

MeshCourier - офлайн-мессенджер с отложенной доставкой сообщений

Курсовой проект | Индивидуальный | Программный

Выполнила: Рамазанова Зарина Робертовна, БПИ-249

Научный руководитель: Новоселов Александр Александрович,
старший разработчик ООО "ТЦР"

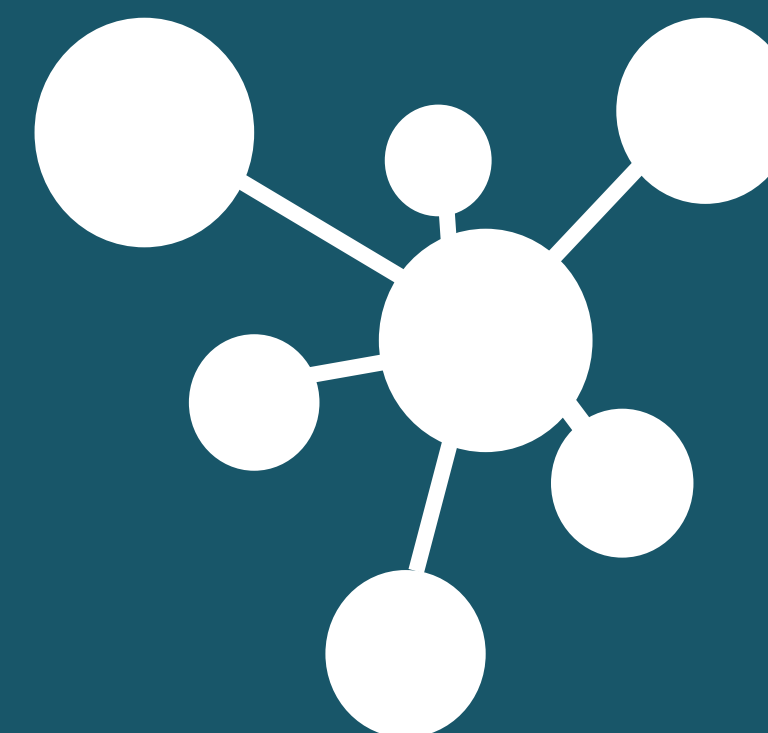


Описание темы проекта

В России участились случаи отключения мобильного интернета, при которых стандартные мессенджеры становятся недоступны. MeshCourier решает эту проблему: приложение работает без интернета и мобильной сети – мобильные устройства самостоятельно находят друг друга через Bluetooth и передают сообщения по цепочке.

Если получатель временно недоступен, сообщение сохраняется на промежуточном устройстве и доставляется позже.

Приложение не зависит от внешней инфраструктуры и обеспечивает доставку сообщений там, где обычные мессенджеры не работают.



Цели и задачи проекта

Цель:

- Реализовать приложение для защищённого обмена сообщениями, работающее без доступа к сети Интернет и поддерживающее отложенную доставку сообщений.

Задачи проекта:

- Анализ аналогов и выяснение функциональных требований
- Проектирование архитектуры и выбор технологий
- Реализация передачи данных по Bluetooth
- Реализация механизма отложенной доставки сообщений
- Интеграция шифрования сообщений в соответствии с российскими стандартами
- Разработка формата пакетов и правил маршрутизации

Функциональные требования

1. Обнаружение соседних устройств с помощью Bluetooth
2. Отправка и получение текстовых сообщений и небольших файлов без подключения к интернету
3. Шифрование и подпись каждого сообщения по российским стандартам
4. Обмен открытыми ключами между устройствами
5. Отображение статуса доставки сообщения
6. Идентификация пользователя по QR-коду
7. Работа приложения в фоновом режиме
8. Восстановление очереди сообщений после перезагрузки устройства

Используемые технологии



Среда разработки -
Android Studio



Язык разработки: Kotlin



UI-фреймворк: Jetpack
Compose



Шифрование сообщений
реализовано с помощью
КриптоПро CSP 5.0

Для внедрения зависимостей использована библиотека Hilt. Для хранения данных - библиотека Room

Архитектура приложения

Clean Architecture + MVVM

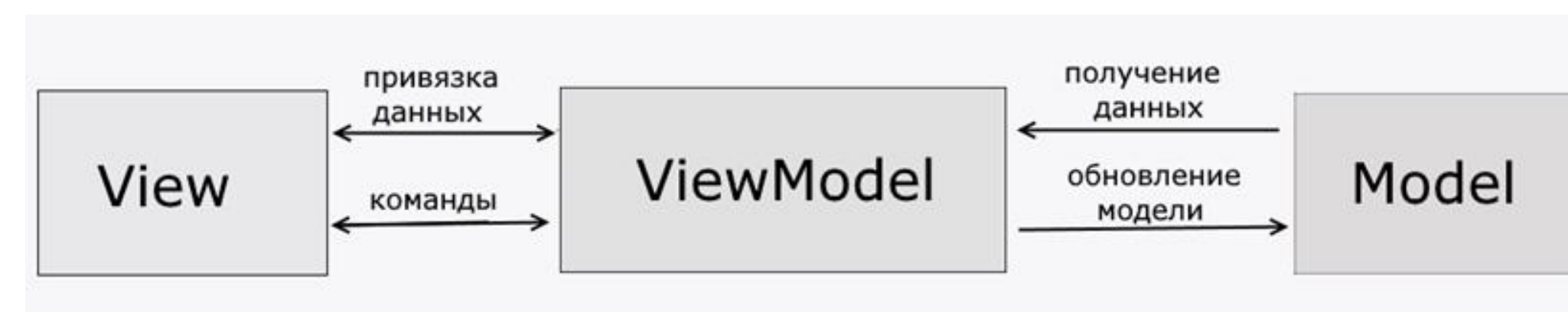
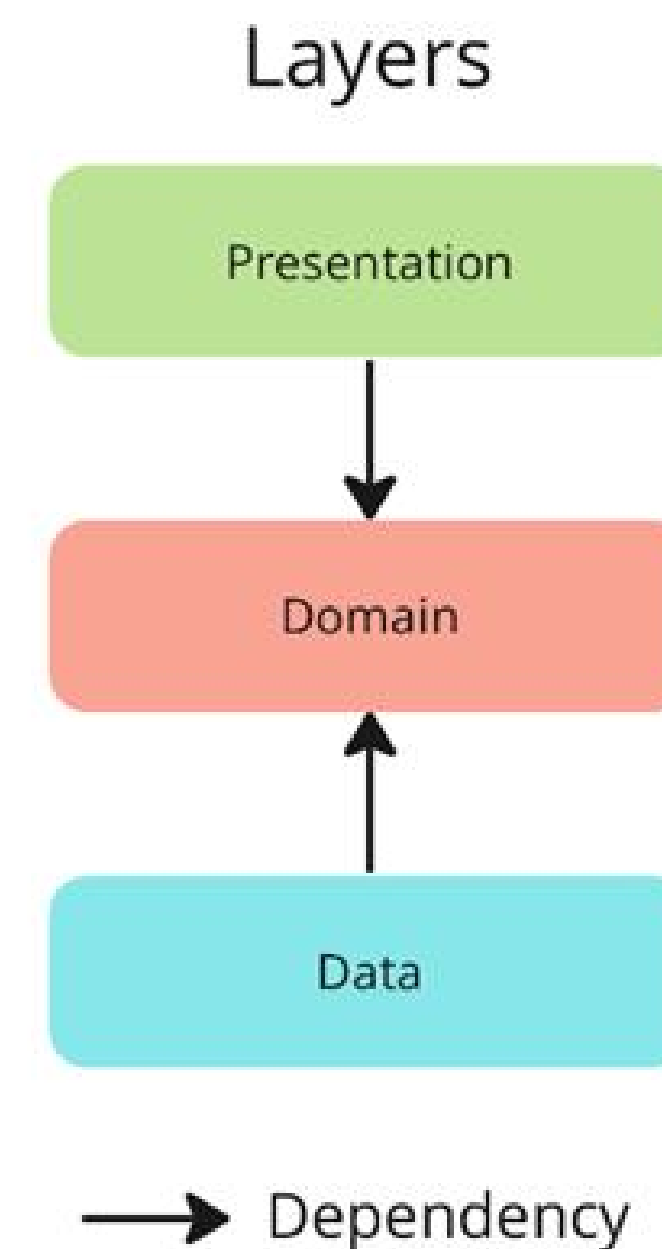
Clean Architecture задает глобальную структуру всего приложения, разбивая его на независимые слои:

Presentation - слой UI (взаимодействие с пользователем)

Domain - бизнес-логика (модели сообщений и пакетов, правила маршрутизации, шифрования и доставки, интерфейсы репозиториев)

Data - слой данных (работа с базой данных, реализации репозиториев, работа с КристоПро CSP)

Слой Presentation разработан с использованием шаблона проектирования MVVM (Model-View-ViewModel)



Передача данных по Bluetooth

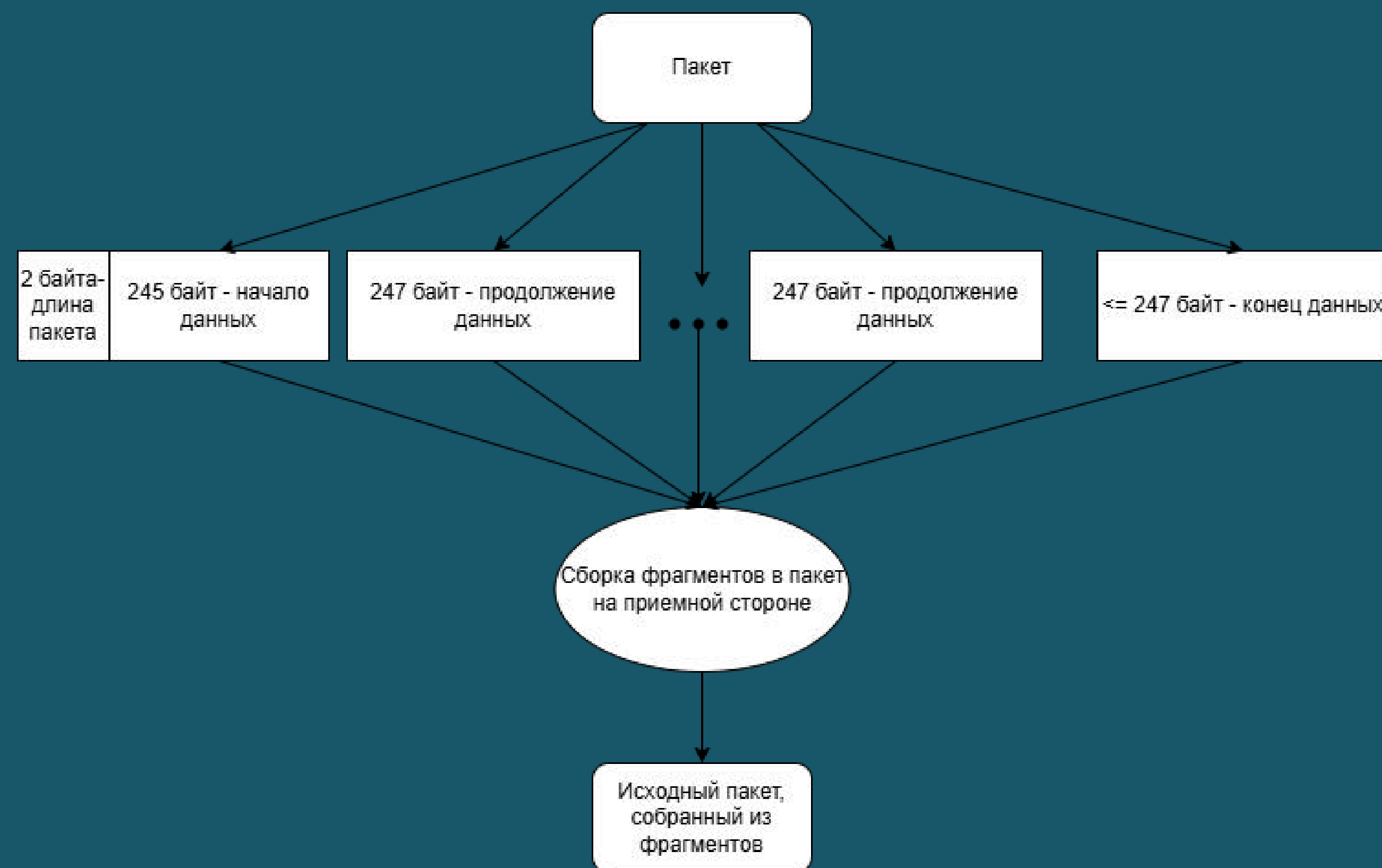
Каждый телефон одновременно:

- адвертайзит себя (рассылает пакеты о своем присутствии в сети) и принимает подключения

- сам ищет соседей и подключается к ним

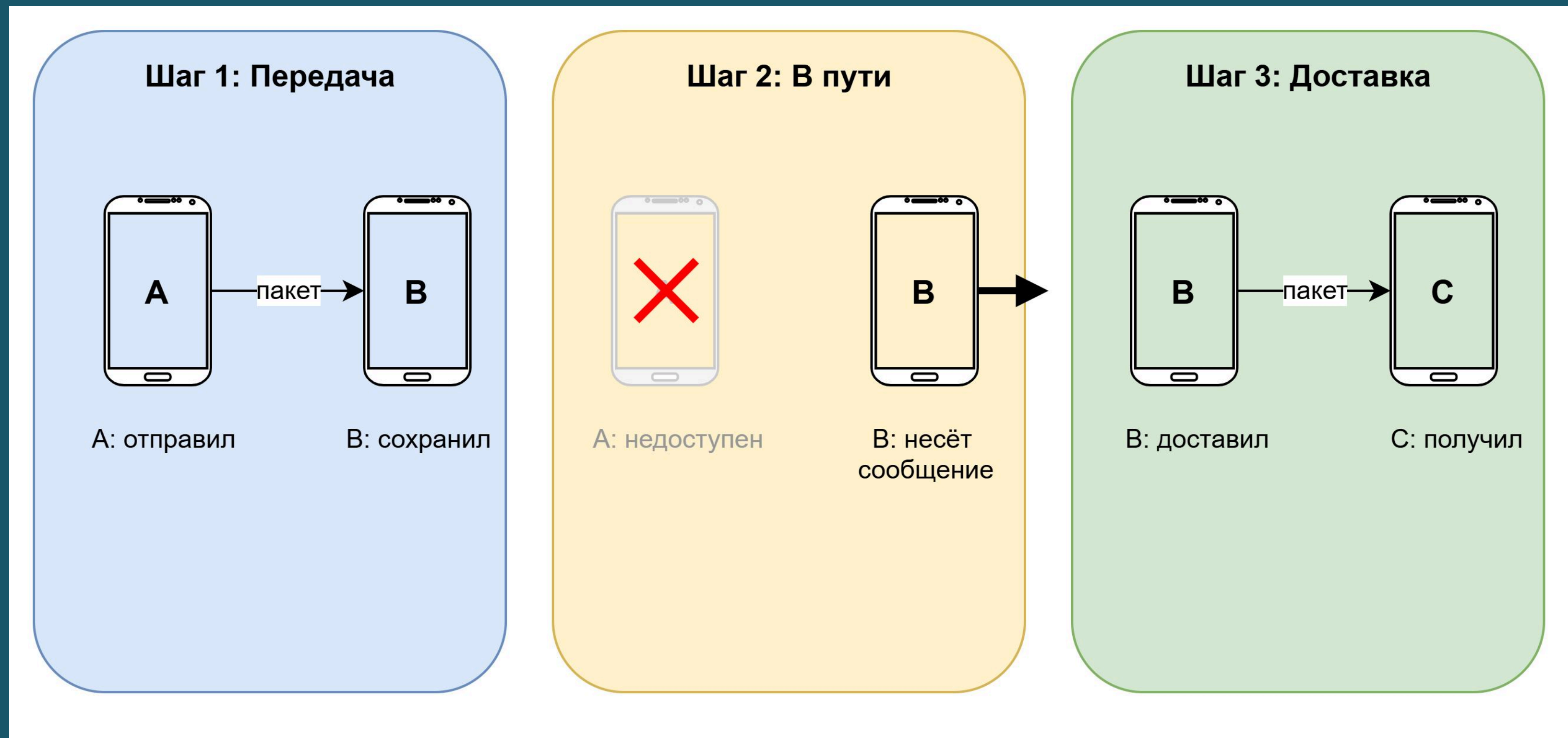
При этом происходит фильтрация по UUID сервиса - телефоны видят только устройства с установленным приложением MeshCourier.

За одну операцию передается не более 247 байт. Если размер пакета превышает заданную верхнюю границу длины полезной нагрузки, он разбивается на фрагменты.



фрагментация пакета

Отложенная доставка сообщений



Шифрование сообщений по российским стандартам

Ключи генерируются по алгоритму ГОСТ Р 34.10-2012 (256 бит) и хранятся в защищённом хранилище КриптоПро на устройстве. Каждое сообщение подписывается приватным ключом отправителя и шифруется публичным ключом получателя. Шифруется алгоритмом Кузнечик. Для каждого сообщения генерируется уникальный случайный ключ сессии.

Обмен публичными ключами происходит напрямую между устройствами через экран «Рядом».

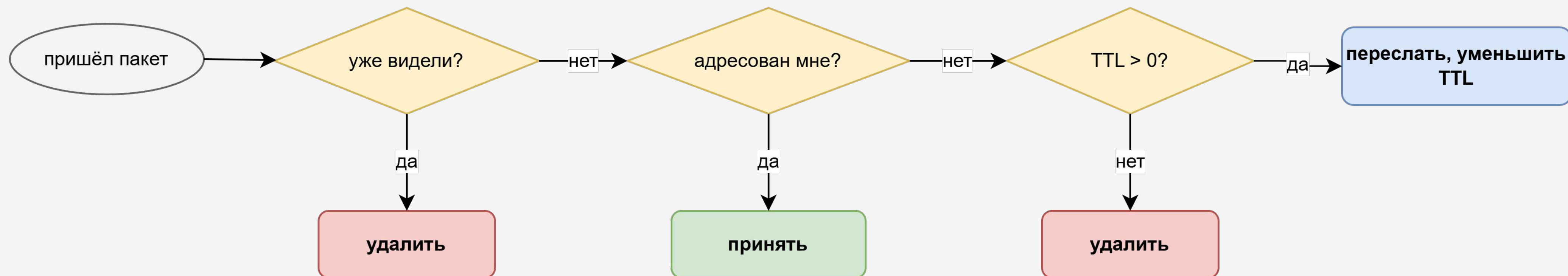


подписанное сообщение

Формат пакетов и правила их маршрутизации



формат пакета



маршрутизация пакетов

Результаты и выводы

В рамках курсового проекта были выполнены следующие задачи:

- Проведен анализ аналогов и выявлен основной функционал приложения
- Спроектирована архитектура приложения и выбраны подходящие технологии для разработки
- Реализована передачи данных по Bluetooth
- Реализован механизм отложенной доставки сообщений
- Интегрировано шифрование сообщений в соответствии с российскими стандартами с использованием КриптоПро CSP
- Разработан формат пакетов и правила маршрутизации

Приложение-мессенджер, работающее без подключения к сети и поддерживающее отложенную доставку зашифрованных сообщений реализовано.

Цель курсового проекта достигнута.

Направления дальнейшей работы

1. Добавление альтернативных транспортных каналов

Добавление Wi-Fi Direct увеличило бы дальность связи с 30 до 200 метров.

Архитектура приложения позволяет сделать это, не затрагивая основную логику.

2. Умная маршрутизация

Переход от рассылки всем соседям к направленной маршрутизации с запоминанием топологии сети - для повышения эффективности передачи в больших сетях.

3. Научная деятельность

Развитие проекта в рамках научной деятельности совместно с научно-учебными лабораториями ФКН

Демонстрация работы приложения

*Спасибо за
внимание!*

