глобулярную структуру; установлено, что наименьший относительный коэффициент трения покрытий (в 3 раза меньше, чем у нержавеющей стали) и максимальное значение твердости (19,7 ГПа) соответствуют пленкам с глобулярной структурой стехиометрического состава.

Литература

1. *Бизюков А.А., Кашаба А.Е., Середа К.Н.,* Автокомпенсация ионного пучка в ускорителе с анодным слоем // Письма в ЖТФ. 1997. Т. 23 С. 69-73
2. *Бурмаков А.П., Кулешов В.Н.,* Оптическое управление реактивным магнетронным осаждением пленочных покрытий // ЖПС. 2007. Т. 74. С. 412-416
3. *Мусил И.,* Физические и механические свойства твердых нанокомпозитных пленок, получаемых реактивным магнетронным напылением // Наноструктурные покрытия. М., 2011. Гл. 10. С. 481–543.

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ НА БАЗЕ ОС ANDROID ДЛЯ КОНТРОЛЯ ПЕРЕМЕЩЕНИЯ ПЕРСОНАЛА

Д. С. Королев

ВВЕДЕНИЕ

Задача повышения эффективности производственного процесса всегда остается важнейшей проблемой в работе предприятий. Мониторинг персонала в реальном режиме времени, дает уникальную возможность обладать точной и достоверной информацией о реальном местоположении работников. Такая возможность позволит контролировать время прибытия и количество часов, проведенных на рабочем месте. Например, контроль перемещений курьера позволяет увидеть полный список охваченных адресатов.

Развитие мобильных устройств не стоит на месте, они завоевывают всё большую популярность среди пользователей. Современные смартфоны обладают встроенным GPS/GLONASS приёмником, большинство из которых работает под управлением мобильной операционной системы Android. ОС Android является самой популярной мобильной операционной системой в мире, её доля составляет 72.4% [1].

Данная статья посвящена разработке приложения на базе ОС Android для контроля перемещения персонала с помощью смартфонов. Особое внимание в данной статье уделено: точности и оперативности определения географических координат, максимальному энергосбережению, вопросам безопасности и коммуникации с открытыми системами мониторинга, что в полной мере не могут обеспечить существующие аналоги в сфере персональных устройств мониторинга местоположения.

МОДУЛИ ПРИЕМА ДАННЫХ О МЕСТОПОЛОЖЕНИИ ОБЪЕКТА

Современные GPS приемники для мобильных телефонов имеют ряд ограничений: длительное время определение начальных координат при первом старте GPS, так называемый «холодный старт»; фиксированное значение частоты обновления местоположения; высокое энергопотребление GPS приемника при постоянном обновлении местоположения. Все эти недостатки требуется компенсировать логикой программного обеспечения, работающего с GPS приемником. Предоставленная Android SDK сглаживает лишь часть проблем, поэтому стандартного набора API для работы с GPS приемником становится недостаточно.

Своевременное получение достоверного местоположения является наивысшим приоритетом в работе нашего приложении. Именно поэтому был создан отдельный поток myLocationListenerThread (наследник класса Thread [2]), отвечающий за прием и обработку координат и реализующий интерфейс LocationListener [2] (рисунок 1). Данный поток запускается с максимальным приоритетом ОС.

На этом этапе стоит отметить, что ни в руководстве по API[3], предоставленном Google'ом, ни в открытых кодах приложений-аналогов, получение и обработка координат не реализуется в отдельном потоке. Опытным путем было доказано, что выделение отдельного потока для работы с координатами существенно сокращает время «холодного» и «теплого» старта GPS приемника и уменьшает вероятность пропуска NMEA-сообщений с актуальными координатами, при одновременном выполнении других задач ОС.

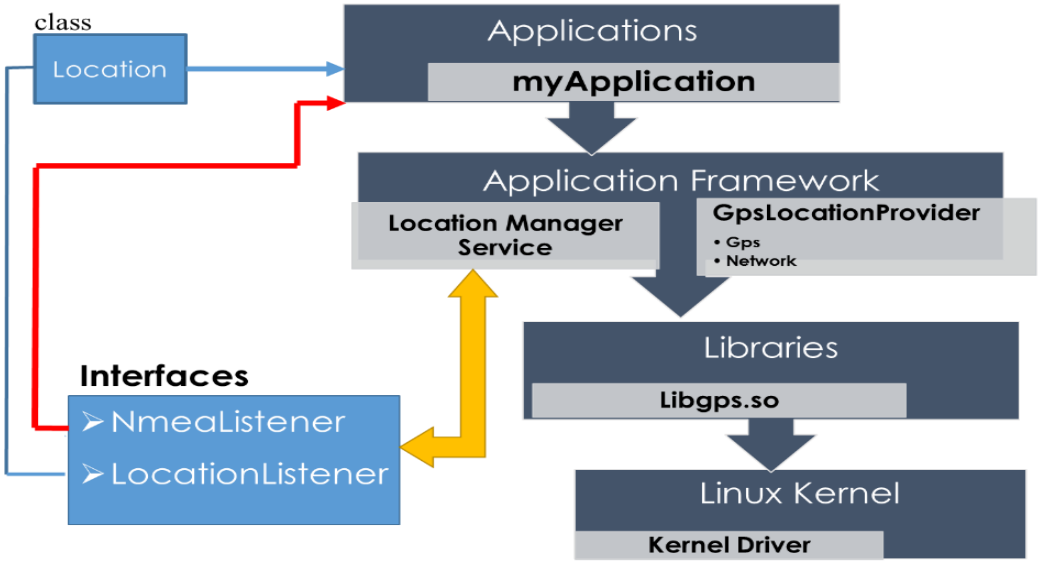

Рис.1. Алгоритм получения координат

На рисунке 1 представлен алгоритм получения координат от уровня приложения до уровня ядра системы. Стоит заострить внимание на использовании фреймворков и особенностях работы с ними.

Фреймворк LocationManagerService [2] предоставляет два интерфейса NmeaListener и LocationListener. Мы отказались от использования LocationListener в пользу NmeaListener, так при работе с LocationListener необходимо получать данные через класс посредник Location [2] в отличии от NmeaListener (рисунок 1), в котором можно получить сырой поток NMEA-сообщений. Именно NmeaListener оказался более гибким и самое главное быстродейственым, на актуальных и более поздних версиях ОС Android.

МЕТОДЫ ЭНЕРГОСБЕРЕЖЕНИЯ

Ресурсоемкость приложения является важным фактором при автономном мониторинге. Для решения этой задачи необходимо было разработать программную логику собственными средствами, так как средства Android не позволяли достичь необходимого уровня энергосбережения без ущерба для точности определения координат и без снижения актуальности переданной информации.

Решения были достигнуты следующими средствами: обработка данных со встроенного датчика ускорения, регистрирующего факты локального перемещения объекта; сохранение и отправление пакетов с данными кратковременными сеансами связи; работа приложения по расписанию день-ночь; обработка флагов внешних событий (заряд встроенного аккумулятора от питающей сети, подключение к Wi-Fi сети с интернет доступом).

Стоит заострить внимание на обработке данных с датчика ускорения. Если устройство покоится (лежит на столе), то нет необходимости постоянно опрашивать GPS приемник, так как местоположение устройства остается неизменным. После того как значение ускорения превысит предельно заданное, приложение вновь начинает опрашивать навигационный модуль GPS для получения достоверных координат на местности.

КОММУНИКАЦИЯ С ОТКРЫТИМИ СИСТЕМАМИ МОНИТОРИНГА МЕСТОПОЛОЖЕНИЯ

Одной из задач, которую необходимо решить, это возможность работы с различными системами мониторинга. Разработанное приложение опробовано для двух систем обладающих разными протоколами обмена между сервером и устройством.

Один из серверов находиться по адресу http://monitoring.kamerton.by или 193.193.165.166 с портом 20332. Данный сервер работает с протоколом Wialon, который разработан фирмой Gurtam. Общий вид строки следующий[4]:

$$\#TP\#msg\backslash r\backslash n \quad (1)$$

где # - стартовый байт, TP - тип пакета, # - разделитель, msg - сообщение, \r\n – окончание пакета.

Другой сервер находиться по адресу http://www.antelis.by/ или 217.21.41.73 с портом 20104. Данный сервер работает со своим внутренним протоколом. Общий вид строки, следующий:

$$TD\$msg*crc\backslash r\backslash n \quad (2)$$

где TD - тип трекера, $ - разделитель, msg - сообщение, *crc - контрольная сумма, \r\n – окончание строки.

ВОПРОСЫ БЕЗОПАСНОСТИ

Так как обычному пользователю нет необходимости в широком выборе настроек, а в некоторых случаях даже нужно огранить доступ к изменению настроек, в приложении был реализован режим администратор/пользователь. Для того чтобы начать работу в статусе администратора, необходимо ввести пароль и логин, который выдает разработчик ограниченному кругу лиц.

Так же стоит отметить, что только администратор может останавливать систему мониторинга, что является еще одним из средств безопасности. Администратор может включить режим автозагрузки приложения, т.е. после перезагрузки ОС приложение запустится автоматически. Пользователю доступны лишь средства визуализации, отражающие состояние устройства в упрощённом виде.

ЗАКЛЮЧЕНИЕ

Разработанное приложение опробовано на нескольких типах мобильных устройств (смартфон, планшет) и испытано на всех текущих версиях ОС Android. В данный момент приложение находится в опытной эксплуатации на одном из коммерческих предприятий РБ, заинтересованном в контроле перемещении персонала.

Литература

1. Интернет-адрес: http://www.kantarworldpanel.com/smartphone-os-market-share.
2. Интернет-адрес: http://developer.android.com/reference/packages.html.

3. Интернет-адрес: http://developer.android.com/guide/index.html.
4. Интернет-адрес: http://extapi.wialon.com/hw/cfg/Wialon%20IPS.pdf.
5. *Брайн Харди.* Программирование под Android (Для профессионалов). – СПб: Питер, 2014. – С. 592.

ИССЛЕДОВАНИЕ ЭЛЕМЕНТОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11

Ю. Ю. Литвинович, П. И. Горбанов

ВВЕДЕНИЕ

Появление стандарта 802.11 послужило толчком для быстрого развития и широкого распространения беспроводных сетей. Однако пользователи этих сетей не всегда осведомлены о существующих угрозах безопасности, которые приносит с собой данная технология [1].

В работе анализируется безопасность элементов защиты сетей стандарта IEEE 802.11 и методом проведения атак исследуется надежность каждого из них.

ЭЛЕМЕНТЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11

Беспроводные сети стандарта 802.11 для приема и передачи информации используют 2.4ГГц и 5ГГц диапазоны радиочастот. Как следствие этого, любая станция, настроенная на данные частоты, имеет возможность принимать и передавать сигналы. Поэтому безопасный обмен информацией в беспроводных сетях возможен только при наличии двух составляющих - контроля доступа и шифрования.

В качестве средств контроля доступа в стандарте 802.11 предусмотрены аутентификация (открытая и с совместно используемым ключом), скрытие SSID-имени сети и фильтрация по MAC-адресам. Сюда также можно отнести изменение мощности сигнала, которое настраивается на большинстве современных точек доступа. К механизмам обеспечения шифрования стандарта 802.11 относятся технологии WEP и WPA/WPA2 [2].

Однако все перечисленные выше элементы имеют уязвимости, которые при их грамотном использовании приводят к нарушению безопасности беспроводных сетей. Исследуем каждый из них.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ

Анализ механизмов аутентификации позволяет выявить в них некоторые уязвимости.