ИСПОЛЬЗОВАНИЕBLUETOOTHLOWENERGYBEACONS ДЛЯ НАВИГАЦИИ ВНУТРИ ЗДАНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лось Л. А., Павлович А. Н.

Волорова Н. А. – кандидат технических наук, доцент

В мире современных технологий широко используются системы навигации и позиционирования. Они позволяют с большой точностью определять текущее местоположение. Повсеместно применяется спутниковые системы навигации: GPS, GLONASS - развиваются Beidou и Galileo, которые позволяют определять скорость и направление движения, местоположение объектов практически в любом месте Земли. Однако спутниковые системы навигации имеет критические недостатки, не позволяющие при определенных условиях доходить сигналу до приемника. Так они не пригодны для определения положения внутри зданий. Несмотря на трудности реализации, системы позиционирования в зданиях становятся все более популярными. Они облегчают ориентирование людей в обширных незнакомых помещениях, позволяют строить маршруты к заданной точке. Данные, полученные с использованием таких систем, могут использоваться производителями и продавцами товаров для анализа посещения магазинов, наплывов покупателей, непосредственно рекламы товаров.

Существует несколько подходов к реализации навигации в зданиях. Можно выделить три приоритетных направления: использование Wi-Fi, геомагнитного позиционирования и Bluetooth маячков (Beacon). Использование Wi-Fi точек дает недостаточную точность, погрешность вычислений может составлять до 25 метров. Конфигурирование же такой сети Wi-Fi, которая будет гарантировать высокий уровень точности, потребует значительных материальных затрат. Подход с реализацией геомагнитного позиционирования имеет один существенный недостаток: в помещениях достаточно много оборудования (проводка), которое может изменять магнитное поле, что сильно влияет на навигацию. Использование же Bluetooth-маячков позволяет поддерживать приемлемую точность измерений при достаточно низкой стоимости реализации.

Работа Bluetooth-маяков базируется на использовании стандарта Bluetooth 4.0 LowEnergy. Использование этого стандарта позволяет обеспечивать работу устройств вплоть до нескольких лет.

В основу работы на канальном уровне положена модель взаимодействия широковещательных устройств (в данном случае маяков) и наблюдателя (пользовательского устройства) - это одна из возможных схем взаимодействия, предусмотренных стандартом Bluetooth Low Energy, и единственная в котором возможна передача от одного устройства - многим.

Широковещательное устройство (broadcaster) - рассылает пакеты сообщений, не устанавливая соединение по отдельности с каждым наблюдателем (observer).

Наблюдатель сканирует заданные частоты в ожидании публикации объявления (advertising).

Система навигации на основе Beacons обычно строится по следующему принципу. По всей территории помещения устанавливаются Bluetooth-маяки, причем мы знаем их координаты в пространстве. Пользовательское приложение получает информационные сообщения через некоторый промежуток времени от этих маяков. Исходя из полученных в сообщении данных и мощности полученного сигнала, циклично определяется текущее положение принимающего устройства.

Beacon с заданным промежутком между сообщениями транслирует один и тот же набор данных, представленный в таблице 1:

Преамбула (4 байта)	Идентификатор группы маяков (UUID) (16 байт)	Мажор (2 байта)	Минор (2 байта)	Эталонное значение мощности маяка (TXPower) (2 байта)

Таблица 1 – структура данных, транслируемых Bluetooth-маяком.

- преамбула – префикс пакета, сообщающий, что это именно Beacon;
- идентификатор группы маяков (UUID) – идентификатор, позволяющий отличать, например, маяки одного магазина от другого. Т.е. все маяки, расположенные в торговом зале одного магазина, будут иметь одинаковый идентификатор;
- мажор – уникальный идентификатор подгруппы маяков в рамках UUID, позволяет выделать в группу маяки, находящиеся в одном зале большого магазина;
- минор – идентификатор, позволяющий определить конкретный маяк;
- эталонное значение мощности маяка – сила сигнала на расстоянии в 1 метр от маячка, используется для определения расстояния до пользователя.

Набор данных, состоящих из идентификатора группы маяков, мажора и минора, позволяет точно определить координаты Beacon.

Для расчёта координат применяется трилатерация. В качестве опорных точек выбираются три и более маячка с наилучшим средним уровнем мощности сигнала. Далее необходима математическая обработка для устранения шумов и построения предсказательной модели. Математическая модель может также

использовать данные с других датчиков, например, акселерометр, гироскоп, магнитометр, которые доступны в современных моделях смартфонов и планшетов с целью повышения точности измерений.

Таким образом, системы, построенные на основе Bluetooth-маячков, являются конкурентоспособной альтернативой другим способам реализации систем навигации внутри помещений, а также могут быть использованы в комбинации с другими технологиями.

Список использованных источников:

1. Kevin Townsend, Carles Cufí, Akiba, Robert Davidson, Getting Started with Bluetooth Low Energy, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.
2. Навигация в помещениях с iBeacon и ИНС [Электронный ресурс] – Режим доступа. – URLhttps://habrahabr.ru/post/245325/ (дата обращения 03.04.2017).
3. BluetoothLowEnergyadoptedspecification [Электронный ресуср] – Режим доступа: – URLhttps://www.bluetooth.org/en-us/specification/adopted-specifications (дата обращения 04.04.2017).

УТИЛИТА ШИФРОВАНИЯ ФАЙЛОВ ДЛЯ WINDOWS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Молчанов И.В.

Жвакина А.В. – канд. техн. наук, доцент

Тема шифрования всегда была крайне важна в программировании, причем не только в больших бизнес-проектах, но и в небольших университетских работах, так как задача по защите данных от несанкционированного вмешательства всегда была, есть и будет актуальна. На данный момент существует большое количество алгоритмов шифрования (от простых перестановочных шифров до стандартизированных асинхронных алгоритмов). В процессе разработки изучены синхронные и асинхронные алгоритмы шифрования среднего уровня сложности, их сильные стороны и уязвимости, также данные алгоритмы реализуются в утилите, созданной для шифрования файлов.

В процессе исследования рассмотрены шифры XOR и RSA, так как являются наиболее простыми из использующихся на практике, но при грамотном использовании и надлежащих модификациях могут быть достаточно эффективными. Материал данной работы предназначен не для профессиональных программистов, давно освоивших более сложные алгоритмы, а для студентов, желающих реализовать какую-либо защиту данных в своих проектах.

Алгоритм шифрования RSA можно представить следующим образом:

- возьмем p, q – достаточно большие простые числа;
- n = p • q;
- выберем случайное d такое, что f = (p – 1) • (q – 1) взаимно просто с d;
- определим e, для которого (e • d) ≡ 1 (modf);
- открытый ключ: {e, n}; закрытый ключ: {d, n};
- блочное шифрование: $F_i = (M_i)^e \mathrm{mod} n$;
- блочная расшифровка: $M_i = (F_i)^d \mathrm{mod} n$.

Основными достоинствами шифра RSA являются:

- использование двух ключей, что позволяет использовать его в клиент-серверных приложениях;
- надежность шифрования при использовании достаточно длинных ключей (512 бит и более).

Основными его недостатками являются:

- необходимость генерации длинных простых чисел, что требует гигантских затрат времени;
- падение криптостойкости при небольших по длине ключах.

Также был проанализирован алгоритм шифрования XOR, описываемый так:

- выбор ключа K (как случайный, так и пользовательский, случайный считается более устойчивым);
- блочное шифрование: Fi = Mi xor K;
- блочная расшифровка: Mi = Fi xor K;

Достоинствами данного шифра являются:

- быстрота шифрования данных;
- простота реализации;
- высокая устойчивость шифра при регулярной смене ключа.

Основными его недостатками являются:

- при использовании чистого XOR и достаточном количестве перехваченных сообщений ключ может быть получен путем анализа зашифрованных данных;
- при известной части текста ключ также может быть получен при перехвате сообщения;
- ключ используется как для шифрования, так и для дешифровки сообщения.

Основной проблемой шифра RSA, по мнению автора, является то, что криптостойкость алгоритма со временем падает (*«По словам исследователей, после их работы в качестве надежной системы шифрования можно рассматривать только RSA-ключи длиной 1024 бита и более. Причём от шифрования ключом длиной в 1024 бит стоит отказаться в ближайшие три-четыре года»*), а для ее повышения