**BC/NW 2018 № 2 (33):8.2**

**ИССЛЕДОВАНИЕ МЕТОДОВ КОНТРОЛЯ СОСТОЯНИЯ ЦИФРОВЫХ КАНАЛОВ СВЯЗИ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ**

Прохоров А.М.

Современный этап политических, военных, экономических и иных процессов в мире характеризуется высоким уровнем нестабильности.

Роль и место России в современном мире в значительной степени определяется ее геополитическим, экономическим и военным потенциалом. Создание новейшего высокоэффективного оружия является одним из главных факторов, сдерживающих желания агрессоров завладеть территориальными, сырьевыми, природными ресурсами. В первую очередь это относится к оружию оборонительного характера, и в частности к средствам и системам воздушно-космической обороны (ВКО) страны.

Современные системы ВКО представляют собой сложные территориальные информационные системы жесткого реального масштаба времени. Радиус действия таких систем составляет до двух-трех тысяч километров. Время реакции системы (от момента обнаружения цели до приема кодового блока по этой цели на командном пункте зенитно-ракетных войск) не превышает нескольких единиц или десятков миллисекунд.

Одними из основных составляющих коммуникационных подсистем в сложных территориальных информационно-управляющих системах ВКО, обеспечивающих взаимодействие комплексов в системах, являются:

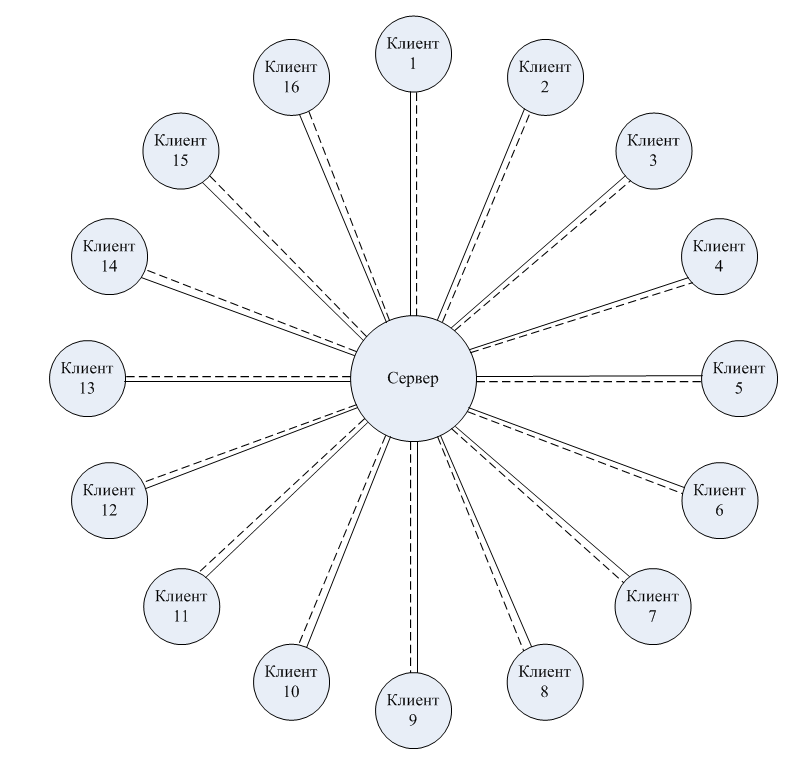
* система автоматизированного обмена данными реального масштаба времени между объектами;
* система оперативно-командной (речевой) связи;
* система автоматизированного документального обмена оперативно-тактической и командно-сигнальной информацией;
* система визуального обмена между операторами (командирами) объектов системы (система видео обмена и видеоконференций);
* система криптозащиты и имитационной защиты сигналов и данных, передаваемых по открытым каналам связи.

**Постановка задачи**

В настоящее время в ВКО происходит переход от аналоговой связи к цифровой связи. В цифровых каналах связи вероятность ошибки намного меньше, по сравнению с аналоговыми каналами, и оценивается примерно в 10-8 [7]. Но, тем не менее, ошибки имеют место быть и при относительно небольшой вероятности. Также стоит учитывать тот факт, что в некоторых условиях могут создаваться дополнительные помехи, что сказывается на качестве передачи данных вплоть до полного прекращения обмена [8]. Исходя из этого, возникает проблема отсутствия надежности передачи данных в рассматриваемых системах. Чтобы минимизировать риск прекращения обмена в рассматриваемых системах применяются резервные каналы связи. Поэтому возникает необходимость контроля состояния цифровых каналов связи. При правильной организации контроля состояния каналов связи можно своевременно принять меры для восстановления качественной передачи данных, либо перейти на резервный канал.

Также из-за жесткой привязки систем ВКО к реальному времени необходимо, чтобы контроль состояния каналов связи не вносил задержки в передачу данных, что также является проблемой.

Далее перейдем к анализу объекта. Рассматриваемая в данной работе модель организации сети передачи данных по цифровым каналам связи представлена на рисунке 1. Данная модель приближенно описывает ПВО и ПРО Москвы [4].



**Рис. 1.** Модель организации сети передачи данных

Обозначения:

- основной канал связи

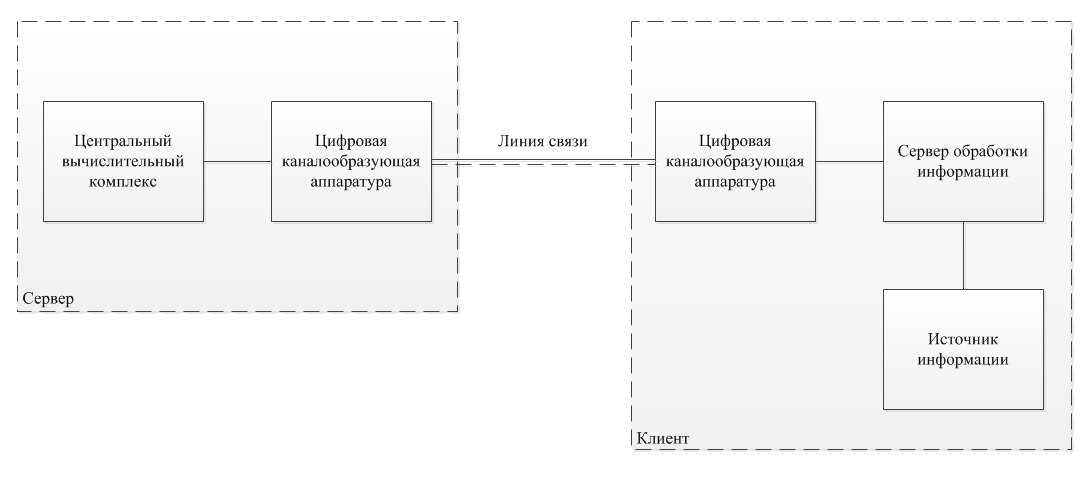
- резервный канал связи

Протяженность каналов связи 100-150 км.

Рассматриваемая сеть основана на стеке протоколов UDP/IP. Канальный уровень основан на сервисе без подтверждений и без установки соединения.

В представленной модели под клиентом понимается совокупность следующей аппаратуры: источник информации (радиотехническая станция), сервер обработки информации и цифровая каналообразующая аппаратура. Клиентская сторона обнаруживает объекты наблюдения, находящиеся в его зоне, и отправляет информацию о них на серверную сторону. Под сервером понимается информационная система (центральный вычислительный комплекс и цифровая каналообразующая аппаратура), принимающая и обрабатывающая данные от клиентов. Под каналом связи (как основного, так и резервного) понимается комплекс технических средств и среды распространения (линия связи), обеспечивающих передачу сигнала электросвязи в полосе частот и скоростью, характерных для данного канала

Структура цифрового канала связи (как основного, так и резервного) представлена на рисунке 2.



**Рис. 2.** Цифровой канал связи

Подводя итог, можно сказать, что в данных системах важно передавать данные надежно и с минимально возможной задержкой.

Целью работы является повышение надежности передачи данных в цифровых каналах связи за счет адаптивного включения резервного канала связи..

Для достижения цели необходимо решить следующие задачи:

* оценка качества цифровых каналов связи в реальном времени;
* разработка алгоритмов для сбора сетевого трафика;
* разработка алгоритмов для анализа сетевого трафика;
* практическая реализация разработанных алгоритмов.

**Сравнение существующего метода контроля качества с отключением канала с предлагаемым методом**

*Метод контроля качества с отключением канала*

Измерения с отключением канала предусматривают, что канал не используется в процессе измерений для передачи реального цифрового трафика. В этом случае в качестве источника и приемника двоичного сигнала используются анализаторы цифрового канала.

При измерениях с отключением канала сигнал передается в виде тестовой последовательности, которая на другом конце канала (приемник) принимается и затем проводится анализ ошибок, вносимых каналом. Для проведения измерений анализатор приемника должен обеспечивать предсказание структуры последовательности, т.е. требуется так называемая синхронизация тестовой последовательности. Для измерений используются разные тестовые последовательности, фиксированные и псевдослучайные, с различными алгоритмами синхронизации тестовой последовательности. Измерения с отключением канала - это единственный метод анализа параметров бинарного цифрового канала с точностью до единичной битовой ошибки. Это гарантируется принципом сравнения реальной принятой последовательности битов с предсказанной, которая, в свою очередь, точно совпадает с генерируемой последовательностью.

*Предлагаемый метод, основанный на алгоритме «Скользящее окно»*

Одним из методов без отключения канала является алгоритм «скользящее окно» [3]. Суть скользящего окна заключается в том, что каждый из n подряд следующих выделенных интервалов имеет собственный весовой коэффициент Kn. При накоплении определённого количества данных для нового интервала, данные самого старого из интервалов удаляются, так что при вычислении скользящего среднего всегда учитываются результаты только n последних интервалов.

Результат Kкач по методу взвешенного скользящего среднего вычисляется по формуле:

, (3)

где kn– весовой коэффициент интервала, Nn ош – количество ошибочно принятых кодограмм в интервале n, а Nn общ– общее количество кодограмм в интервале n, ожидаемых для принятия.

Если N1 общ = N2 общ = Nn общ= Nобщ, то формула преобразуется в

(4)

В данных формулах под кодограммами понимаются блоки данных алгоритма «Аккорд», применяющегося в ПВО. Ниже рассмотрим краткое описание формата кодограмм данного алгоритма.

Структура кодограммы приведена на рис. 5. Контрольные разряды образуются путем деления информационного блока, включая служебные разряды, блок данных и разряд решающей обратной связи (РОС), на образующий полином вида:

F(x) = x16 + x12 + x5 + 1 (5)

|  |  |  |  |
| --- | --- | --- | --- |
| СР | Блок данных | РОС | Контрольные разряды |
| 4 разряда | 144 разряда | 1 разряд | 16 разрядов |

**Рис. 5.** Формат кодограмм алгоритма «Аккорд»

**-** СР – служебные разряды;

**-** Блок данных – информационная часть кодограммы;

**-** РОС – признак решающей обратной связи.

Служебные разряды вместе с признаком РОС определяют тип кодограммы, показанного на рис. 6.

|  |  |  |
| --- | --- | --- |
| Значения разрядов | | Тип кодограммы |
| СР | РОС |
| 0101 | 1 | комбинация фазирования (Ф1 или Ф2) |
| 010х | 0 | комбинация покоя (х – произвольное состояние) |
| zzz0 | 0 | информационный блок, при этом значения zzz  определяют код задержки при повторной передаче |

**Рис. 6.** Типы кодограмм

Вычисление количества ошибок предлагается выполнять следующим образом: с некоторой периодичностью клиент будет передавать фиксированное число P блоков данных (если количество информационных блоков данных будет меньше P, то необходимо добавить контрольные блоки данных до числа P). Сервер будет ожидать принятия P блоков данных и в случае, если получено менее ожидаемого числа, то можно легко посчитать количество потерянных блоков данных и, следовательно, оценить качество канала:

, (6)

где Р – максимальное число объектов наблюдения, I – число полученных кодограмм от радиолокатора, K – число кодограмм, необходимых для формирования N кодограмм для отправки (K ϵ [0;N]).

Серверная сторона принимает и обрабатывает кодограммы следующим образом:

, (7)

где Nош – число потерянных кодограмм, N – общее число кодограмм, Nпрн – число принятых кодограмм.

Так как на транспортном уровне применяется протокол UDP, а на канальном уровне используется сервис без подтверждений и без установки соединения, данный метод позволяет оценивать состояние канала связи без отключения канала.

*Сравнение методов по основным характеристикам* приводится в таблице 1.

Таблица 1. Сравнение методов

|  |  |  |
| --- | --- | --- |
|  | Метод с отключением канала | Метод без отключения канала, основанный на алгоритме «скользящее окно» |
| Возможность передачи данных во время оценки качества канала | нет | да |
| Возможность применения метода в системе реального времени | нет | да |
| Точность метода | высокая | средняя |
| Реакция на изменение качества канала | очень низкая | высокая |
| Необходимость синхронизации | необходима | необходима |
| Нужно ли дополнительное оборудование | нужно | не нужно |

Как видно из таблицы 1, предлагаемый метод без отключения канала, основанный на алгоритме «скользящее окно», выглядит более предпочтительным по сравнению с методом с отключением канала.

**Эксперименты по тестированию разработки**

Эксперименты проводился на внутреннем сетевом интерфейсе (LOOPBACK) одного компьютера и на двух компьютерах, находящихся в локальной сети. Проведено по 4 эксперимента:

1. отправление клиентской стороной числа кодограмм, равное максимальному числу объектов наблюдения. В этом случае симулируется «идеальные» условия, при которых клиентская сторона работает постоянно, и, в случае передачи через внутренний интерфейс, серверная сторона должна принять все отправленные кодограммы;
2. отправление клиентской стороной числа кодограмм, равное максимальному числу объектов наблюдения, с прекращением работы клиентской стороны. В этом случае симулируются условия полного отсутствия канала связи путем прекращения отправки кодограмм клиентской стороной. В данном случае серверная сторона должна моментально определять отсутствие приема кодограмм;
3. отправление клиентской стороной числа кодограмм, равное 10% от максимального числа объектов наблюдения. В этом случае симулируются условия частичной потери кодограмм при передаче по каналу связи. В данном случае серверная сторона должна определить частичные потери кодограмм;
4. отправление клиентской стороной числа кодограмм, равное максимальному числу объектов наблюдения за вычетом некоторого случайного числа. В этом случае симулируются приближенные случайные условия воздействия помех на канал связи. В данном случае серверная сторона должна определять все потерянные кодограммы.

Во всех экспериментах ширина окна принималась равной 10, а длина окна принималась равной 1 секунде. Каждый эксперимент проводился в течение 5 минут.

*Проведение эксперимента на внутреннем сетевом интерфейсе LOOPBACK*

Отправление клиентской стороной числа кодограмм, равное максимальному числу объектов наблюдения.

В данном эксперименте были установлены следующие параметры работы программы:

* Р = 500;
* IP-адрес:порт серверного сокета: INADDR\_ANY:3425;
* IP-адрес:порт клиентского сокета: INADDR\_LOOPBACK:3425.

Результаты эксперимента представлены на рисунке №.Х

Рис. 3-1Эксперимент № 1 на внутреннем интерфейсе

Из рисунка 3-1 видно, что серверная сторона приняла все отправленные кодограммы, как и ожидалось. Также необходимо отметить, что начальное нулевое качество канала здесь и на графиках ниже объясняется накоплением статистики для вычисления качества. Время накопления статистики равно произведению ширины окна на длину окна.

Отправление клиентской стороной числа кодограмм, равному максимальному числу объектов наблюдения, с прекращением работы клиентской стороны.

В данном эксперименте были установлены такие же параметры, как и в предыдущем. Отличие состояло в принудительной остановке работы клиентской стороны 6 раз в разные моменты времени. Результаты эксперимента представлены на рисунке 3-2.

Рис. 3-2 Эксперимент № 2 на внутреннем интерфейсе

Из рисунка 3-2 видно, что серверная сторонаобнаружила все 6 отключений клиента (отключения происходили в следующие моменты времени: 20:41:09, 20:41:33, 20:42:09, 20:42:50, 20:43:31, 20:43:47), что отразилось на качестве канала. В данном случае можно наблюдать преимущество метода скользящего окна, заключающегося в моментальном определении приема кодограмм. При возобновлении передачи качество канала начинает увеличиваться, достигая максимума (при отсутствии очередных потерь).

Отправление клиентской стороной числа кодограмм, равному 10% от максимального числа объектов наблюдения.

В данном эксперименте, в отличие от предыдущих, параметру Р было присвоено значение, равное 450. Результаты эксперимента представлены на рисунке 3-3

Рис. 3-3. Эксперимент № 3 на внутреннем интерфейсе

Из рисунка 3-3 видно, что серверная сторона определяла частичные потери кодограмм на всем периоде проведения эксперимента.

Отправление клиентской стороной числа кодограмм, равному максимальному числу объектов наблюдения за вычетом некоторого случайного числа.

В данном эксперименте, в отличие от предыдущих, из параметра Р вычиталось случайное число в диапазоне от 0 до 200. Результаты эксперимента представлены на рисунке 3-4

Рис. 3-4.Эксперимент № 4 на внутреннем интерфейсе

Из рисунка 3-4 видно, что серверная сторона определяла потери кодограмм. При этом можно наблюдать флуктуацию качества канала, что объясняется тем, что клиентской стороной передавалось различное число кодограмм.

*Проведение эксперимента на двух компьютерах, находящихся в локальной сети*

В следующих экспериментах были заданы аналогичные параметры работы программы в соответствии с пунктами предыдущих экспериментов, за исключением адреса клиентского сокета: он был настроен на передачу на адрес серверной стороны. По графикам экспериментов, проведенных на двух компьютерах, находящихся в локальной сети, можно сделать такие же выводы, как и по графикам экспериментов, проведенных на внутреннем сетевом интерфейсе, за исключением того факта, что были дополнительные потери кодограмм вследствие загрузки сети. Данные потери также можно увидеть на графиках, представленных ниже.

Отправление клиентской стороной числа кодограмм, равному максимальному числу объектов наблюдения.

Результаты эксперимента представлены на рисунке 4-1

Рис. 4-1. Эксперимент № 1 на двух компьютерах, находящихся в локальной сети

Отправление клиентской стороной числа кодограмм, равному максимальному числу объектов наблюдения, с прекращением работы клиентской стороны.

Результаты эксперимента представлены на рисунке 4-2

Рис. 4-2**.**Эксперимент № 2 на двух компьютерах, находящихся в локальной сети

Отправление клиентской стороной числа кодограмм, равному 10% от максимального числа объектов наблюдения.

Результаты эксперимента представлены на рисунке 4-3

Рис. 4-3.Эксперимент № 3 на двух компьютерах, находящихся в локальной сети

Отправление клиентской стороной числа кодограмм, равному максимальному числу объектов наблюдения за вычетом некоторого случайного числа.

Результаты эксперимента представлены на рисунке 4-4

Рис. 4-4 Эксперимент № 4 на двух компьютерах, находящихся в локальной сети

**Выводы**

Разработанное клиент-серверное приложение соответствует требованиям технического задания, а именно выполняет обмен сетевым трафиком с его сбором и анализом с применением метода без отключения канала. Данное программное обеспечение может применяться в системах реального масштаба времени, при этом оно производит контроль качества канала, что является важной составляющей для обеспечения надежности системы.

**Литература**

1) Савватеев В.С., Нимира М.Г. Патент на изобретение № 2598807 «Способ контроля качества каналов передачи данных».

2) http://www.aif.ru/dontknows/infographics/protivovozdushnaya\_i\_protivoraket naya\_oborona\_moskvy\_infografika

3) https://ru.wikipedia.org/wiki/Помехоустойчивость\_линии

4) http://nptel.ac.in/courses/117101051/24

5) http://www.pitri-tv.ru/pdf/21.pdf

6) http://vii.sfu-kras.ru/images/libs/Osnovi\_repp.pdf

7) Сборник докладов Шестой межвузовской студенческой конференции «Научная сессия – современная радиоэлектроника». Москва, 31 марта 2017 года / под общей редакцией канд. техн. наук Н.Э. Ненартовича. – М.: ПАО «НПО «Алмаз», 2017. – 480 с.: ил.

8) Прохоров А.М. Способ контроля качества цифровых каналов передачи данных. Электронный журнал «Вычислительные сети. Теория и практика», номер 30, июнь 2017.

9) XV Молодежная научно-техническая конференция «Радиолокация и связь – перспективные технологии» (Москва, 7 декабря 2017 г.) Материалы конференции – М.: Мир науки, 2017. – Режим доступа: http://izd-mn.com/PDF/25MNNPK17.pdf – Загл. с экрана.

10) XV Молодежная научно-техническая конференция «Радиолокация и связь – перспективные технологии» (Москва, 7 декабря 2017 г.) Тезисы докладов