола SIP является протокол переноса гипертекста - HTTP (Hypertext Transfer Protocol, RFC 2068). Протокол SIP унаследовал от него синтаксис и архитектуру «клиент-сервер», которую иллюстрирует рисунок 2.1.

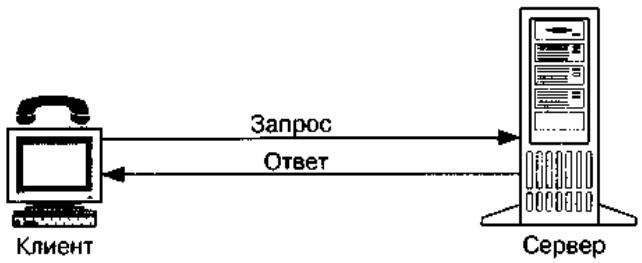

Рисунок 2.1 – Архитектура «клиент-сервер»

Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об ошибке или информацию, затребованную клиентом.

Управление процессом обслуживания вызова распределено между разными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением, является терминал. Остальные элементы сети отвечают за маршрутизацию вызовов, а в некоторых случаях предоставляют дополнительные услуги[18].

2.3.1 Терминал

В случае, когда клиент и сервер взаимодействуют непосредственно с пользователем (т.е. реализованы в оконечном оборудовании пользователя), они называются, соответственно, клиентом агента пользователя - User Agent Client (UAC) - и сервером агента пользователя - User Agent Server (UAS).

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. Если в устройстве присутствуют и сервер UAS, и клиент UAC, то оно называется агентом пользователя - User Agent (UA), а по своей сути представляет собой терминальное оборудование SIR

Кроме терминалов определены два основных типа сетевых элементов SIP: прокси-сервер (proxy server) и сервер переадресации (redirect server).

2.3.2 Прокси-сервер

Прокси-сервер (от английского proxy - представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Прокси-сервер может быть физически совмещен с сервером определения местоположения (в этом случае он называется registrar) или существовать отдельно от этого сервера, но иметь возможность взаимодействовать с ним по протоколам LDAP (RFC 1777), rwhois (RFC 2167) и по любым другим протоколам.

Предусмотрено два типа прокси-серверов - с сохранением состояний (stateful) и без сохранения состояний (stateless).

Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения ответов на запросы.

Сервер первого типа позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа. Он может применяться для обслуживания небольшого количества клиентов, например, в локальной сети. Прокси-сервер должен сохранять информацию о состояниях, если он:

- использует протокол TCP для передачи сигнальной информации;
- работает в режиме многоадресной рассылки сигнальной информации;
- размножает запросы.

Последний случай имеет место, когда прокси-сервер ведет поиск вызываемого пользователя сразу в нескольких направлениях, т.е. один запрос, который пришел к прокси-серверу, размножается и передается одновременно по всем этим направлениям.

Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний для других.

Алгоритм работы пользователей с прокси-сервером выглядит следующим образом. Поставщик услуг IP-телефонии сообщает адрес прокси-сервера своим пользователям. Вызывающий пользователь передает к прокси-серверу запрос соединения. Сервер обрабатывает запрос, определяет местоположение вызываемого пользователя и передает запрос этому пользователю, а затем получает от него ответ, подтверждающий успешную обработку запроса, и транслирует этот ответ пользователю, передавшему запрос. Прокси-сервер может модифицировать некоторые заголовки сообщений, которые он транслирует, причем каждый сервер, обработавший запрос в процессе его передачи от источника к приемнику, должен указать это в SIP-запросе для того, чтобы ответ на запрос вернулся по такому же пути.

2.3.3 Сервер переадресации

Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

Сервер переадресации не терминирует вызовы как сервер RAS и не инициирует собственные запросы как прокси-сервер. Он только сообщает адрес либо вызываемого пользователя, либо прокси-сервера. По этому адресу инициатор запроса передает новый запрос. Сервер переадресации не содержит клиентскую часть программного обеспечения.

Но пользователю не обязательно связываться с каким-либо SIP-сервером. Он может сам вызвать другого пользователя при условии, что знает его текущий адрес.

2.3.4 Сервер определения местоположения пользователей

Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени. Например, сотрудник предприятия уезжает в командировку, и все вызовы, адресованные ему, должны быть направлены в другой город на его временное место работы. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения REGISTER. Возможны два режима регистрации: пользователь может сообщить свой новый адрес один раз, а может

регистрироваться периодически через определенные промежутки времени. Первый способ подходит для случая, когда терминал, доступный пользователю, включен постоянно, и его не перемещают по сети, а второй - если терминал часто перемещается или выключается.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

Этот сервер может быть совмещен с прокси-сервером (в таком случае он называется registrar) или быть реализован отдельно от прокси-сервера, но иметь возможность связываться с ним.

В RFC 2543 сервер определения местоположения представлен как отдельный сетевой элемент, но принципы его работы в этом документе не регламентированы. Стоит обратить внимание на то, что вызывающий пользователь, которому нужен текущий адрес вызываемого пользователя, не связывается с сервером определения местоположения напрямую. Эту функцию выполняют SIP-серверы при помощи протоколов LDAP (RFC 1777), rwhois (RFC 2167), или других протоколов[19].

2.3.5 Пример SIP- сети

Резюмируя все сказанное выше, отметим, что сети SIP строятся из элементов трех основных типов: терминалов, прокси-серверов и серверов переадресации. На рисунке 2.2 приведен пример возможного построения сети SIP.

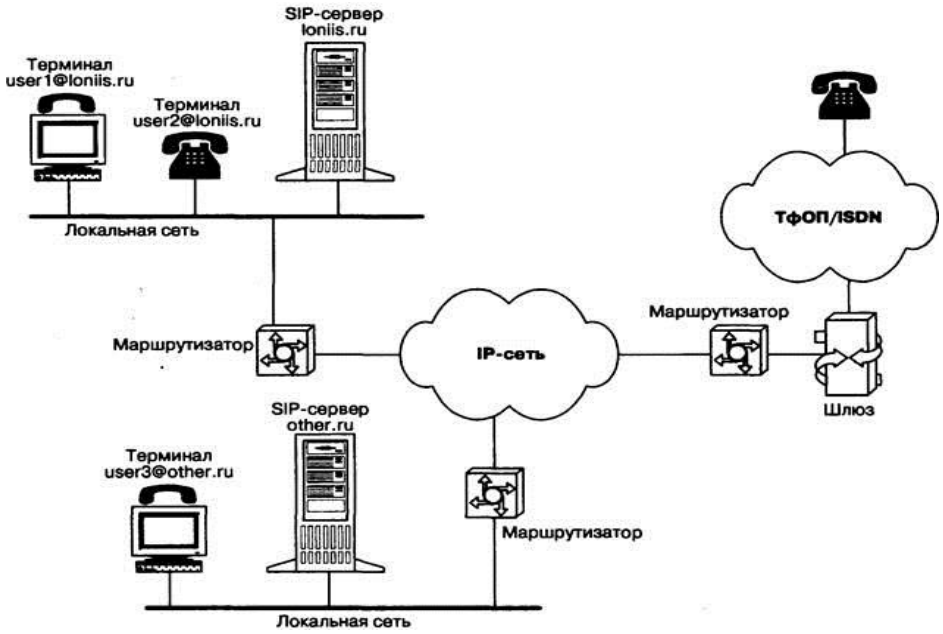

Рисунок 2.2 – Пример построения сети SIP

Стоит обратить внимание на то что, что SIP-серверы, представленные на рисунке 16, являются отдельными функциональными сетевыми элементами. Физически они могут быть реализованы на базе серверов локальной сети, которые, помимо выполнения своих основных функций, будут также обрабатывать SIP-сообщения. Терминалы же могут быть двух типов: персональный компьютер со звуковой платой и программным обеспечением SIP-клиента (UA) или SIP-телефон, подключающийся непосредственно к ЛВС Ethernet (SIP-телефоны, производимые компанией Cisco Systems, недавно появились на российском рынке). Таким образом, пользователь локальной вычислительной сети передает все запросы к своему SIP-серверу, а тот обрабатывает их и обеспечивает установление соединений. Путем программирования сервер можно настроить на разные алгоритмы работы: он может обслуживать часть пользователей (например, руководство предприятия или особо важных лиц) по одним правилам, а другую часть - по иным. Возможно также, что сервер будет учитывать категорию и срочность вызовов, а также вести начисление платы за разговоры.

Структурная схема организации услуг SIP-сервера представлена на рисунке 2.3.

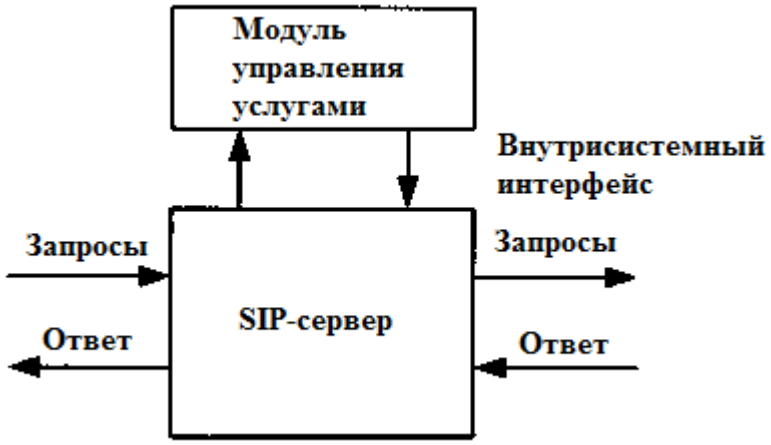

Рисунок 2.3 – Структурная схема организации услуг SIP-сервера

Модуль управления услугами отвечает за предоставление услуг и за общее управление сервером. Принятые сервером запросы и ответы поступают в модуль управления услугами и обрабатываются им, на основании чего определяется реакция на полученные сообщения. Интерфейс человек-машина позволяет гибко менять настройки сервера и вести мониторинг сети.

2.4 Сообщения протокола SIP

2.4.1 Структура сообщений

Согласно архитектуре «клиент-сервер» все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

Например, чтобы инициировать установление соединения, вызывающий пользователь должен сообщить серверу ряд параметров, в частности, адрес вызываемого пользователя, параметры информационных каналов и др. Эти параметры передаются в специальном SIP-запросе. От вызываемого пользователя к вызывающему передается ответ на запрос, также содержащий ряд параметров.

Все сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP, как уже упоминалось ранее, идентичны используемым в протоколе HTTP. На рисунке 2.4 представлена структура сообщений протокола SIP.

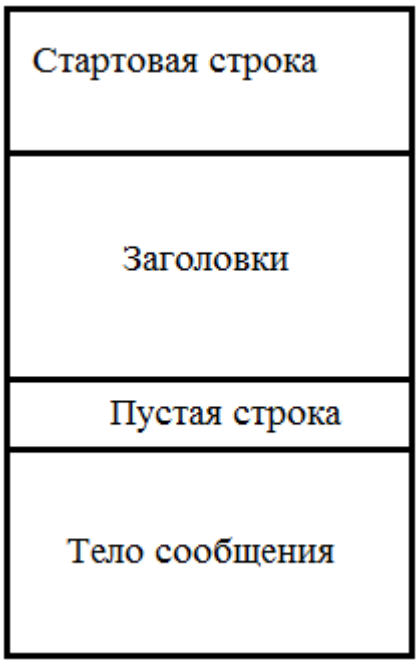

Рисунок 2.4 – Структура сообщений протокола SIP

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, в этой строке указываются тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в стартовой строке указываются номер версии протокола, тип ответа и его короткая расшифровка, предназначенная только для пользователя.

Заголовки сообщений содержат сведения об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания данного сообщения. О типе заголовка можно узнать по его имени. Оно не зависит от регистра (т.е. буквы могут быть прописные и строчные), но обычно имя пишут с большой буквы, за которой идут строчные.

Сообщения протокола SIP могут содержать так называемое тело сообщения. В запросах ACK, INVITE и OPTIONS тело сообщения содержит описание сеансов связи, например, в формате протокола SDP Запрос BYE тела

сообщения не содержит, а ситуация с запросом REGISTER подлежит дальнейшему изучению[20]. С ответами дело обстоит иначе: любые ответы могут содержать тело сообщения, но содержимое тела в них бывает разным.

2.4.2 В протоколе SIP определено четыре вида заголовков:

– Общие заголовки, присутствующие в запросах и ответах;

– Заголовки содержания, переносят информацию о размере тела сообщения или об источнике запроса (начинаются со слова «Content»);

– Заголовки запросов, передающие дополнительную информацию о запросе;

– Заголовки ответов, передающее дополнительную информацию об ответе.

Заголовок содержит название, за которым, отделенное двоеточием, следует значение заголовка. В поле значения содержатся передаваемые данные. Следует отметить, что если сервер принимает сообщения, заголовки которых ему не известны, то эти заголовки игнорируются.

Ниже представлены наиболее часто используемые заголовки.

Заголовок Call-ID - уникальный идентификатор сеанса связи или всех регистрации отдельного клиента, он подобен метке соединения (call reference) в сигнализации DSS-1. Значение идентификатору присваивает сторона, которая инициирует вызов. Заголовок Call-ID состоит из буквенно-числового значения и имени рабочей станции, которая присвоила значение этому идентификатору. Между ними должен стоять символ @, например, 2345call@rts.loniis.ru. Возможна следующая ситуация: к одной мультимедийной конференции относятся несколько соединений, тогда все они будут иметь разные идентификаторы Call-ID.

Заголовок To - определяет адресата. Кроме SIP-адреса здесь может стоять параметр «tag» для идентификации конкретного терминала пользователя (например, домашнего, рабочего или сотового телефона) в том случае, когда все его терминалы зарегистрированы под одним адресом SIP URL. Запрос может множиться и достичь разных терминалов пользователя; чтобы их различать, необходимо иметь метку tag. Ее вставляет в заголовок терминальное оборудование вызванного пользователя при ответе на принятый запрос.

Если необходим визуальный вывод имени пользователя, например, на дисплей, то имя пользователя также размещается в поле To.

Заголовок From - идентифицирует отправителя запроса; по структуре аналогичен полю To.

Заголовок Via служит для того, чтобы избежать ситуации, в которых запрос пойдет по замкнутому пути, а также для тех случаев, когда необходимо, чтобы запросы и ответы обязательно проходили по одному и тому же пути (например, в случае использования межсетевого экрана - firewall). Дело в том, что запрос может проходить через несколько прокси-серверов, каждый из которых принимает, обрабатывает и переправляет запрос к следующему прокси-серверу, и так до тех пор, пока запрос не достигнет адресата. Таким

образом, в заголовке Via указывается весь путь, пройденный запросом: каждый прокси-сервер добавляет поле со своим адресом. При необходимости (например, чтобы обеспечить секретность) действительный адрес может скрываться.

Например, запрос на своем пути обрабатывался двумя прокси-серверами: сначала сервером loniis.ru, потом sip.telecom.com. Тогда в запросе появятся следующие поля:

Via: SIP/2.0/UDPsip.telecom.com:5060;branch=721e418c4.1

Via: SIP/2.0/UDP loniis.ru:5060,

где параметр «branch» означает, что на сервере sip.telecom.com запрос был размножен и направлен одновременно по разным направлениям, и наш запрос был передан по направлению, которое идентифицируется следующим образом: 721 e418c4.1.

Содержимое полей Via копируется из запросов в ответы на них, и каждый сервер, через который проходит ответ, удаляет поле Via со своим именем.

В заголовок Record-route прокси-сервер вписывает свой адрес - SIP URL, - если хочет, чтобы последующие запросы прошли через него.

Заголовок Content-Type определяет формат описания сеанса связи. Само описание сеанса, например, в формате протокола SDP, включается в тело сообщения.

Заголовок Content-Length указывает размер тела сообщения.

2.4.3 Типы запросов протокола SIP

В настоящей версии протокола SIP определено шесть типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. С помощью запросов клиент сообщает о текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке. В той же строке в поле Request-URI указан SIP-адрес оборудования, которому этот запрос адресован. Содержание полей To и Request-URI может различаться, например, в поле To может быть указан публикуемый адрес абонента, а в поле Request-URI - текущий адрес пользователя.

Запрос INVITE приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, в котором указывается вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, а также может указываться вид информации, которую вызываемый пользователь желает передавать. В ответе на запрос типа INVITE указывается вид информации, которая будет приниматься вызываемым пользователем, и, кроме того, может указываться вид информации, которую вызываемый пользователь собирается передавать (возможные параметры передачи информации).

В этом сообщении могут содержаться также данные, необходимые для аутентификации абонента, и, следовательно, доступа клиентов к SIP-серверу. При необходимости изменить характеристики уже организованных каналов передается запрос INVITE с новым описанием сеанса связи. Для приглашения нового участника к уже установленному соединению также используется сообщение INVITE.

Запрос ACK подтверждает прием ответа на запрос INVITE. Следует отметить, что запрос ACK используется только совместно с запросом INVITE, т.е. этим сообщением оборудование вызывающего пользователя показывает, что оно получило окончательный ответ на свой запрос INVITE. В сообщении ACK может содержаться окончательное описание сеанса связи, передаваемое вызывающим пользователем.

Запрос CANCEL отменяет обработку ранее переданных запросов с теми же, что и в запросе CANCEL, значениями полей Call-ID, To, From и CSeq, но не влияет на те запросы, обработка которых уже завершена. Например, запрос CANCEL применяется тогда, когда прокси-сервер размножает запросы для поиска пользователя по нескольким направлениям и в одном из них его находит. Обработку запросов, разосланных во всех остальных направлениях, сервер отменяет при помощи сообщения CANCEL[21].

Запросом BYE оборудование вызываемого или вызывающего пользователя завершает соединение. Сторона, получившая запрос BYE, должна прекратить передачу речевой (мультимедийной) информации и подтвердить его выполнение ответом 200 OK.

При помощи запроса типа REGISTER пользователь сообщает свое текущее местоположение. В этом сообщении содержатся следующие поля:

– Поле To содержит адресную информацию, которую надо сохранить или модифицировать на сервере;

– Поле From содержит адрес инициатора регистрации. Зарегистрировать пользователя может либо он сам, либо другое лицо, например, секретарь может зарегистрировать своего начальника;

– Поле Contact содержит новый адрес пользователя, по которому должны передаваться все дальнейшие запросы INVITE. Если в запросе REGISTER поле Contact отсутствует, то регистрация остается прежней. В случае отмены регистрации здесь помещается символ «*»;

– В поле Expires указывается время в секундах, в течение которого регистрация действительна. Если данное поле отсутствует, то по умолчанию назначается время - 1 час, после чего регистрация отменяется. Регистрацию можно также отменить, передав сообщение REGISTER с полем Expires, которому присвоено значение О, и с соответствующим полем Contact.

Запросом OPTIONS вызываемый пользователь запрашивает информацию о функциональных возможностях терминального оборудования вызываемого пользователя. В ответ на этот запрос оборудование вызываемого пользователя сообщает требуемые сведения. Применение запроса OPTIONS ограничено теми случаями, когда необходимо узнать о функциональных возможностях

оборудования до установления соединения. Для установления соединения запрос этого типа не используется.

После испытаний протокола SIP в реальных сетях оказалось, что для решения ряда задач вышеуказанных шести типов запросов недостаточно. Поэтому возможно, что в протокол будут введены новые сообщения. Так, в текущей версии протокола SIP не предусмотрен способ передачи информации управления соединением или другой информации во время сеанса связи. Для решения этой задачи был предложен новый тип запроса - INFO. Он может использоваться в следующих случаях:

– для переноса сигнальных сообщений ТфОП/13ОМ/сотовых сетей между шлюзами в течение разговорной сессии;

– для переноса сигналов DTMF в течение разговорной сессии;

– для переноса биллинговой информации.

Завершив описание запросов протокола SIP, рассмотрим, в качестве примера, типичный запрос типа INVITE:

```
INVITE sip: watson@boston.bell-tel.com SIP/2.0
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip: a.g.bell@bell-tel.com>
To: T. Watson <sip: watson@bell-tel.com>
Call-ID: 3298420296@kton.bell-tel.com
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: ...
v=0
o=bell 53655765 2353687637 IN IP4 128.3.4.5
C=IN IP4 kton.bell-tel.com
m=audio 3456 RTP/AVP 0345
```

В этом примере пользователь Bell (a.g.bell@bell-tel.com) вызывает пользователя Watson (watson@bell-tel.com). Запрос передается к прокси-серверу (boston.bell-tel.com). В полях To и From перед адресом стоит запись, которую вызывающий пользователь желает вывести на дисплей вызываемого пользователя. В теле сообщения оборудование вызывающего пользователя указывает в формате протокола SDR что оно может принимать в порту 3456 речевую информацию, упакованную в пакеты RTP и закодированную по одному из следующих алгоритмов кодирования: 0 - PCMU, 3 - GSM, 4 - G.723 и 5 - DVI4.

При передаче сообщений протокола SIP, упакованных в сигнальные сообщения протокола UDP, существует вероятность того, что размер запроса или ответа окажется больше максимально допустимого для данной сети, и произойдет фрагментация пакета. Чтобы избежать этого, используется сжатый формат имен основных заголовков, подобно тому, как это делается в протоколе SDP.

При написании имен заголовков в сжатом виде сообщение INVITE, показанное ранее на рисунке 19, будет выглядеть следующим образом:

INVITE sip: watson@boston.bell-tel.com SIP/2.0
v: SIP/2.0/0DP kton.bell-tel.com
f: A. Bell <sip: a.g.bell@bell-tel.com>
t: T. Watson <sip: watson@bell-tel.con»
i: 3298420296@kton.bell-tel.com Cseq: 1 INVITE
c: application/sdp
1: ...
v=0
0=bell 53655765 2353687637 IN IP4 128.3.4.5
C=IN IP4 kton.bell-tel.com
m=audio 3456 RTP/AVP 0345

2.4.4 Типы ответов и запросов

После приема и интерпретации запроса, адресат (прокси-сервер) передает ответ на этот запрос. Содержание ответов бывает разным: подтверждение установления соединения, передача запрошенной информации, сведения о неисправностях и т.д. Структуру ответов и их виды протокол SIP унаследовал от протокола HTTP.

Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется трехзначным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование даже может не знать все коды ответов, но оно обязательно должно интерпретировать первую цифру ответа. Все ответы делятся на две группы: информационные и финальные. Информационные ответы показывают, что запрос находится в стадии обработки. Они кодируются трехзначным числом, начинающимся с единицы, - 1xx. Некоторые информационные ответы, например, 100 Trying, предназначены для установки на нуль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов - 180 Ringing; по назначению он идентичен сигналу «Контроль посылки вызова» в СТОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

Финальные ответы кодируются трехзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса. Назначение финальных ответов каждого типа рассматривается ниже.

Ответы 2xx означают, что запрос был успешно обработан. В настоящее время из всех ответов типа 2xx определен лишь один -200 ОК. Его значение зависит от того, на какой запрос он отвечает:

– ответ 200 OK на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;

– ответ 200 OK на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится;

– ответ 200 OK на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится;

– ответ 200 OK на запрос REGISTER означает, что регистрация прошла успешно;

– ответ 200 OK на запрос OPTION служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответы 3xx информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована для нового вызова:

– в ответе 300 Multiple Choices указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и вызывающему пользователю предлагается выбрать один из них;

– ответ 301 Moved Permanently означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле Contact;

– ответ 302 Moved Temporary означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, который указывается в поле Contact.

Ответы 4xx информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации:

– ответ 400 Bad Request означает, что запрос не понят из-за наличия в нем синтаксических ошибок;

– ответ 401 Unauthorized означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае;

– ответ 403 Forbidden означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого адреса не обслуживаются и т.д.;

– ответ 485 Ambiguous означает, что адрес в запросе не определяет вызываемого пользователя однозначно;

– ответ 486 Busy Here означает, что вызываемый пользователь в настоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

Ответы 5xx информируют о том, что запрос не может быть обработан из-за отказа сервера:

– ответ 500 Server Internal Error означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться повторно послать запрос через некоторое время;

– ответ 501 Not Implemented означает, что в сервере не реализованы функции, необходимые для обслуживания этого запроса. Ответ передается, например в том случае, когда сервер не может распознать тип запроса;

– ответ 502 Bad Gateway информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;

– ответ 503 Service Unavailable говорит от том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы 6xx информируют о том, что соединение с вызываемым пользователем установить невозможно:

– ответ 600 Busy Everywhere сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;

– ответ 603 Decline означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;

– ответ 604 Does Not Exist Anywhere означает, что вызываемого пользователя не существует.

Напомним, что запросы и ответы на них образуют SIP-транзакцию. Она осуществляется между клиентом и сервером и включает в себя все сообщения, начиная с первого запроса и заканчивая финальным ответом. При использовании в качестве транспорта протокола TCP все запросы и ответы, относящиеся к одной транзакции, передаются по одному TCP-соединению.

Ниже представлен пример ответа на запрос INVITE:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip:a.g.bell@bell-tel.com>
Tp: <sip:watson@bell-tel.com>;
Call-ID: 3298420296@kton.bell-tel.com
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: ...
v=0
o=watson 4858949 4858949 IN IP4 192.1.2.3
t=3149329600 0
```

```
c=IN IP4 boston.bell-tel.com
m=audio 5004 RTP/AVP 0 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
```

В этом примере приведен ответ пользователя Watson на приглашение принять участие в сеансе связи, полученное от пользователя Bell. Наиболее вероятный формат приглашения рассмотрен нами ранее (рис. 7.7). Вызываемая сторона информирует вызывающую о том, что она может принимать в порту 5004 речевую информацию, закодированную в соответствии с алгоритмами кодирования PCMU, GSM. Поля From, To, Via, Call-ID взяты из запроса, показанного на рисунке 21. Из примера видно, что это ответ на запрос INVITE с полем CSeq: 1.

После того, как мы рассмотрели запросы и ответы на них, можно отметить, что протокол SIP предусматривает разные алгоритмы установления соединения. При этом стоит обратить внимание, что одни и те же ответы можно интерпретировать по-разному в зависимости от конкретной ситуации.

2.5 Алгоритмы установления соединения

Протоколом SIP предусмотрены 3 основных сценария установления соединения: с участием прокси-сервера, с участием сервера переадресации и непосредственно между пользователями. Различие между перечисленными сценариями заключается в том, что по-разному осуществляется поиск и приглашение вызываемого пользователя. В первом случае эти функции возлагает на себя прокси-сервер, а вызывающему пользователю необходимо знать только постоянный SIP-адрес вызываемого пользователя. Во втором случае вызывающая сторона самостоятельно устанавливает соединение, а сервер переадресации лишь реализует преобразование постоянного адреса вызываемого абонента в его текущий адрес. И, наконец, в третьем случае вызывающему пользователю для установления соединения необходимо знать текущий адрес вызываемого пользователя.

Перечисленные сценарии являются простейшими. Ведь прежде чем вызов достигнет адресата, он может пройти через несколько прокси-серверов, или сначала направляется к серверу переадресации, а затем проходит через один или несколько прокси-серверов. Кроме того, прокси-серверы могут размножать запросы и передавать их по разным направлениям и т.д. Но, все же, как уже было уже отмечено в начале параграфа, эти три сценария являются основными. Здесь мы рассмотрим подробно два первых сценария; третий сценарий в данной главе рассматриваться не будет.

2.5.1 Установление соединения с участием сервера переадресации

В этом параграфе описан алгоритм установления соединения с участием сервера переадресации вызовов. Администратор сети сообщает пользователям

адрес сервера переадресации. Вызывающий пользователь передает запрос INVITE (1) на известный ему адрес сервера переадресации и порт 5060, используемый по умолчанию (рисунок 2.5). В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (2), который сообщает ему этот адрес (3). Сервер переадресации в ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого пользователя (4), или он может сообщить список зарегистрированных адресов вызываемого пользователя и предложить вызывающему пользователю самому выбрать один из них. Вызывающая сторона подтверждает прием ответа 302 посылкой сообщения АСК (5).

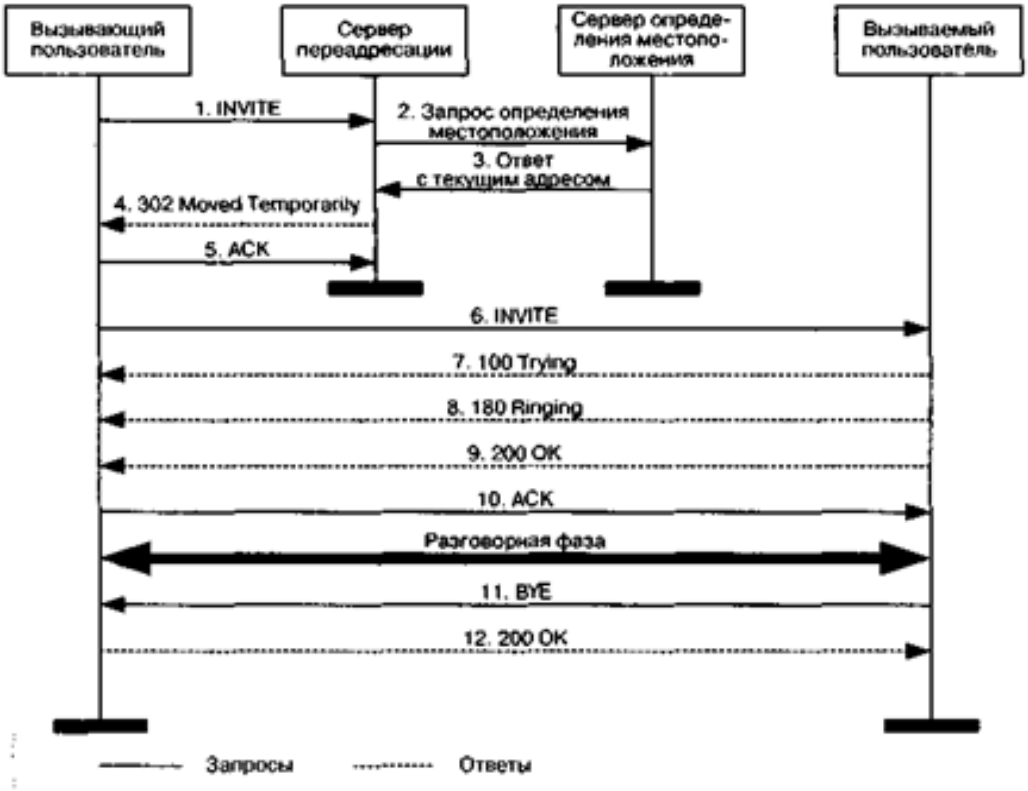

Рисунок 2.5 – Сценарий установления соединения через сервер переадресации

Теперь вызывающая сторона может связаться непосредственно с вызываемой стороной. Для этого она передает новый запрос INVITE (6) с тем же идентификатором Call-ID, но другим номером CSeq. В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDR Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров. После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). После приема вызываемым пользователем входящего вызова

удаленной стороне передается сообщение 200 ОК (9), в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDR Терминал вызывающего пользователя подтверждает прием ответа запросом АСК (10). На этом фаза установления соединения закончена и начинается разговорная фаза.

По завершении разговорной фазы любой из сторон передается запрос BYE (11), который подтверждается ответом 200 ОК (12).

2.5.2. Установление соединения с участием прокси-сервера

В этом параграфе описан алгоритм установления соединения с участием прокси-сервера. Администратор сети сообщает адрес этого сервера пользователям. Вызывающий пользователь передает запрос INVITE (1) на адрес прокси-сервера и порт 5060, используемый по умолчанию (рисунок 2.6). В запросе пользователь указывает известный ему адрес вызываемого пользователя. Прокси-сервер запрашивает текущий адрес вызываемого пользователя у сервера определения местоположения (2), который и сообщает ему этот адрес (3). Далее прокси-сервер передает запрос INVITE непосредственно вызываемому оборудованию (4). Опять в запросе содержатся данные о функциональных возможностях вызывающего терминала, но при этом в запрос добавляется поле Via с адресом прокси-сервера для того, чтобы ответы на обратном пути шли через него. После приема и обработки запроса вызываемое оборудование сообщает своему пользователю о входящем вызове, *а* встречной стороне передает ответ 180 Ringing (5), копируя в него из запроса поля To, From, Call-ID, CSeq и Via. После приема вызова пользователем встречной стороне передается сообщение 200 ОК (6), содержащее данные о функциональных возможностях вызываемого терминала в формате протокола SDR Терминал вызывающего пользователя подтверждает прием ответа запросом АСК (7). На этом фаза установления соединения закончена и начинается разговорная фаза.

По завершении разговорной фазы одной из сторон передается запрос BYE (8), который подтверждается ответом 200 ОК (9).

Все сообщения проходят через прокси-сервер, который может модифицировать в них некоторые поля[22].

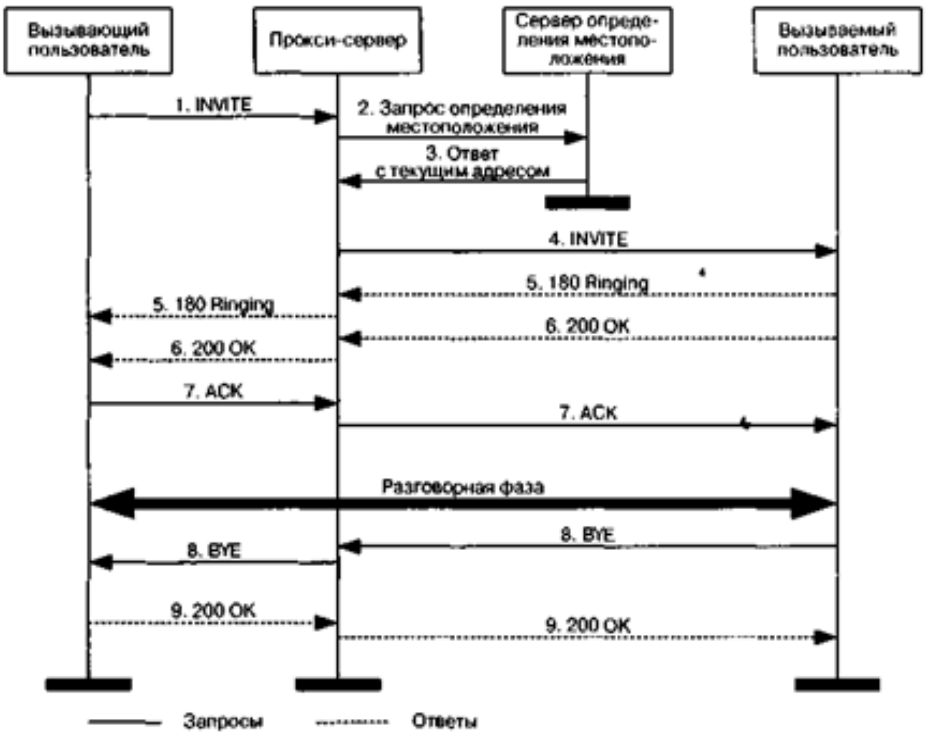

Рисунок 2.6 – Сценарий установления соединения через прокси-сервер

3 Особенности взаимодействия SIP с протоколами управления СТОП

Для взаимодействия с традиционными телефонными сетями, использующими сигнализацию ОКС-7, была разработана модификация протокола SIP для телефонии: Session Initiation Protocol for Telephones (SIP-T). Основная задача, которой заключается в прозрачной передаче сообщений ISUP по IP-сети. Эта задача реализуется путём инкапсуляции или трансляции сигнальных единиц ОКС в сообщения SIP.

Требование к сети IP-телефонии - это возможность так называемой прозрачности услуг относительно СТОП. Традиционные телефонные услуги, такие как call waiting, услуга 800 и т.д. должны иметь возможность реализации с помощью системы сигнализации №7[23].

SIP-T имеет 2 метода взаимодействия с ОКС-7:

– Инкапсуляция сообщений ОКС7/DSS-1 в сообщения SIP;
– Трансляция информации из сообщений ОКС7/DSS-1.

3.1 Процедуры инкапсуляции сигнальных сообщений

Возможность инкапсуляции сигнализации СТОП является одним из основных требований к SIP–T. SIP–T использует разделяемое на необходимое число частей тело сообщения в кодировке MIME, что в свою очередь позволяет включать в сообщения SIP любую информацию (данные протоколов ISUP, SDP и т.д.). Есть много различных вариантов ISUP и поэтому для того, чтобы определить используемый вариант введен специальный тип MIME - ISUP Media Type, и это позволяет удобно получить информацию об используемом варианте протокола ISUP.

ISUP Media Type содержит нижеприведенную информацию (см. таблицу 3.1):

Таблица 3.1 – Тип сообщения и параметры

Тип сообщения	Параметры
Media type name:	application
Media subtype name:	ISUP
Required parameters:	version
Optional parameters:	base
Encoding scheme:	binary

Если использовать параметр «version» то это позволяет узнать тип ISUP для системных администраторов. Это позволяет каждому SoftSwitch/MGC правильно обработать сообщение, или отправить пользователю сообщение о том, что тот или иной тип ISUP не поддерживается. Данная спецификация не

ограничивает значения, которые могут быть использованы в «version»; это оставлено на усмотрение системным администраторам.

Параметр «version» также может быть использован для идентификации реализации ISUP в сети (например, X-NetxProprietaryISUPv3), или же для того, чтобы определить известные стандартны версии ISUP, такие как версия ANSI или ITU-T.

Параметр «base» может включаться опционально в некоторые сообщения, если же необходимо, чтобы получатель корректно распознал используемый тип ISUP, т.к. параметр «version» может быть не понятен или не корректен. В таблице 3.2 представлены возможные значения для параметра «base», которые поддерживаются в теле сообщения типа application/ISUP[24].

Таблица 3.2 – Значение параметра «base»

Значение параметра «base»	Протокол
Itu-t88	ITU-T Q.761-4 (1988)
Itu-t92+	ITU-T Q.761-4 (1992)
Ansi88	ANSI T1.113-1988
Ansi00	ANSI T1.113-2000
Etsi121	ETS 300 121
Etsi356	ES 300 356
Gr317	BELLCORE GR-317
Ttc87	JT-Q761-4(1987-1992)
Ttc93+	JT-Q761-4(1993-)

Заголовок Content-Disposition иногда может служить для описания процесса обработки, во вложенном сообщении ISUP, также какие действия нужно предпринять, если же в приемнике было непонятно содержимое заголовка Content-Type. По умолчанию значение заголовка Content-Disposition для ISUP сообщений - signal. Это показывает, что данная часть тела сообщения содержит в себе сигнальную информацию, но не содержит описания соединения.

Ниже представлен пример встречающихся заголовка (параметр «base» может отсутствовать):

Content-Type: application/ISUP; version=nxv3; base=etsi121;

Content-Disposition: signal; handling=optional.

Ниже на рисунке 3.3 приведен пример сообщения INVITE, которое содержит информацию протокола SDP и инкапсулированное сообщение ISUP IAM.

Также части сообщения разделяются пустой строкой, которые задаются параметром boundary. В данном примере для разделения используется пустая строка unique-boundary-1:

```
INVITE sip:78123877658@max.loniis.ru SIP/2.0
Via: SIP/2.0/UDP anton.loniis.ru
From: sip:78124513355@anton.loniis.ru
To: sip:78123877658@max.loniis.ru
Call-ID: MAX123199902171209550099@max.loniis.ru
CSeq: 8348 INVITE
Contact: <sip:anton@loniis.ru>
Content-Length: 436
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0
[
--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646
[
v=0
o=jpeterson 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP seminar
c=IN IP4 MG122.loniis.ru
t= 2873397496  2873404696
m=audio 9092 RTP/AVP 0 3 4
--unique-boundary-1
Content-Type: application/ISUP; version=nxv3;
base=etsi121
Content-Disposition: signal; handling=optional
[
01 00 49 00 00 03 02 00 07 04 10 00 33 63 21
43 00 00 03 06 0d 03 80 90 a2 07 03 10 03 63
53 00 10 0a 07 03 10 27 80 88 03 00 00 89 8b
0e 95 1e 1e 1e 06 26 05 0d f5 01 06 10 04 00
--unique-boundary-1
```

3.2 Процедуры трансляции сигнальных сообщений

Трансляция применяется для преобразовании сигнальной информации между протоколами ISUP и SIP. Трансляция включает в себя два компонента:

– преобразование/конвертирование сигнализации ISUP в SIP на уровне сообщений. В SIP–T используются MGC, которые создают сообщения ISUP из поступающих сообщений SIP и наоборот. Для этого нужно точное описание или определение правил преобразования между сообщениями ISUP и SIP, каждое из сообщений ISUP должно быть транслировано в конкретное сообщение SIP. Например, IAM в INVITE, REL в BYE и т.д.

– преобразование/конвертирование параметров сообщения ISUP в заголовок SIP сообщения: В запросе SIP, который используется для установки соединения, должна быть необходимая для маршрутизации прокси-серверами информация, например это телефонный номер, набранный вызывающим абонентом.

На практике важно стандартизировать процедуры трансляции информации из ISUP в SIP (например, Called Party Number в ISUP IAM записывается в заголовок To и поле Request-URI и т.д.).

Одной из возможных проблем трансляции при транзите трафика через сеть SIP это то, что параметр ISUP, переведенный в заголовок сообщения SIP, может измениться промежуточными узлами на сети. Конечный MGC (точка выхода из сети SIP) иногда может получить сообщение, в котором параметры заголовка сообщения SIP не соответствуют параметрам вложенного сообщения ISUP. Например, параметр заголовка To и поля Request-URI запроса SIP отличаются от параметра Called Party Number (номер вызываемого абонента) во вложенном сообщении ISUP. В таком случае приоритет имеют значения заголовков, т.е. при создании нового сообщения параметры заполняются значениями из заголовков запроса SIP, а отсутствующая информация будет заимствована из вложенного сообщения ISUP, если оно присутствует.

3.3 Согласование содержимого сообщений протокола SIP

Шлюз, который отправляет запрос, включает в сообщение тело, которая состоит из нескольких частей различных типов: например, описание сеанса SDP и сообщение ISUP. Если же получатель не поддерживает разделители тела сообщения на несколько частей (формат multipart/mixed) и/или пришедший в сообщении тип ISUP MIME (application/ISUP), то он отклоняет поступивший запрос и отправит ответ с кодом 415 (Unsupported Media Type), в котором будут содержаться поддерживаемые форматы (по умолчанию - application/SDP). Шлюз, который отсылал сообщение, далее должен переслать запрос повторно, перед этим удалив из него часть тела с сообщением ISUP, оставив только описание SDP, после этого запрос будет принят.

Это приводит к необходимости наличия механизма, в котором устройство, которое отправляет сообщение, отмечает, какие части тела сообщения в запросе необходимые, а какие опциональные. На принимающей стороне, если же устройство не будет поддерживать необходимый формат, оно проверит, к какому классу относится определенная часть тела сообщения: если это необязательная часть, то она, конечно, отклоняется, а сообщение анализируется дальше, если же часть входит в обязательные, то отклоняется все сообщение целиком. Например, для терминала SIP потеря части тела, в которой содержится сообщение ISUP, совершенно не критична[25].

Примеры реализации данного механизма:

3.3.1 Поддержка ISUP необязательна

UA 2 принимает INVITE, независимо от того может он обработать ISUP или нет. Представлена диаграмма обмена сообщениями в между узлами в сети SIP:

```
UA1                UA2
  INVITE-->
    (Content-type:multipart/mixed;
    Content-type: application/sdp;
    Content-disposition: session; handling=required;
    Content-type: application/isup;
    Content-disposition: signal; handling=optional;)

                    <--18x
```

3.3.2 Поддержка ISUP предпочтительна

UA 2 не поддерживает ISUP и отклоняет запрос, посылая сообщение об ошибке 415 (Unsupported Media Type). UA 1 выбрасывает из запроса часть с ISUP и опять посылает сообщение, содержащее только информацию SDP и оно принимается UA 2. Представлена диаграмма обмена сообщениями в между узлами в сети SIP.

```
UA1                UA2
  INVITE--> (Content-type:multipart/mixed;
    Content-type: application/sdp;
    Content-disposition: session; handling=required;
    Content-type: application/isup;
    Content-disposition: signal; handling=required;)

                      <--415
                (Accept: application/sdp)

  ACK-->

  INVITE-->
  (Content-type: application/sdp)

                    <--18x
```

3.3.3 Поддержка ISUP обязательна для входящего звонка

UA2 не поддерживает ISUP и посылает сообщение об ошибке 415 (Unsupported Media Type). Тогда UA1 перенаправляет запрос на UA 3. Представлена диаграмма обмена сообщениями в между узлами в сети SIP:

UA1 UA2

INVITE--> (Content-type:multipart/mixed;
Content-type: application/sdp;
Content-disposition: session; handling=required;
Content-type: application/isup;
Content-disposition: signal; handling=required;)

<--415
(Accept: application/sdp)

ACK-->

UA1 UA3

INVITE--> (Content-type:multipart/mixed;
Content-type: application/sdp;
Content-disposition: session; handling=required;
Content-type: application/isup;
Content-disposition: signal; handling=required;)

3.4 Преобразование сигнальных протоколов ISUP и SIP

3.4.1 Общие принципы взаимодействия

Протокол SIP работает поверх протокола IP, разговор пользователей анализируется как мультимедийный сеанс связи, который включает передачу аудио данных.

ISUP работает в стеке протоколов ОКС №7 поверх подистемы MTP, и может функционировать на базе технологий IP [RFC 2960]. ISUP на самом деле предназначен для установления соединений и управления ими, а также для обслуживания сети.

Устройство, которое содержит модуль преобразования сообщений между протоколами ISUP и SIP называются Media Gateway Controller (MGC), также используется термин «softswitch» или «call agent». MGC имеет в себе логический интерфейс для того, чтобы осуществлять работы с обоими типами сетей, ISUP и SIP. Преобразование аудио информации из формата, принятого в сети SIP в формат СТОП берет на себя Media Gateway (MG) с магистральным интерфейсом E1/T1 (со стороны СТОП) и интерфейсом IP (со стороны сети IP). MGC и MG могут быть объединены физически в одно и тоже устройство или же располагаться отдельно[26].

MGC используют как связующее звено между СТОП и сетями SIP, так как вызовы из телефонной сети могут поступать на IP–телефоны и наоборот, а вызовы из СТОП могут проходить транзитом через сеть SIP.

Взаимодействие между этими двумя сетями основано на следующих принципах: инкапсуляции сообщений ISUP в тело запросов SIP и трансляции

части информации сообщения ISUP, необходимой для правильной маршрутизации, в заголовок запроса SIP.

Для сообщений ISUP, проходящих через сеть SIP, трансляция позволяет таким элементам сети SIP, как прокси–серверы, которые не работают непосредственно с сообщениями ISUP, правильно пересылать сообщение, основываясь при этом на данных, транслированных из сообщения ISUP в заголовок запроса SIP (это может быть номер вызываемого абонента).

3.4.2 Требования к протоколу SIP при взаимодействии с сетью СТОП

Для того, чтобы обеспечить преобразование сообщений из формата ISUP в SIP и наоборот, при этом, чтобы проходило правильно и без ошибок, обычно используются несколько различных механизмов, приведенных ниже. Если SIP UAC/UAS получает сообщение в том формате, который не поддерживает, то установление сеанса возможно, но при этом сценарий обмена сообщениями, скорее всего, будет отличаться от стандартного.

Процедуры прозрачной передачи сообщений ISUP необходимы для того, чтобы можно было позволить шлюзам использовать весь объем услуг, которые предоставляются существующей телефонной сетью при транзите сообщений СТОП через сеть SIP (СТОП-SIP-СТОП), запрос SIP должен транспортировать полезную нагрузку в виде инкапсулированного сообщения ISUP от шлюза к шлюзу.

4 Экспериментальное исследование методов взаимодействия

Основная задача протокола SIP-T заключается в «прозрачности» (понятности) при передаче сообщений ISUP по IP-сети. Данная задача осуществляется путём инкапсуляции сигнальных единиц ОКС-7 в сообщения SIP. Сообщение ISUP содержит информацию, которую невозможно отобразить в заголовках. Поэтому отображается информация в SIP-T лишь частично или отбрасывается, что является недостатком данного метода.

В работе производится исследование методов взаимодействия протоколов сигнализации и установления соединения для сетей IP-телефонии. При построении алгоритма работы переадресации собрана информация, касающаяся протокола SIP-T, его основных и дополнительных функций в соответствии с документами RFC комитета IETF. Раскрываются функциональные возможности элементов, взаимодействующих по данному протоколу, исследуются процедуры управления соединением. Приводятся примеры сценариев обмена сообщениями и их недостатки, такие как: некорректность перевода сообщения ISUP в SIP, в результате чего может произойти ошибка при установлении соединения.

В исследуемом сценарии начальной точкой является пользователь сети телекоммуникаций общего пользования, а конечной точкой – пользователь сети SIP.

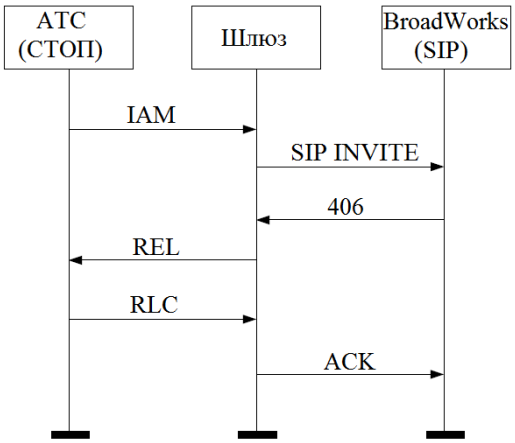

Рисунок 4.1 – Алгоритм установления соединения.

На рисунке 4.1 приведена схема организации взаимодействия для данного сценария. Требуется шлюз, который при получении сообщения от пользователя СТОП переводит его в SIP запрос, который посылается в сеть, но соединение установить не удается из-за того, что пользователь SIP не может распознать сообщение ISUP. Далее шлюз уведомляет пользователей о невозможности установления соединения.

Поэтому требование к сети IP-телефонии необходимо для возможности «прозрачности» команд для организации услуг относительно сети телекоммуникаций общего пользования. Традиционные телефонные услуги,

такие как: ожидание (call waiting), конференц-связь (conference), определитель номера (CLIP), антиопределитель номера (CLIR) и другие дополнительные виды обслуживания должны иметь возможность реализации с помощью системы сигнализации №7.

4.1 Исследование метода инкапсуляции

На рисунке 4.2 приведен пример сообщения INVITE при методе инкапсуляции.

```
INVITE sip:390039@10.55.9.29:5060;user=phone;transport=udp SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.29V5060-0-59
717006-1225961134-1305789491994-
From:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>;tag=1225961134
-1305789491994-
To:<sip:390039@10.55.9.29:5060;user=phone>
Call-ID:BW131811994190511-142793611?@10.55.9.6
CSeq:59717006 INVITE
Contact:<sip:10.55.9.6:5060>
P-Asserted-Identity:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>
Privacy:none
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept:multipart/mixed,application/media_control+xml,application/sdp
Supported:timer
Min-SE:600
Max-Forwards:70
Content-Type: multipart/mixed; boundary=SDP-ISUP-boundary
Content-Length:165
MIME-Version: 1.0

--SDP-ISUP-boundary
Content-Type: application/sdp
v=0
o=BroadWorks 154254420 1 IN IP4 10.55.9.24
s=-
c=IN IP4 10.55.9.24
t=0 0
m=audio 15848 RTP/AVP 8 0
a=ptime:20
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000

--SDP-ISUP-boundary
Content-Type: application/ISUP; version=ANSI
Content-Encoding: binary
1A 00 01 00 60 00 0A 06 0D 03 80 90 A2 07
03 10 18 27 85 31 48 0A 07 03 11 12 74 66 69
53 EA 01 00 00
--SDP-ISUP-boundary--
```

Рисунок 4.2 – Пример сообщения INVITE

Из рисунка 4.2 видно, что в стартовой строке указан тип запроса, адресат и номер версии протокола. В заголовке сообщения указаны номера вызывающего и вызываемого пользователей и уникальный номер звонка. Также видим, что в теле сообщения информация кодирована и это может привести к ошибке при переводе сообщения.

На рисунке 4.3 приведен пример ответа на запрос INVITE.

```
SIP/2.0 406 NOT ACCEPTABLE
Via: SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.29V5060-0-5
9717006-1225961134-1305789491994-
From: "animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>;tag=122596113
4-1305789491994-
To: <sip:390039@10.55.9.29:5060;user=phone>;tag=2f5c65609572011519132637
Call-ID: BW131811994190511-1427936117@10.55.9.6
CSeq: 59717006 INVITE
Server: CS2000_NGSS/9.0
k: 100rel,timer
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY,PRACK,UPDATE
Contact: <sip:390039@10.55.9.29:5060;transport=udp>
c: application/sdp
Content-Length: 251
```

Рисунок 4.3 – Пример ответа на запрос INVITE

Из рисунка 4.3 видно, что на запрос INVITE получен ответ с ошибкой 406 о недоступности установления соединения.

При методе инкапсуляции сообщение было некорректно интерпретировано прокси-сервером, в результате чего произошел отказ в обслуживании из-за неправильно переведенной адресной информации. Данный эпизод довольно часто встречается в сетях на стыке сетей SIP-T и ОКС-7. Если описать подробнее, то в шлюзах SIP-ISUP, сообщения ISUP ОКС-7 инкапсулируется в сообщение протокола SIP, при этом сохраняется только необходимая информация для обслуживания, чего недостаточно для прокси-сервера при передаче. Прокси-сервер принимает решения о продвижении запроса SIP дальше по сети, но не может правильно распознать ISUP. Поэтому считаем, что данный метод не надежен для взаимодействия ОКС-7 и SIP.

На рисунке 4.4 приведен алгоритм неуспешного установления соединения при методе инкапсуляции.

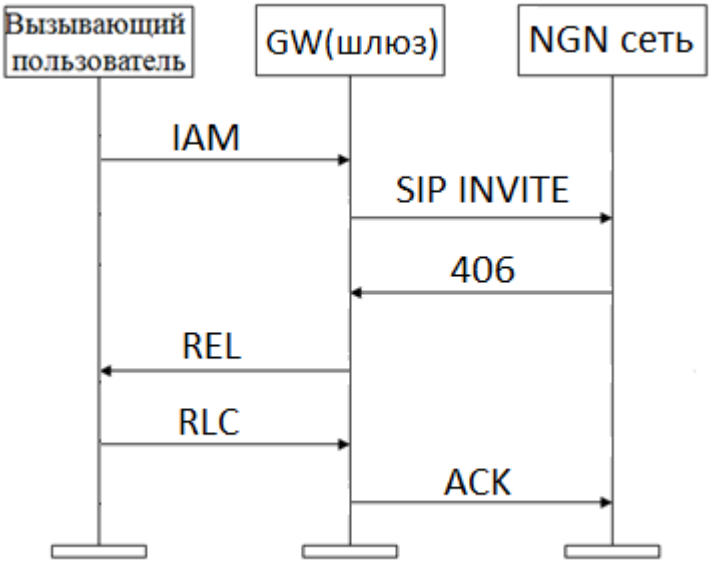

Рисунок 4.4 – Алгоритм неуспешного установления соединения

4.2 Исследование метода трансляции

SIP-T имеет 2-ой метод взаимодействия с ОКС-7 - трансляция информации из сообщений ОКС-7.

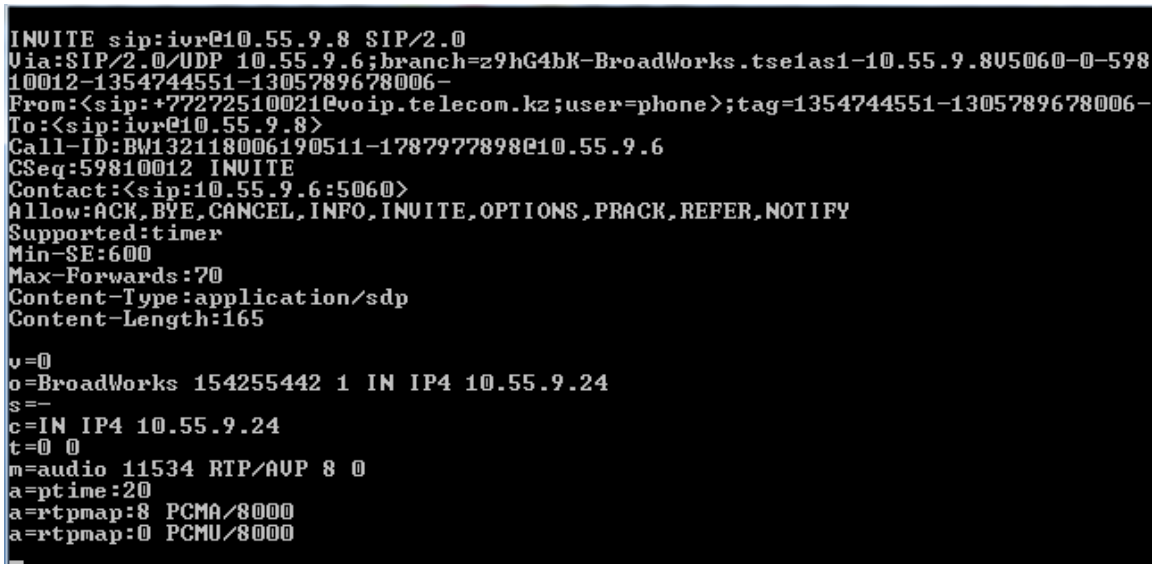

Рисунок 4.5 – Пример сообщения INVITE

Из рисунка 4.5 видно, что при методе трансляции информация в теле сообщения не кодируется и без каких-либо проблем может быть переведена дальше в сеть. Тем самым выполняется требование необходимости «прозрачности» команд для организации услуг относительно сети телекоммуникаций общего пользования.

На рисунке 4.6 показан пример успешного ответа на запрос INVITE.

Рисунок 4.6 – Пример ответа на запрос INVITE

Из рисунка 4.6 видно, что на запрос INVITE получен ответ – «200 ОК» об успешном установлении соединения.

При методе трансляции сообщение было корректно распознано сообщение прокси-сервером. Если описать подробнее, то в шлюзах SIP-ISUP, сообщения ISUP ОКС-7 транслируется в сообщение протокола SIP, при этом сохраняя только необходимую информацию для обслуживания. Прокси-сервер принимает решения о продвижении запроса SIP дальше по сети, правильно распознав ISUP. Поэтому считаем, что данный метод надежен для взаимодействия и подходит для взаимодействия общеканальной сигнализации №7 и протокола установления соединения. Это в свою очередь позволяет использовать протокол установления соединения к построению сетей IP-телефонии.

Алгоритм успешного установления соединения при методе трансляции по результатам прозвонки и полученным логам показан на рисунке 4.7.

Рисунок 4.7 – Алгоритм успешного установления соединения

При эксперименте переадресации по полученным логам прозвонки с номера 510021 на номер 390039 был построен алгоритм работы переадресации, (см. рисунок 4.8). Результаты (логи, листинг) приведен в Приложении А.

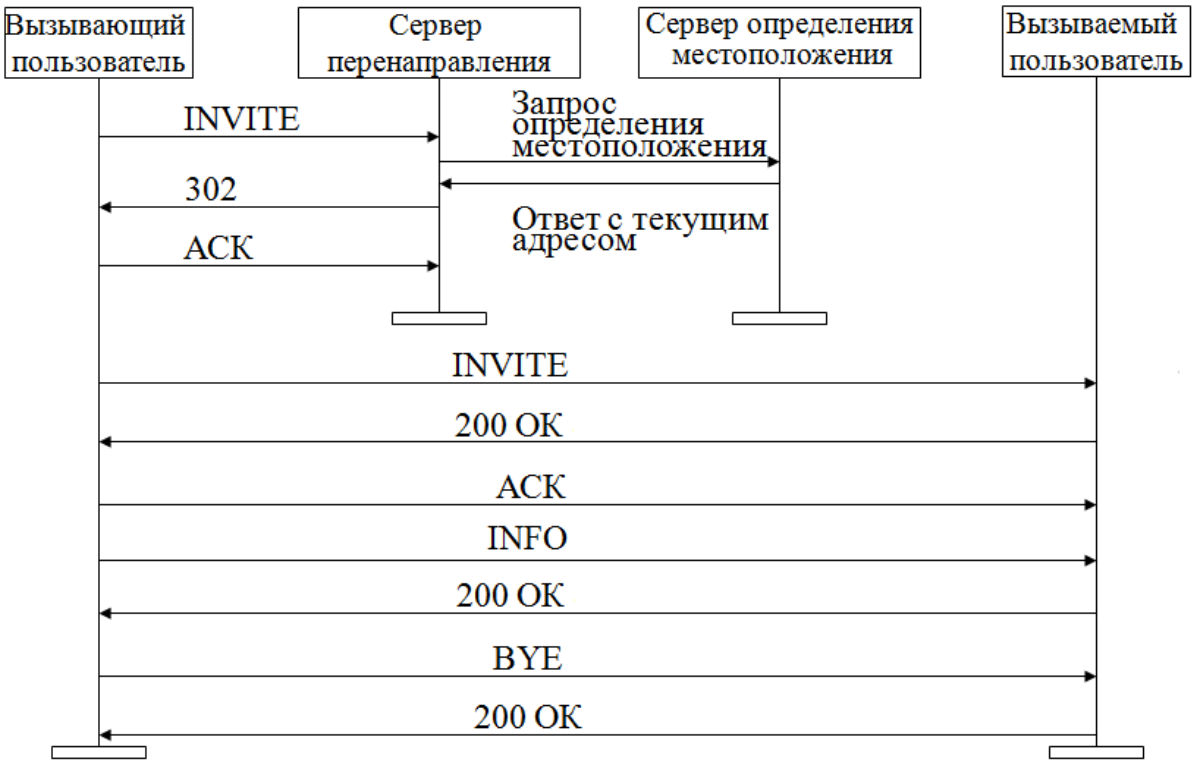

Рисунок 4.8 – Алгоритм работы переадресации.

5 Расчет сигнального трафика протокола SIP

Исходные данные для анализа собирались на сети одного из крупнейших российских операторов IP-телефонии. Объект, на котором собирались данные, в архитектуре протокола SIP представляет собой Full State SIP Proxy/Registrar/Redirect, то есть SIP-прокси сервер, участвующий во всех фазах установления/разрушения вызова (голос, видео, факс), сервер регистрации и сервер переадресации. Также данный объект реализует различные дополнительные виды обслуживания (ДВО) как традиционные для телефонной сети (удержание вызова, переадресация, ожидание вызова и др.), так и специфические для сети SIP (3-х сторонняя конференция, регистрация одного номера за несколькими устройствами, обратный вызов занятого абонента, передачи сообщений и др.). Среди абонентов, зарегистрированных на сервере, присутствуют как абоненты делового (бизнес) сектора, так и домашние абоненты. В качестве абонентских устройств используются как обычные аналоговые телефоны, так и цифровые телефоны с функцией передачи видео и сообщений. Все это делает сигнальный трафик весьма разнообразным и по своей структуре не похожим на сигнализацию в традиционных сетях связи.

Полученные данные представляют собой временные метки прихода различных сообщений SIP (INVITE, NOTIFY, OPTION и др.), взятые из трассировки, сделанной с помощью программы tcpdump. Точность временных отчетов - до 10^6 секунды. Данные на сети собирались в течение недели 24 часа в сутки. В итоге было собрано около 5 миллионов временных отметок. На рисунках 5.1-5.2 представлены графики зависимости количества сообщений протокола SIP от времени за различные периоды наблюдения: недельный (см. рисунок 5.1) и 6-ти часовой (см. рисунок 5.2).

В данной работе рассматривается трафик в максимальном масштабе времени до нескольких десятков секунд. Данный масштаб времени является особенно интересным, так как специфические свойства статистических характеристик протокола SIP проявляются именно на таких интервалах, а в масштабах недели трафик SIP выглядят почти также, как и трафик традиционной телефонии. К тому же методы борьбы с перегрузками, основанные на самоподобии трафика на небольших масштабах времени, являются наиболее эффективными, так как позволяют быстро реагировать на изменения нагрузки в сети.

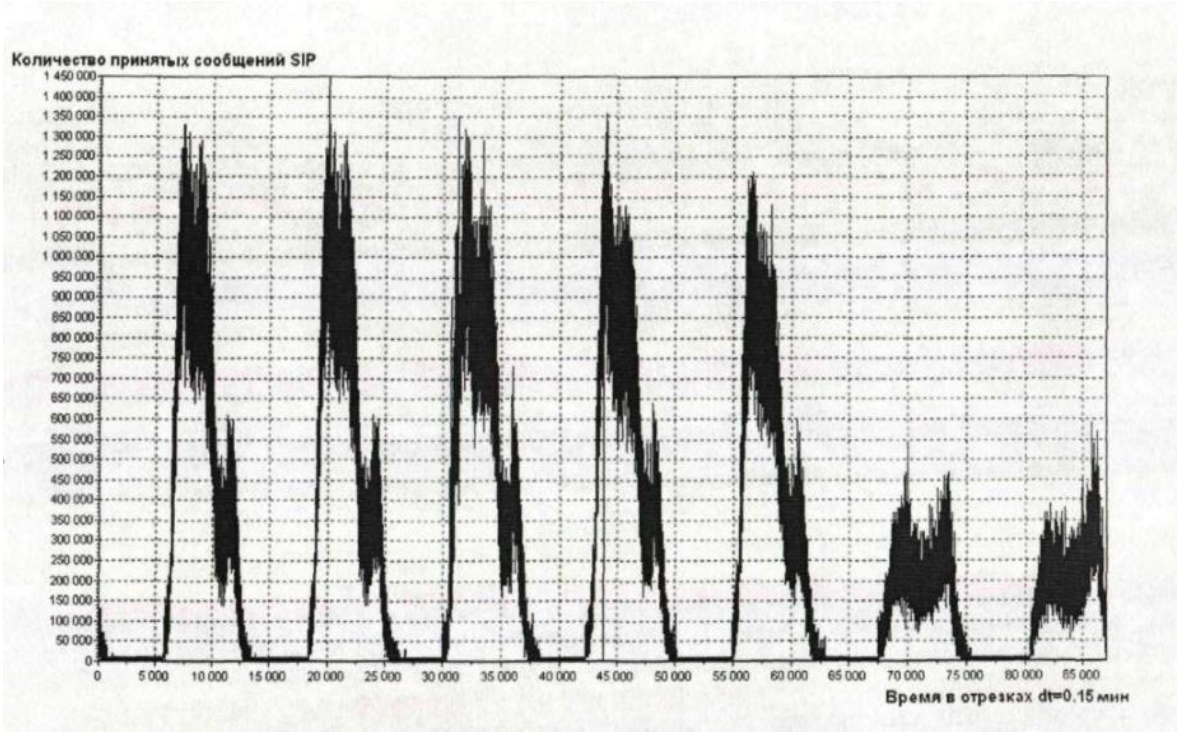

Рисунок 5.1 – Изменение количества сигнальных сообщений протокола SIP от времени за недельный период наблюдения

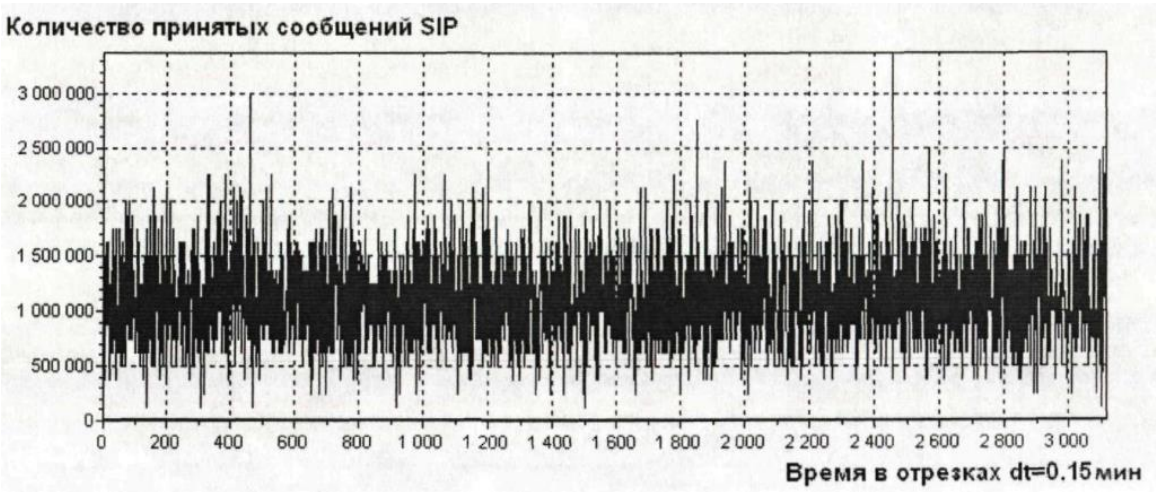

Рисунок 5.2 – Изменение количества сигнальных сообщений протокола SIP от времени за 6-ти часовой период наблюдения

5.1 Основные свойства самоподобных процессов

5.1.1 Определения дискретных свойств

Большинство свойств самоподобных процессов определяется особенностями их статистических характеристик (математическое ожидание, дисперсия, коэффициент корреляции). Поэтому необходимо для начала дать определения самоподобным процессам в широком и в узком смысле,

определить их основные статические характеристики, а также их специфические особенности.

Допустим, имеется исходный временной ряд $X(t) = (X_1 + X_2 + ...)$ для всех $t \in N=\{1,2,...\}$. Процесс X(t) - стационарный в широком смысле случайный процесс с математическим ожиданием $\mu = E[X(t)]$ и дисперсией $\sigma^2 = E[X(t)-\mu)^2]$. То есть математическое ожидание такого процесса постоянно, а автоковариация: $\gamma(t,k)= E[(X(t)- \mu)-(X(t + к) - \mu))]$ удовлетворяет условию:

$$\gamma(t,t+k)= \gamma(t,k), \quad (2.1)$$

где E - означает операцию усреднения (математическое ожидание). Из условия стационарности также следует, что коэффициент корреляции;

$r(k)= \gamma(k)/ \sigma^2$ и автоковариация не зависят от времени.

Для рассмотрения масштабной инвариантности введем агрегированный процесс $X(t)\text{-}X^{(m)}$ с уровнем агрегации равным m.

$$X^{(m)}(i)=1/m \sum_{t=m(i-1)+1} X(t), \text{ где } m,t \in N=\{1,2,\ldots\}, \quad (2.2)$$

Данный процесс получается из исходного путем усреднения по неперекрывающимся блокам размера т и представляет собой, по сути, менее детализированную копию исходного процесса. Через μ_m, $\sigma_m^2= \gamma_m(0)$ и γ_m обозначим соответственно мат ожидание, дисперсию и автоковариацию агрегированного процесса.

Определение: Процесс называется самоподобным в узком смысле с параметром $H=(0<H<1)$, если

$$X(t)^d=m^{1-H}X^{(m)}(t), \quad (2.3)$$

То есть процесс *X(t)* и нормализованный коэффициентом m^{1-H} процесс $X^{(m)}$ должны иметь одинаковые плотности распределения.

Определение: Процесс называется строго самоподобным в широком смысле с параметром $H=(1/2<H<1)$, если его автоковариация имеет вид:

$$\gamma(k)= \sigma^2/2((k+1)^{2H}-2k^{2H}+(k-1)^{2H}), \quad (2.4)$$

Для всех $k\geq 1$. В данном случае:

$$\gamma(k)= \gamma(k)_m, \quad (2.5)$$

Для любых $m \geq 1$.

Форма автоковариации (2.4) не случайна и подразумевает наличие долговременной зависимости.

Зная, что $\sigma^2(aX)=a^2\,\sigma^2(X)$, можно показать, что

$$\sigma^2_m = \sigma^2/m^\beta, \qquad (2.6)$$

где $0<\beta<1$; $\beta = 2-2H$.

Используемый в определениях параметр *H* - это так называемый параметр Херста, показывающей степень самоподобия. Более детально этот параметр будет рассмотрен далее.

5.1.2 Обработка исходных данных.

Для исследования наличия признаков самопободия в исходном временном ряде нам потребуется произвести его агрегирование, то есть приведение его к ряду с постоянным шагом т по шкале времени, где т является уровнем агрегации. Процедура происходит следующим образом: исходный ряд *X* разбивается на интервалы времени длительностью *m*. Каждый отчет нового агрегированного ряда будет являться отношением количества пришедших за данный интервал сообщений к длительности интервала т. В качестве исходного ряда возьмем ряд представленный на рисунке 5.2, далее его будем обозначать как *X*. Уровни агрегации *m* = 10 и 40 секунд. Агрегированные ряды $\boldsymbol{X^{(m)}}$ показаны на рисунках 5.3, 5.4 для соответствующих *m*.

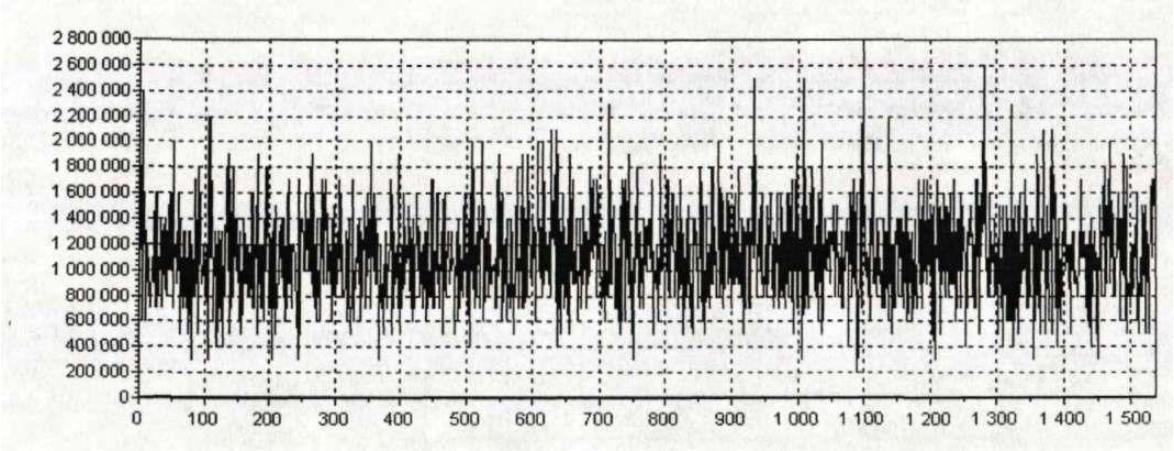

Рисунок 5.3 – Ряд $X^{(т)}$ для *m* = 10 секунд

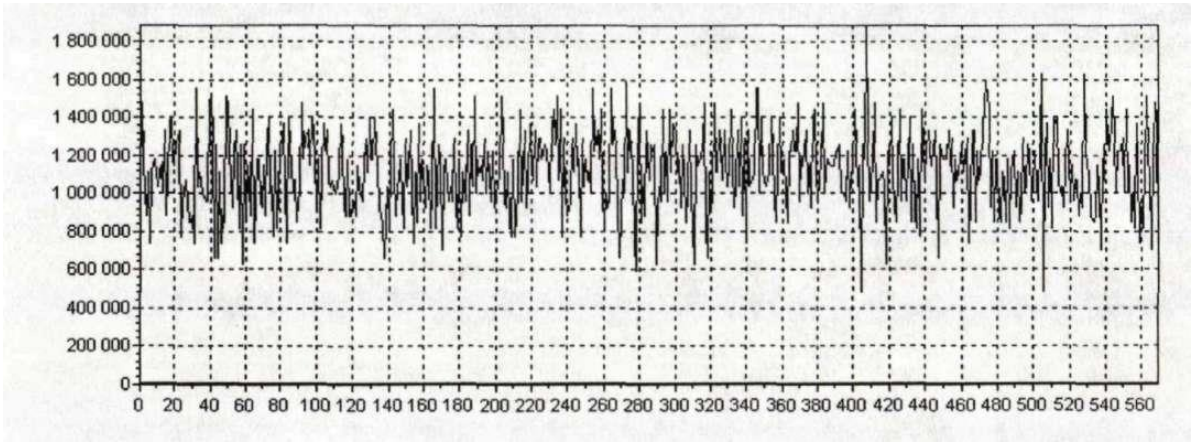

Рисунок 5.4 – Ряд $X^{(m)}$ для $m = 40$ секунд

Полученные ряды в дальнейшем будут использоваться для проверки наличия эффекта самоподобия в исследуемом трафике протокола SIP.

5.1.3 Анализ автокорреляционных функций

Долговременная зависимость или медленно убывающая зависимость (далее эти термины будут использоваться взаимозаменяемо) процесса $X(t)$ проявляется, когда его автокорреляционная функция $r(k)=\gamma(k)/\sigma^2$ убывает гиперболически (по степенному закону) так, чтобы:

$$\sum_{k=\infty} r^{(k)} = \infty, \tag{2.7}$$

Автокорреляционная функции (АКФ) $r(к)$ для процессов с долговременной (медленно убывающей) зависимостью LRD (Long Range Dependence) имеет вид:

$$r(k) = c_1 \cdot k^{\beta}, \; k \to \infty \tag{2.8}$$

В то время как для процессов с быстро убывающей зависимостью SRD (Short Range Dependence) та же функция имеет вид.

$$r(k) = c_2^{\,k}, \; k \to \infty \tag{2.9}$$

где c_1, c_2 - некоторые положительные константы, $0<\beta<1$, $\beta = 2-2H$.

Примеры долговременных зависимостей для разных значений параметра Херста H приведены на рисунке 5.5.

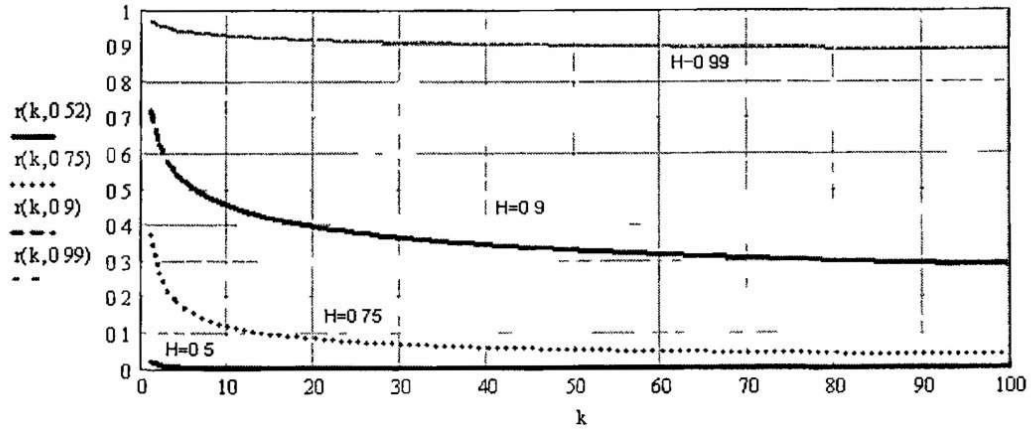

Рисунок 5.5 – Пример поведения автокорреляционной функции *r(к)* для различных *H=1-β/2*

Для обработанных временных рядов построим графики автокорреляционных функций. Для сравнения на каждом рисунке изобразим еще функции быстро и медленно убывающих зависимостей (SRD и LRD соответственно). Следует также заметить, что, не смотря на то, что в исследуемых временных рядах количество отчетов конечно и предельное условие несуммирования АКФ (см. рисунок 5.6) не может выполняться, наличие или отсутствие долговременной зависимости нас интересует только в исследуемых временных рамках.

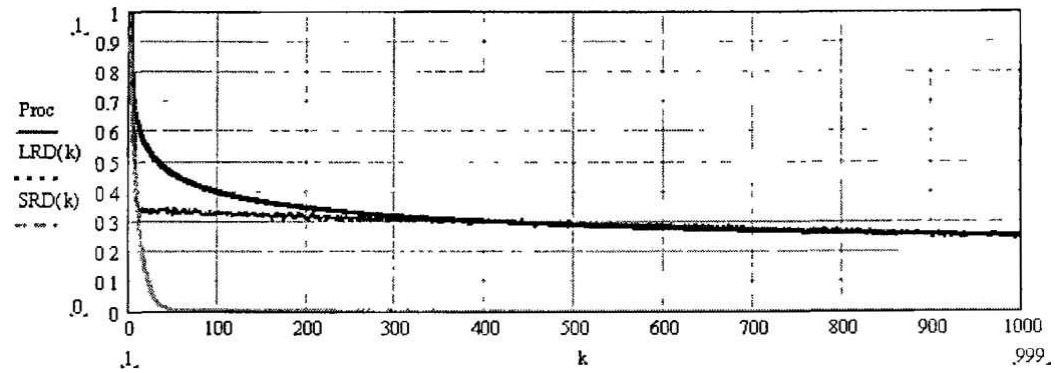

Рисунок 5.6 – Автокорреляционная функция исходного ряда и зависимостей LRD и SRD с параметрами $c_1 = c_2 = 1$, $\beta = 0.2$

Из рисунка видно, что *r(k)*исходного ряда практически совпадает с АКФ LRD, а при параметрах с, = 0.37 и β = 0.04 они полностью совпадают (см. рисунок 5.7).

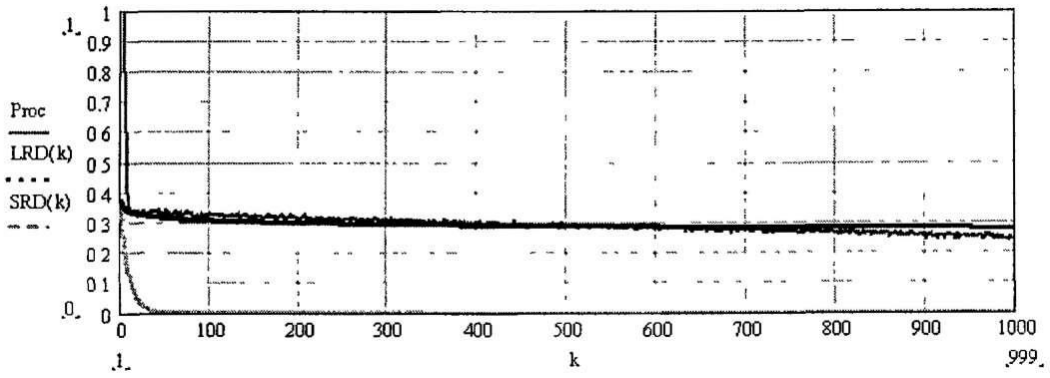

Рисунок 5.7 – Автокорреляционная функция исходного ряда и зависимостей LRD и SRD при $c_1 = c_2 = 0.37$, $\beta = 0.04$

Из приведенных выше графиков видно, что АКФ процессов убывает гиперболически, а не экспоненциально, как у SRD, и практически совпадает с АКФ медленно убывающей зависимости при определенных значениях коэффициентов c_1, c_2 и β.

5.1.4 Анализ дисперсии

Как уже отмечалось выше, дисперсия агрегированного процесса убывает медленнее, чем величина, обратная выборке агрегации (для достаточно больших значений m).

$$\sigma^2 \sim 1/m^{\beta}, \qquad (2.10)$$

Наличие медленно убывающей дисперсии легко протестировать. Достаточно нанести на log-log график зависимость дисперсии от величины т. В результате должна получиться прямая с отрицательным наклоном, меньшим единицы в широком диапазоне m.

Одним из важных свойств медленно убывающей дисперсии является то, что в случае классических статистических тестов, например вычисление доверительных интервалов, обычная мера среднеквадратического отклонения σ является ошибочной на величину, стремящуюся к бесконечности, с возрастанием размера выборки.

На рисунке 5.8 изображены графики зависимости логарифмов дисперсии исследуемого процесса (Var) и быстро убывающего процесса (Vr(m)) от логарифма m.

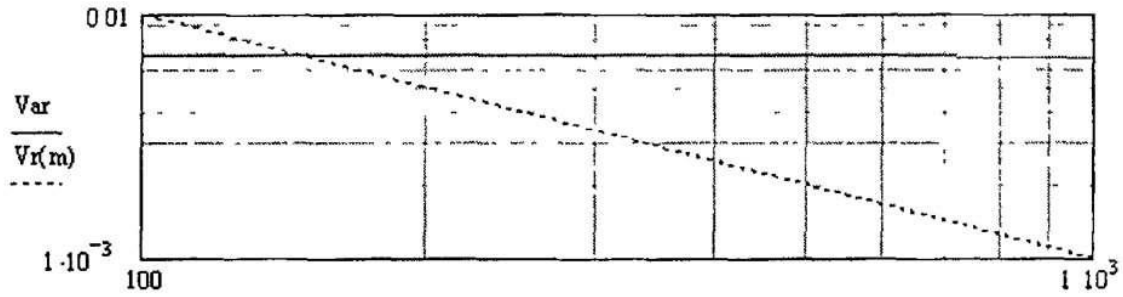

Рисунок 5.8 – Зависимость дисперсии исследуемого временного ряда от величины *m* на log-log графике

Из рисунка видно, что дисперсия исследуемого процесса убывает значительно медленнее, чем дисперсия кратковременно зависимого процесса, из чего можно сделать вывод, что исследуемый процесс имеет долговременную зависимость.

5.2 Параметр Херста и его оценка

Параметр Херста может являться мерой самоподобия процесса. Значение параметра $0.5 < H < 1$ определяют степень самоподобия. Чем ближе параметр H к 1, тем больше процесс самоподобен, то есть тем больше вероятность того, что если процесс возрастал/убывал в предыдущие промежутки времени, то он будет продолжать рост/убывание и дальше. В случае $H = 0.5$ можно говорить о полном отсутствии самоподобия, то есть приращения процесса на предыдущих шагах никак не повлияют на приращения в последующих шагах. В случае, если значения параметра лежат в пределах $0<H<0.5$, то вероятность того, что на следующем шаге процесс отклонится в сторону, противоположную той, в которую он отклонялся на предыдущем, тем выше, чем ближе параметр H к нулю.

5.2.1 R/S статистика

Отношение *R/S* было введено Гарольдом Херстом при изучении разливов реки Нил и было названо также нормированным размахом. Для заданного набора наблюдений $\{X_n, n \in N = \{1,2,...\}\}$ вводились следующие понятия:

- выборочное среднее $X(n)=1/n \sum_{i=1}^{n} Xi$;
- выборочная дисперсия $S^2(n)=1/n\sum_{i=1}^{n}[Xi - X]^2$;
- размах $R(n)= max(0,1,\Delta_1, \Delta_2... \Delta_n)-min(0,1,\Delta_1, \Delta_2... \Delta_n)$

где $\Delta_k=\sum_{i=1}^{k} Xi - kX, k=1,2...n.$

Соответственно отношение *R/S* имеет следующий вид:

$$\frac{R(n)}{S(n)} = \frac{max\Delta n - min\Delta n}{\sqrt{\sum_{i=1}^{n}[Xi - X]}}, \quad (2.13)$$

Гарольдом Херстом было показано, что для многих природных явлений данное отношение принимает вид:

$$E\left[\frac{R(n)}{S(n)}\right] \sim c\, n^H, n \to \infty, \quad (2.14)$$

где *c* - некоторая положительная константа, не зависящая от *n*.

Чтобы получить оценку параметра *H* надо, прологарифмировав обе части:

$$\log_E \left[\frac{R(n)}{S(n)}\right] \sim H \log(n) + \log(c), \quad (2.15)$$

построить график зависимости : от log(n) и используя метод наименьших квадратов, подобрать прямую линию, наклон которой и будет равен параметру *H* (см. рисунок 5.9).

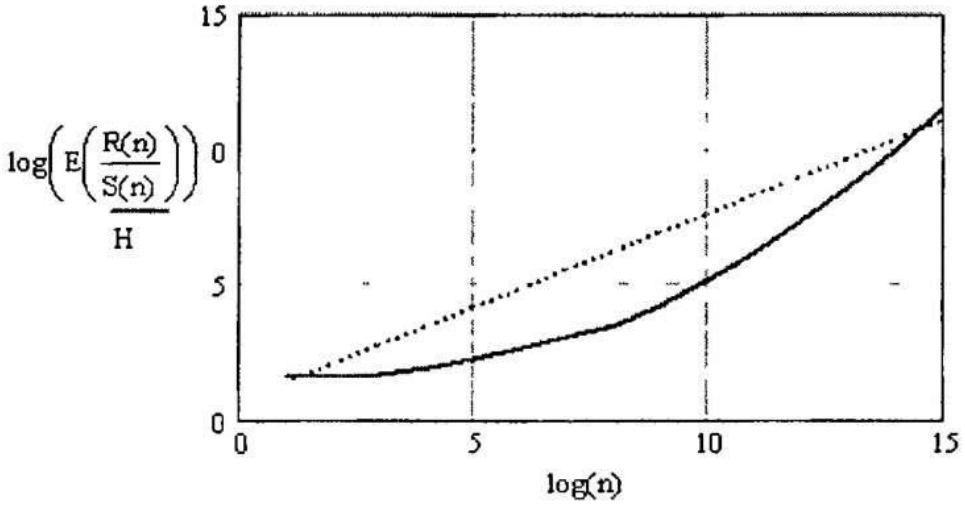

Рисунок 5.9 – Оценка параметра Хёрста *H* методом *R/S* статистики

Надо заметить, что данный метод дает лишь грубую оценку параметра Херста и может применяться лишь для оценки наличия свойства самоподобия в исследуемом процессе.

5.2.2 Дисперсионный анализ

Данный метод основан на свойстве дисперсии самоподобных процессов, описанном выше. В соответствии с ним дисперсия агрегированного процесса может быть вычислена следующим образом:

$$\sigma^2_m = \sigma^2/m^\beta \ , \qquad (2.16)$$

где $0 < \beta < 1$; $\beta = 2 - 2H$.

Прологарифмировав обе части равенства, получим:

$$\log(\sigma 2) = \log(\sigma 2) - \beta \log(m), \qquad (2.17)$$

Предполагая, что $\log(\sigma^2)$ - константа, не зависящая от m, можно найти значение $(-\beta)$ как наклон прямой, найденной по методу наименьших квадратов из точек, представляющих собой график зависимости $\log(\sigma^2_m)$ от log(m) (см. рисунок 5.9). Зная оценку β можно найти и значение $H = t - \beta/2$.

Стоит отметить, что данный метод, также как и *R/S* метод дает очень грубую оценку параметра H и может быть использован только для оценки наличия самоподобия в исследуемом процессе.

5.2.3 Оценка Виттла

Важной особенностью данного, не графического метода, является то, что он предполагает, что исследуемый процесс - самоподобен, но с неизвестным параметром *H* , и дает оценку этого параметра с определенной точностью. В данном методе используется спектральная плотность $\boldsymbol{S(w,H)}$ известной модели самоподобного процесса, ***fbm*** - фрактального броуновского процесса. Для оценки параметра *H* используется, так называемое, выражение Виттла:

Параметр Херста оценивается путем подбора его значения, которое минимизирует указанное выше выражение Виттла.

Существуют также множество других методов оценки параметра Херста, например, метод Эрби-Витча, метод абсолютных моментов, вейвлет анализ и метод дисперсии остатков.

5.2.4 Оценка параметра Херста

Все методы оценки параметра Херста, кроме оценки Эрби-Витча и Виттла, дают лишь приблизительную его оценку, так как все являются графическими и основываются на принципе аппроксимации, что может вносить значительные искажения в результаты. Поэтому, для этих методов даже в случае достаточно большой величины коэффициента корреляции, между исследуемым и аппроксимируемым процессами, нельзя утверждать, что параметр Хёрста посчитан правильно. Эти методы могут лишь позволить предположить, есть ли в анализируемых процессах долговременная зависимость.

Были получены оценки параметра Хёрста H исследуемых временных рядов большинством из указанных выше способов. В среднем оценка параметра Хёрста для всех исследуемых рядов находится в пределах $0.6 < H$

<0.8, что позволяет сделать вывод о том, что исследуемый трафик действительно является самоподобным, то есть обладает долгой памятью.

В данной главе был произведен статистический анализ трафика сигнального протокола SIP на предмет выявления в нем свойств самоподобия. Было проанализировано несколько сот тысяч пакетов в период наибольшей нагрузки на сети. Для анализа было произведено агрегирование исходного временного ряда на трех уровнях - 10 и 40 секунд. В результате было показано, что данный трафик обладает большинством из свойств самоподобного трафика. Получена оценка параметра Хёрста, характеризующего степень самоподобия трафика, которая находится в пределах $0.6<H<0.8$, что свидетельствует о достаточно сильной степени самоподобия.

Таким образом, на основе анализа параметра Херста, а также большинства самоподобных свойств, можно утверждать, что исследуемый сигнальный трафик протокола SIP является асимптотически (благодаря не бесконечной АКФ) самоподобным в широком смысле. Поскольку одним из основных свойств самоподобных процессов является долговременная зависимость, полученные выводы в дальнейшем могут быть использованы для прогнозирования трафика. Полученный прогноз может быть использован для целей борьбы с перегрузками в сетях протокола SIP.

Заключение

Для выполнения задач, поставленных в ходе диссертационной работы, были произведены исследования инкапсуляции, метода взаимодействия протоколов сигнализации и установления соединения для сетей IP-телефонии, и получены следующие основные результаты:

– подробно исследован алгоритм работы методов взаимодействия: инкапсуляции и трансляции;

– произведен анализ результатов исследования;

– приведены примеры сценариев обмена сообщениями;

– предложен наиболее подходящий метод для взаимодействия систем сигнализации и протокола установления соединения.

Показано, что в теле сообщения при методе инкапсуляции информация кодирована и это привело к ошибке при переводе сообщения, т.к. в приведенной схеме организации взаимодействия для данного сценария не выполняется требование к сети IP-телефонии, а именно – «прозрачность команд для организации услуг относительно сети телекоммуникаций общего пользования. При методе инкапсуляции сообщение было некорректно интерпретировано прокси-сервером, в результате чего произошел отказ в обслуживании из-за неправильно переведенной адресной информации. Данный эпизод довольно часто встречается в сетях на стыке сетей SIP-T и ОКС-7 и данный метод не надежен для взаимодействия ОКС-7 и SIP.

При методе трансляции информация в теле сообщения не кодируется и без каких-либо проблем может быть переведена дальше в сеть, как показано в приведенных сценариях. Тем самым выполняется требование необходимости «прозрачности» команд для организации услуг относительно сети телекоммуникаций общего пользования.

Проведённое исследование и полученные результаты несомненно имеют огромную практическую значимость. Поскольку, метод трансляции подходит для взаимодействия общеканальной сигнализации №7 и протокола установления соединения. Это в свою очередь позволяет использовать протокол установления соединения к построению сетей IP-телефонии.

Список литературы

1 Росляков А.В., Общеканальная система сигналиации 7 М. Эко-Трендз, 1999.

2 Росляков А.В., Сети и системы связи, 2002.

3 Толковый словарь по системам, средствам и услугам связи / Под ред. В.А. Докучаева. М.: Радио и связь, 2003. 548 с.

4 Сети электросвязи / Г.Б. Давыдов, М.: Связь, 1977. 360 с.

5 Иванова О.Н., Телефония в датах: Справ. М.: Инсвязьиздат, 2006.

6 Шварц М., Сети связи: протоколы, моделирование и анализ: В 2 т. Т. 1. М.: Наука, 1992. 276 с.

7 Шварц М., Сети связи: протоколы, моделирование и анализ: В 2 т. Т. 2. М.: Наука, 1992. 276 с.

8 Олифер В.Г., Олифер Н.А., Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 1999. 672 с.

9 Мартин Дж., Сети связи и ЭВМ. Ч. 1 / Пер. с англ. под ред. В.Н. Рогинского. М.: Связь, 1974. 230 с.

10 Автоматическая коммутация: Учеб. Для вузов / О.Н. Иванова, М.Ф. Копп, З.С. Коханова, Г.Б. Метельский; Под ред. О.Н. Ивановой. М.: Радио и связь, 1988. 624 с.

11 Рекомендации МСЭ-Т Е-164. The international public telecommunication numbering plan.

12 Левин Л.С., Плоткин М.А., Цифровые системы передачи информации. М.: Радио и связь, 1982. 261 с.

13 Ли У.К., Техника подвижных систем связи. Москва.: Радио и связь, 1985. 392 с.

14 Беллами Дж., Цифровая телефония / Пер. с англ. под ред. А.Н. Берлина, Ю.Н. Чернышова. М.: Эко-Трендз, 2004. 640 с.

15 Слепов Н.Н., Синхронные цифровые сети SDH. М.: Эко-Трендз, 1988, 148 с.

16 Гольдштейн Б.С., Протоколы сети доступа. М.: Радио и связь, 1999. 317 с.

17 Гольдштейн Б.С., Сигнализации в сетях связи. М.: Радио и связь, 1997. 423 с. // Электронная версия на сайте:
http://knowledge.allbest.ru/radio/3c0b65625a2ac78a4d43a89521206d37_0.html

18 Ликвиц Б.С., Пшеничников А.П., Харкевич А.Д., Теория телетрафика.

19 Росляков А.В., Общеканальная система сигнализации ОКС №7. М.: Эко-Трендз, 1999. 170 с. // Электронная версия на сайте:
http://www.osp.ru/data/www2/nets/1996/07/15.htm

20 Клейнрок Л., Теория массового обслуживания: Пер. с англ. М.: Машиностроение, 1979. 600 с.

21 Гольдштейн Б.С., Ехриелъ И.М., Рерле Р.Д., Стек протоколов ОКС-7. Подсистема MTP. – М.: Радио и связь, 2003. // Электронная версия на сайте: http://knowledge.allbest.ru/radio/3c0b65625a2ac78a4d43a89521206d37_0.html

22 Гольдштейн Б.С., Системы коммутации: Учебник для вузов. 2-ое издание. – СПб: БХВ – Санкт-Петербург, 2004.

23 Гольдштейн Б.С., Ехриелъ И.М., Рерле Р.Д., Стек протоколов ОКС-7. Подсистема SCCP. – СПб: БХВ – Санкт-Петербург, 2006. // Электронная версия на сайте: http://knowledge.allbest.ru/radio/3c0b65625a2ac78a4d43a89521206d37_0.html

24 Гольдштейн Б.С., Ехриелъ И.М., Рерле Р.Д., Стек протоколов ОКС-7. Подсистема ISUP. – СПб: БХВ – Санкт-Петербург, 2003. // Электронная версия на сайте: http://knowledge.allbest.ru/radio/3c0b65625a2ac78a4d43a89521206d37_0.html

25 Гольдштейн Б.С., Протокол SIP. Справочник. – СПб.: БХВ – Санкт-Петербург, 2005. 456 с. // Электронная версия на сайте: http://www.scriru.com/15/SIP-SIPT74838788227.php

26 Гольдштейн Б.С., IP телефония – М.: Радио и связь, 2001. 336 с.

27 Айтбай Тимур, Сборник статей АУЭС, 2 том, 2014. 75-77 с.

Приложение А

Листинг(лог) прозвонки

INVITE sip:390039@10.55.21.67:5060;user=phone SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.21.67V5060-0-59810005-971371182-1305789677993-
From:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>;tag=971371182-1305789677993-
To:<sip:390039@10.55.21.67:5060;user=phone>
Call-ID:BW132117993190511137829969 7@10.55.9.6
CSeq:59810005 INVITE
Contact:<sip:10.55.9.6:5060>
P-Asserted-Identity:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>
Privacy:none
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Supported:timer
Min-SE:600
Max-Forwards:70
Content-Type:application/sdp
Content-Length:165

v=0
o=BroadWorks 154255442 1 IN IP4 10.55.9.24
s=-
c=IN IP4 10.55.9.24
t=0 0
m=audio 11534 RTP/AVP 8 0
a=ptime:20
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000

****

SIP/2.0 302 Moved temporarily
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.21.67V5060-0-59810005-971371182-1305789677993-
From:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>;tag=971371182-1305789677993-
To:<sip:390039@10.55.21.67:5060;user=phone>
Call-ID:BW132117993190511137829969 7@10.55.9.6
CSeq:59810005 INVITE
Contact:<sip:390039@10.55.9.29:5060;transport=udp;user=phone;net-ind=InterNetwork>;q=0.5
Content-Length:0

****

ACK sip:390039@10.55.21.67:5060;user=phone SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.21.67V5060-0-59810005-971371182-1305789677993-

From:"animedia1 am1"<sip:+77272510021@voip.telecom.kz;user=phone>;tag=971371182-1305789677993-
To:<sip:390039@10.55.21.67:5060;user=phone>
Call-ID:BW132117993190511137829969 7@10.55.9.6
CSeq:59810005 ACK
Max-Forwards:70
Content-Length:0

****

INVITE sip:ivr@10.55.9.8 SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810012-1354744551-1305789678006-
From:<sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To:<sip:ivr@10.55.9.8>
Call-ID:BW132118006190511-1787977898@10.55.9.6
CSeq:59810012 INVITE
Contact:<sip:10.55.9.6:5060>
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Supported:timer
Min-SE:600
Max-Forwards:70
Content-Type:application/sdp
Content-Length:165

v=0
o=BroadWorks 154255442 1 IN IP4 10.55.9.24
s=-
c=IN IP4 10.55.9.24
t=0 0
m=audio 11534 RTP/AVP 8 0
a=ptime:20
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000

****

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810012-1354744551-1305789678006-
From: <sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To: <sip:ivr@10.55.9.8>;tag=1882437732
Call-ID: BW132118006190511-1787977898@10.55.9.6
CSeq: 59810012 INVITE
Contact: <sip:10.55.9.8:5060>
Allow: INVITE, ACK, BYE, INFO, CANCEL
Content-Type: application/sdp
Content-Length: 138

```
v=0
o=BroadWks 2904442 0 IN IP4 10.55.9.8
s=Media Server SDP
c=IN IP4 10.55.9.8
t=0 0
m=audio 10366 RTP/AVP 8
a=rtpmap:8 PCMA/8000

**********

ACK sip:10.55.9.8:5060 SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-
59810012A1354744551-1305789678006-
From:<sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To:<sip:ivr@10.55.9.8>;tag=1882437732
Call-ID:BW132118006190511-1787977898@10.55.9.6
CSeq:59810012 ACK
Contact:<sip:10.55.9.6:5060>
Max-Forwards:70
Content-Length:0

**********

INFO sip:10.55.9.8:5060 SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810013-
1354744551-1305789678006-
From:<sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To:<sip:ivr@10.55.9.8>;tag=1882437732
Call-ID:BW132118006190511-1787977898@10.55.9.6
CSeq:59810013 INFO
Contact:<sip:10.55.9.6:5060>
Max-Forwards:70
Content-Type:application/mediaservercontrol+xml
Content-Length:374

<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0-bw">
 <request>
  <play>
   <prompt>
    <audio url="http://10.55.9.6/media/en/TrtOutCallRestrict.wav"/>
    <audio url="http://10.55.9.6/media/en/silence10s.wav"/>
    <audio url="http://10.55.9.6/media/en/TrtOutCallRestrict.wav"/>
   </prompt>
  </play>
 </request>
</MediaServerControl>

**********
```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810013-1354744551-1305789678006-
From: <sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To: <sip:ivr@10.55.9.8>;tag=1882437732
Call-ID: BW132118006190511-1787977898@10.55.9.6
CSeq: 59810013 INFO
Contact: <sip:10.55.9.8:5060>
Content-Length: 0

****

BYE sip:10.55.9.8:5060 SIP/2.0
Via:SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810014-1354744551-1305789678006-
From:<sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To:<sip:ivr@10.55.9.8>;tag=1882437732
Call-ID:BW132118006190511-1787977898@10.55.9.6
CSeq:59810014 BYE
Max-Forwards:70
Content-Length:0

****

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.55.9.6;branch=z9hG4bK-BroadWorks.tse1as1-10.55.9.8V5060-0-59810014-1354744551-1305789678006-
From: <sip:+77272510021@voip.telecom.kz;user=phone>;tag=1354744551-1305789678006-
To: <sip:ivr@10.55.9.8>;tag=1882437732
Call-ID: BW132118006190511-1787977898@10.55.9.6
CSeq: 59810014 BYE
Contact: <sip:10.55.9.8:5060>
Content-Length: 0