УДК 004.056.5:621.396.2

# Определение местоположения смартфона по его идентификационной информации и данным сенсоров

**Е.А. КРИШТОПОВА,**
к. т. н., доцент УО «БГУИР»,
зам. дир-ра по производственному обучению ф-ла БГУИР «Минский радиотехнический колледж»

**И.С. ТЕРЕХ,**
к. т. н., начальник технического отдела ООО «Ньюлэнд»

**Рассмотрены варианты определения местоположения смартфона с использованием его идентификационных данных при авторизации в сетях поставщиков услуг связи. Показана возможность поиска смартфона через анализ подключений устройства к сетям передачи данных. Предложено дополнительно использовать данные сенсоров смартфона для его локализации, определения характера движения.**

***Ключевые слова:***
*смартфон, определение местоположения, IMEI, IMSI, MAC-адрес, сенсоры.*

**Введение.** Сегодня практически любой человек является владельцем мобильного устройства (МУ), как правило, смартфона. Современный уровень развития технологий позволяет использовать смартфон не только для связи, но и для определения местоположения его владельца. Последнее может быть полезно родителям для контроля за перемещениями ребенка, владельцам МУ в случае его кражи, правоохранительным органам при поиске преступников. Функции отслеживания могут понадобиться в экстремальных ситуациях, например, когда человек находится в зоне действия природных катаклизмов, техногенных катастроф, массовых беспорядков и т. п.

В настоящее время известны следующие способы отслеживания смартфона:

1) через доступ к учетным записям владельца;

2) по его идентификаторам оператором сотовой электросвязи;

3) через открытые данные, извлекаемые из других приложений и сенсоров смартфона.

Каждый способ имеет достоинства и недостатки, которые рассмотрим ниже.

**1. Отслеживание смартфона через доступ к учетным записям владельца.** Операционные системы, а также встроенное программное обеспечение (прошивка) смартфонов содержат функции поиска, например Find My iPhone от Apple, Android Device Manager от Google, Find My Mobile от Samsung и др. Для успешного поиска смартфона необходимо выполнение следующих условий:

желательна включенная функция отслеживания мобильного устройства на самом мобильном устройстве;

активная на отслеживаемом мобильном устройстве учетная запись владельца;

желательна включенная функция определения местоположения посредством GPS или другой системы геопозиционирования. В этом случае данные не всегда достоверны, т. к. не являются аутентифицируемыми и могут быть подменены злоумышленником [1].

Для поиска смартфона могут быть использованы данные о Wi-Fi-подключениях, базовых станциях, местоположение которых предоставляется интернет-сервисам провайдерами, чтобы локализировать местонахождение владельца для вызова такси, определения прогнозов погоды и др. При установлении соединения МУ передает в сеть свои идентификационные данные, в частности MAC-адрес, который уникален и не зависит от местоположения, а информация о местоположении и устройстве входа фиксируется в учетных записях (Google, Apple, Yandex, Skype и др.), приложениях электронной коммерции и т. д. Используя доступ к учетной записи на другом устройстве, можно узнать о местоположении МУ.

Приложение Google Nearby позволяет пользователям смартфонов Android, которые находятся на расстоянии до 30 метров друг от друга, подключать свои устройства, обмениваться данными и взаимодействовать с сервисами. Для обнаружения используются Bluetooth, Wi-Fi и ультразвук. Обмен данными между устройствами Android осуществляется по протоколу Eddystone, который компания Google сделала открытым для разработчиков. Владельцы технологии заявляют, что идентификатор смартфона-маяка меняется псевдослучайным образом не позже чем через 9 часов, частота смены идентификатора определяется разработчиком приложения. У Apple также имеется подобное решение, оно называется iBeacon и является платным для разработчиков [2].

Отслеживание МУ по Wi-Fi (MAC-адресу) и Bluetooth ограничено из-за относительно небольшой мощности передатчиков, используемых в этих технологиях. Но этого достаточно для определения перемещения человека внутри заданной площади (например, вышел из здания или вошел в него и т. п.) [3].

**2. Отслеживание смартфона по его идентификаторам оператором сотовой электросвязи.** Оператор сотовой электросвязи отслеживает перемещение смартфона в своей сети, используя IMSI (International Mobile Subscriber Identity – международный идентификатор мобильного абонента (SIM-карты), ассоциированный с каждым пользователем сотовой электросвязи), и/или IMEI (International Mobile Equipment Identity – международный идентификатор мобильного оборудования). Последний является уникальным для идентификации МУ. Мобильным устройствам, работающим с несколькими SIM-картами, может быть присвоено несколько IMEI. Данный идентификатор смартфона может быть изменен с помощью программ подмены IMEI или переустановки встроенного программного обеспечения, но в ряде стран это уголовно наказуемо.

Для управления сетью операторы сотовой электросвязи используют набор сигнальных телефонных протоколов SS7 (Signaling System № 7), одним из которых является MAP (Mobile Application Part – подсистема мобильных приложений). Начиная с установки соединения, протокол работает для обмена пользовательской информацией, маршрутизации звонков, взаимодействия с биллингом и поддержки интеллектуальных услуг. SS7 разделяет информационные и сигнальные (управляющие) каналы [4, 5].

С целью обеспечения абонента связью оператор сотовой электросвязи хранит и обновляет информацию о местоположении МУ, для чего используется система регистров HLR/AuC и MSC/VLR, где HLR (Home Location Register) – регистр местоположения домашних абонентов, AuC (Authentication Center) – центр аутентификации, MSC (Mobile Switching Center) – центральный коммутатор сети сотовой электросвязи, VLR (Visitor Location Register) – гостевой регистр местоположения (см. рис.).

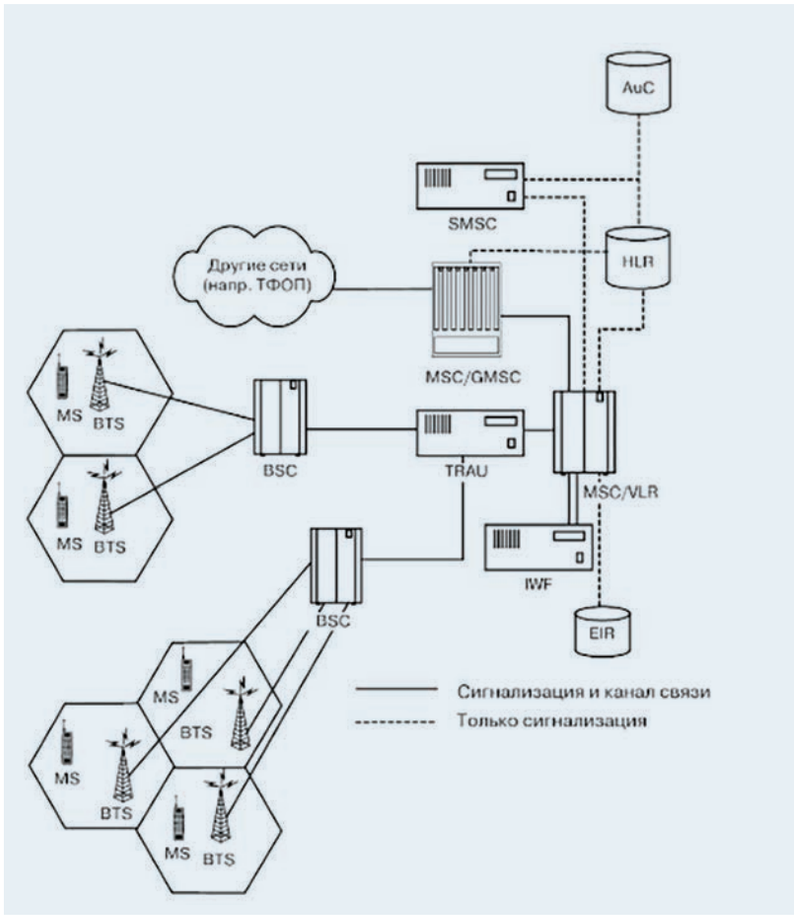



**Рисунок – Упрощенная структура сети связи оператора сотовой электросвязи**

Для минимизации объема транзакций с HLR данный регистр содержит только информацию о местонахождении MSC/VLR, к которым в данный момент подключено МУ, тогда как VLR содержит более детальную информацию о зоне местонахождения смартфона, обычно определяемой контроллером базовой станции BTS.

В VLR информация о местонахождении смартфона обновляется каждый раз, когда МУ меняет зону местонахождения, а в HLR – только тогда, когда устройство меняет зону обслуживания, т. е. VLR. Обновление этой информации происходит в следующих случаях [5, 6]:

– МУ только что включилось;

– МУ переместилось в пределах зоны того же VLR, но в новую зону местонахождения;

– МУ переместилось в новую зону обслуживания (к новому VLR);

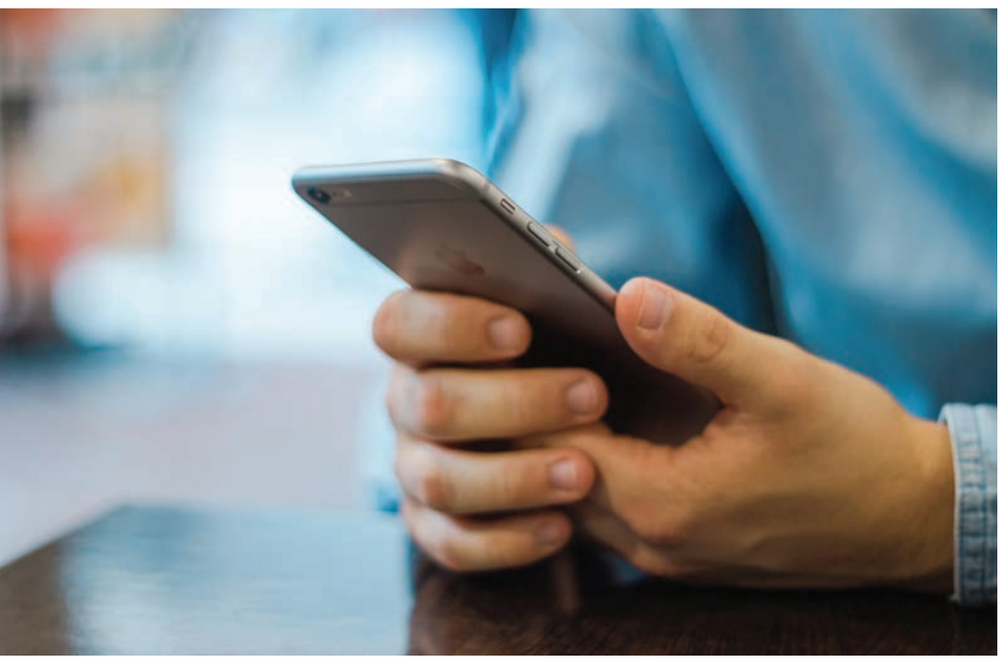
– сработал таймер обновления информации о местонахождении МУ.

При регистрации МУ в сети мобильного оператора сотовой электросвязи в эфир передаются следующие данные: IMSI, TMSI (Temporary Mobile Station Identity – временный идентификатор МУ, назначается VLR после успешной аутентификации и используется в процессе установки звонка, регистрации в сети только в пределах одной соты), в зависимости от аппаратно-программного оснащения сети оператора сотовой электросвязи может быть запрошен IMEI.

Для поиска смартфона по IMEI в сети оператора сотовой электросвязи необходимо, чтобы с HLR/AuC был интегрирован EIR (Equipment Identity Register) – реестр идентификации оборудования, содержащий перечень IMEI смартфонов, которым запрещен доступ в сеть (например, украденные устройства), а также тех, которые находятся под наблюдением правоохранительных органов. Использование EIR является опциональным для оператора сотовой электросвязи. При наличии EIR у оператора сотовой электросвязи мобильные устройства с заданными IMEI могут блокироваться в сети. Проверка осуществляется через запрос MSC в EIR по протоколу MAP: MAP_CHECK_IMEI.

Отсутствие в SS7 аутентификации и шифрования позволяет злоумышленникам реализовать нелегальный поиск МУ в сети оператора сотовой электросвязи [3, 4].

Для поиска смартфона оператором сотовой электросвязи может быть использована система глубокого анализа трафика (Deep Packet Inspection, DPI) – программно-аппаратного комплекса для классификации проходящего через сети оператора интернет-трафика по типу данных (веб-страница, документ, аудио, видео), протоколу (HTTP, BitTorrent, VoIP/SIP) и конкретным программам (Skype, WhatsApp). Традиционно DPI применяется для приоритизации контента в сети интернет и выполнения уровня качества (QoS) в канале передачи данных ограниченной пропускной способности [7, 8]. Во многих странах DPI провайдеров используются для распространения контекстной рекламы, т. к. позволяют отслеживать и анализировать статистику использования интернет-ресурсов и выявлять предпочтения владельцев смартфонов.



Система DPI добавляет служебные HTTP-заголовки при выполнении HTTP-запроса на сайты (хосты) из заданного оператором сотовой электросвязи списка, например веб-сайт оператора, ресурсы мультимедиа и т. п. В заголовках может содержаться внутренний IP-адрес абонента, номер телефона (MSISDN), IMEI и IMSI, идентификатор базовой станции, к которой подключен абонент.

**3. Отслеживание через открытые данные, извлекаемые из других приложений и сенсоров смартфона.** Смартфон оснащен набором компактных датчиков, которые постоянно собирают данные об окружающей пользователя среде с достаточно

**Таблица – Сенсоры современных смартфонов и собираемые ими данные**

| Наименование сенсора | Собираемые сенсором данные |
|---|---|
| Акселерометр | Расчет разности между истинным ускорением объекта и гравитационным ускорением |
| Барометр | Измерение атмосферного давления |
| Магнитометр | Определение ориентации устройства относительно направления «север – юг» |
| Гироскоп | Определение положения МУ в пространстве с большей точностью, чем магнитометр |
| Датчик приближения | Через использование ИК-излучения определение приближения объекта (лица пользователя к фронтальной части смартфона) и отключение сенсорного экрана |
| Термометр | Измерение температуры внутри устройства (в большинстве смартфонов), но на рынке присутствуют МУ, способные измерять температуру окружающей среды или тела человека |
| Датчик окружающего света | Оценка окружающего света и сглаживание яркости экрана устройства, чтобы соответствовать окружающему свету |
| GPS | Определение географического положения при помощи спутников. GPS не использует данные мобильной сети, поэтому геолокация работает и вне зоны покрытия сотовой связи |
| Камера | Выполнение фото- и видеосъемки |
| Датчик влажности воздуха | Определение влажности воздуха в окружающем пространстве |
| Педометр (шагомер) | Расчет пройденного расстояния и количества пройденных шагов. Используется совместно с акселерометром |
| Сканер отпечатков пальцев | Считывание отпечатка пальца для дальнейшего сравнения системой с эталонным изображением или сравнивание хешей от эталонного и считанного отпечатков |
| Модуль Wi-Fi | Обмен сигналами с роутером, точкой доступа, репитером или любым другим устройством, транслирующим данные по технологии беспроводной локальной сети на основе стандартов IEEE 802.11 |
| Модуль Bluetooth | Обмен сигналами по беспроводному соединению с подобными устройствами по стандарту IEEE 802.15.1 |
| Модуль NFC | Бесконтактная связь на расстоянии до 10 см с существующими смарт-картами, считывателями стандарта ISO 14443 и другими устройствами NFC |
| Микрофон | Преобразование акустических колебаний в электрический сигнал. Рабочий диапазон микрофонов смартфона захватывает и не воспринимаемый человеческим ухом ультразвук |
| Динамик | Воспроизведение звука |

высокой частотой дискретизации. Информация, получаемая с сенсоров смартфона (см. табл.), может быть использована для определения местоположения устройства, характера его движения.

Акселерометр показывает скорость движения, магнитометр определяет ориентацию устройства относительно направления «север – юг»; барометр измеряет давление воздуха в окружающей среде. Операционная система смартфона также располагает такими данными, как IP-адрес устройства, часовой пояс и состояние сети, которые могут быть использованы как исходные данные для определения местоположения и характера движения устройства. Эти данные могут быть доступны для любого приложения, в т. ч. не требующего разрешения доступа к спискам контактов, фотографиям или GPS.

Для оценки высоты нахождения над уровнем моря могут быть использованы данные о давлении воздуха, которые предоставляются службами погоды или картами Google, в сравнении с показаниями на барометре мобильного устройства. В сочетании с общедоступной информацией, такой как метеорологические отчеты, расписание транспорта и т. п., этих данных достаточно, чтобы точно локализировать МУ, вплоть до определения вида транспорта, на котором оно перемещается.

О передвижении на автомобиле свидетельствуют частые остановки при торможении на перекрестках и пешеходных переходах, повороты на 90°, которые можно обнаружить с помощью магнитометра. При перелетах часто изменяются часовые пояса, давление воздуха изменяется хаотично, что может быть зафиксировано барометром. В случае передвижения на поезде, как правило, происходит ускорение в одном направлении.

В [9] приведены примеры использования ультразвука для скрытых запросов о местонахождении МУ. Например, приложение SilverPush может определить ультразвук, встроенный в ТВ- или браузерную рекламу. Оно перехватывает сообщения со встроенного микрофона на смартфоне и отправляет на серверы компании-владельца IMEI, местоположение пользователя, версию его операционной системы и данные самого пользователя [10].

Примеры алгоритмов сбора и обработки данных, полученных с сенсоров смартфона для отслеживания местоположения смартфона, приведены в [11].

Во встроенном программном обеспечении смартфонов не предусмотрен запрет для приложений на считывание данных с датчиков. При этом одни приложения могут считывать незащищенные данные о местоположении с других приложений, имеющих доступ к критичной и не только информации о местоположении и параметрах окружающей среды, например, сервисов прогнозов погоды, приложений управления фитнес-браслетами, умными часами и IoT-устройствами.

**Выводы.** Сбор, обработка и хранение смартфоном огромного количества данных о параметрах подключения и состоянии окружающей среды позволяет легко определить местоположение устройства.

При подключении смартфона к сетям связи осуществляется его идентификация через передачу уникальных идентификационных кодов устройств – IMEI, IMSI, TMSI, MAC-адреса, Bluetooth-адреса, идентификационного номера производителя и т. д. Идентификационные коды используются на всех уровнях модели взаимодействия открытых систем не только для первоначальной аутентификации МУ в сети, но и в работе отдельных приложений и для отслеживания трафика владельца. Эти данные собирает и хранит в своих базах поставщик услуг электросвязи с привязкой к зоне обслуживания, что позволяет локализовать смартфон. Использование операторами мобильной электросвязи EIR и заблаговременное предоставление клиентам услуг по связыванию IMEI и IMSI значительно облегчают поиск устройства. Последнее позволяет сделать смартфон нерабочим в зоне обслуживания оператора по запросу владельца.

Google, Apple, Yandex, социальные сети и мессенджеры собирают данные для определения местоположения устройства, включая его идентификаторы, данные о местоположении точек доступа в сеть и т. п. Эта информация доступна в учетной записи владельца при подключении с любого устройства.

Так как большинство смартфонов не ограничивает запросы приложений к данным со своих сенсоров, это открывает большие возможности для отслеживания смартфона и определения характера его движения.

**ЛИТЕРАТУРА**


1. **Криштопова, Е.А., Терех, И.С.** Возможности спуфинга GPS сигналов и методы его предотвращения / Материалы XXII Междунар. науч.-техн. конф. «Современные средства связи», г. Минск, 19–20 окт. 2017 г. / БГАС; редкол. А.О. Зеневич [и др.], Респ. Беларусь. – С. 233–234.
2. Маячки Eddystone / Блог компании Google. Разработка для «интернета вещей». Разработка мобильных приложений. Разработка под Android [Электронный ресурс]. – Режим доступа: https://habr.com/company/google/blog/310486/. – Дата доступа: 17.11.2018.
3. **Райтман, М.А.** Искусство легального анонимного и безопасного доступа к ресурсам интернета. – СПб.: БХВ-Петербург, 2016. – 624 с.
4. **Гойхман, В.Ю.** Протоколы стека ОКС7: подсистема МАР. Серия «Телекоммуникационные протоколы». Книга 10. / В.Ю. Гойхман, Б.С. Голдштейн, Н.Г.Сибирякова. – СПб.: БХВ-Петербург, 2014. – 200 с.
5. **Голдштейн, Б.С.** Сети связи: учебник для ВУЗов / Б.С. Голдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб.: БХВ-Петербург, 2014. – 400 с.
6. **Пузанков, С.** Найти и обезвредить. Как раскрыть местоположение мобильного абонента // Информационная безопасность. Блог компании Positive Technologies [Электронный ресурс]. – Режим доступа: https://habr.com/company/pt/blog/191384/. – Дата доступа: 17.11.2018.
7. Deep packet inspection [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Deep_packet_inspection. – Дата доступа: 17.11.2018.
8. **Nabatov, S.** DPI мобильных операторов: от бесплатного интернета до раскрытия номера и местоположения [Электронный ресурс]. – Режим доступа: https://habr.com/post/345852/. – Дата доступа: 17.11.2018.
9. FTC Issues Warning Letters to App Developers Using 'Silverpush' Code / Federal Trade Commission [Электронный ресурс]. – Режим доступа: https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code. – Дата доступа 17.11.2018.
10. Сайт компании Silverpush [Электронный ресурс]. – Режим доступа: https://www.silverpush.co/. – Дата доступа: 17.11.2018. – Дата доступа 17.11.2018.
11. **Mosenia, A.** PinMe: Tracking a Smartphone User around the World / A. Mosenia, D. Xiaoliang, M. Prateek, K. J. Niraj // IEEE Transactions on Multi-Scale Computing Systems. – 2018. – Volume: 4, Issue: 3. – P. 420–435.


***The variants of localization of smartphone using its identification data when authorizing the networks of service providers are considered. The abilities to search for smartphone through the analysis of device connections to data networks is reviewed. It has been proposed to use additionally the sensor data of the smartphone for its localizing and determining the method of its movement.***

*Получено 03.01.2019.*