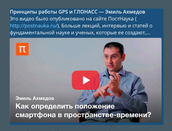
GNSS

- **Кто я?**
  - Дмитрий Полищук
  - Руковожу/Разрабатываю партнерские продукты в Яндекс.Такси
- **Зачем я сегодня это буду рассказывать?**
  - Многие спрашивали как мы фиксим проблем с локацией
  - Сам очень давно хотел рассказать
  - И возможно благодаря фидбеку - появятся еще новые идеи
  - Ну и кажется будут еще доклада от меня про эту тему, т.к. тут минимум на десять лекций материала
- GNSS в Android
  - В Android LocationManager встроенный гугловый LaaS - NETWORK_PROVIDER
  - FusedLocationProvider
    - Часть Google Play Services
    - Делает scoring координат с NETWORK и GPS
      - Два вектора координат
        - Время
        - Скорость
        - Очки качества (прыжки)
        - Принимаем решение откуда берем координату
    - Отличное готовое универсальное решение, способное повысить качество координат в разы
  - Мы используем свое решение
    - Google LaaS
    - Yandex LaaS
      - Тоже умеет выкусывать регионы где идут помехи или подмена координат
    - GPS
      - FusedLocationProvider
    - Yandex.MapKit LocationManager
    - Притягиваем координаты к графу
      - У нас свой граф дорог
      - Но можно заменить на
        - **OSRM** http://project-osrm.org
    - И в отличии от FusedLocationProvider
      - Мы больше не верим GPS координатам, чем верим
      - Т.е, как только мы зафиксируем скачок, мы сравним скачки со всеми другими источниками
      - И переключимся на наиболее правдоподобный
    - Edge cases
      - Пользователь открыл приложение в зоне GPS Spoofing
        - Мы собираем все координаты известные системе и показываем экран пользователю с ними

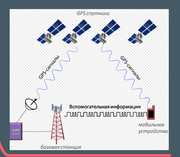
      - Пользователь резко переместился из одного города в другой (физически), а у нас координаты запомненые
        - Если все источники координат указывают, что пользователь фактически правда находится в другом городе, то мы так же покажем этот скрин
          - И заресетим эти координаты новыми
    - Все параметры доверительных интервалов о принятии решения о переключении приходят нам с сервера
    - Собираем весь трек водителя и периодически досылаем на сервер
      - Сервер дополнительно притянет трек к дороге и сгладит
  - Как мы это тестируем?
    - Все эти кейсы заложены в наш тестплан по тестированию GPS
    - Android Emulator
    - adb
    - Mocks for Geo Location Sources
  - Куда двигаемся дальше?
    - Фильтр Калмана
      - Пробовали - не работает. Просто притягивание координат к графу с акселерометром работает лучше, чем этот всемогутор
    - GNSS Raw Measurements
      - С Android 7 появился API позволяющий захватывать с драйвера GPS сырые данные о псевдодальностях
      - **Android Doc** https://developer.android.com/guide/topics/sensors/gnss
      - **Standalone matlab app + android logger** https://github.com/google/gps-measurement-tools
      - **Библиотека для вычисления Псевдодальностей (часть AOSP)** https://github.com/google/gps-measurement-tools/tree/master/GNSSLogger/pseudorange
      - Т.е. этот API позволяет нам самим рассчитать координаты на основании более низкоуровневых данных
- GNSS в iOS
  - CoreLocation
    - К сожалению, iOS не дает такой свободы в обработке координат

    - Компания Apple на предложения о любых изменениях просит репортить в Radar и они сами будут это исправлять
    - Как тестируем?
      - **iTools** https://www.thinkskysoft.com/itools/
    - Из коробки умеют противодействовать статическому спуфингу
    - Если спуфинг по динамическому треку - то ломается их антиспуф
- 4 спутника для определения

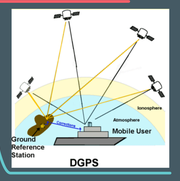


https://www.youtube.com/watch?v=gDc_UFIXsg0

- A-GPS



- Differential GPS



- Location as a Service
  - Это база со всеми wifi и сотовыми точками с привязкой к координате
    - Буквально эта база это hashmap и выглядит так
      - MAC адрес роутера -> гео точка
      - Cell Id вышки -> гео точка
      - ip address -> гео точка
      - ... другие атрибуты -> гео точка
    - Собирает эту базу приложение установленное у пользователей, которое сканирует ближайшие wifi, cell id и отправляет на сервер с привязкой к гео координате
      - Причем понятно что там есть скоринг этого качества
    - А дальше, уже другие приложения могут узнавать координаты без использования GPS, только отправляя запрос на сервер с видимыми wifi и cell ids
  - **Google** - https://developers.google.com/maps/documentation/geolocation/intro
  - **Yandex** - https://yandex.ru/dev/locator/doc/dg/concepts/geolocation-docpage/
- Spoofing GPS
  - Подмена сигнала GPS на физическом уровне
    - С помощью чего это можно сделать?
      - Software-defined radio
        - HackRF https://greatscottgadgets.com/hackrf/
          - Передача радиосигналов с помощью HackRF https://habr.com/ru/post/372177/
          - Умеет генерировать GPS сигнал
            - https://github.com/osqzss/gps-sdr-sim
        - BladeRF
      - Специальная техника позволяющая подменять сигнал в радиусе 150 км в прямой видимости
      - Опыт показывает, что в Москве подменяется сигнал только на GPS L1 канале
        - Двух диапазонные GNSS приемники могут помочь
          - **Third-Generation GNSS Location Hub with Dual Frequency Support** https://www.broadcom.com/products/wireless/gnss-gps-socs/bcm47755
          - **Huawei Kirin980** https://consumer.huawei.com/en/campaign/kirin980/
          - **Dual-frequency GNSS on Android devices** https://medium.com/@sjbarbeau/dual-frequency-gnss-on-android-devices-152b8826e1c
  - Jamming GPS - разновидность spoofing
    - Просто посылаем шум в тракт
- **Доп литература**
  - https://www.rfbr.ru/rffi/ru/books/o_18293

  - https://www.bloomberg.com/news/features/2018-07-25/the-world-economy-runs-on-gps-it-needs-a-backup-plan

  - https://www.youtube.com/watch?v=vywGgSrGODU&

  - Курс - Software Defined Radio with HackRF https://greatscottgadgets.com/sdr/1/
  - **Rethinking GPS: Engineering Next-Gen Location at Uber** https://eng.uber.com/rethinking-gps/