Макаров И.О., Попрыгин А.Ю. Выбор беспроводной технологии передачи данных и учет ее особенностей при обмене информацией на малых или средних расстояниях// Международный журнал информационных технологий и энергоэффективности. – 2021. – Т. 6 № 4(22) с. 3–11

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.73

ВЫБОР БЕСПРОВОДНОЙ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ И УЧЕТ ЕЕ ОСОБЕННОСТЕЙ ПРИ ОБМЕНЕ ИНФОРМАЦИЕЙ НА МАЛЫХ ИЛИ СРЕДНИХ РАССТОЯНИЯХ

Макаров И.О., Попрыгин А.Ю.
Филиал ФГБОУ ВО «Национальный исследовательский университет «МЭИ» в г. Смоленске, Россия, (214013, г. Смоленск, Энергетический проезд, 1), e-mail: Knyaghichigor@mail.ru

В статье на примере рассматривается процесс выбора беспроводной технологии передачи данных на малых и средних расстояниях. В качестве примера взята автономная беспроводная система управления запирающими устройствами. В статье приведен алгоритм выбора беспроводной технологии передачи данных, рассмотрены основные характеристики наиболее распространенных в настоящий момент беспроводных технологий. Основное внимание уделяется вопросам безопасности и энергоэффективности, так как выбор беспроводной технологии осуществляется для автономной распределённой системы управления запирающими устройствами. Данная статья будет полезна специалистам, начинающим разработку беспроводной системы

Ключевые слова: беспроводные технологии, BLE v 4.0, беспроводной контроллер для замков.

SELECTION OF WIRELESS DATA TRANSMISSION TECHNOLOGY AND TAKING INTO ACCOUNT ITS FEATURES WHEN EXCHANGING INFORMATION OVER SHORT OR MEDIUM DISTANCES

Makarov I.O., Poprygin A. Yu.
Smolensk Branch of the National Research University "Moscow Power Engineering Institute", Smolensk, Russia (214013, Smolensk, Energetichesky proezd, 1), e-mail: Knyaghichigor@mail.ru

The article examines the process of choosing a wireless personal area net. An autonomous wireless control system for locking devices is taken as an example. The article provides an algorithm for choosing a wireless technology for data transfer, considers the main characteristics of the most common wireless technologies at the moment. The focus is on the topic of security and energy efficiency, as the choice of wireless technologies is carried out for an autonomous distributed control system for locking devices. This article will be useful to those professionals who are starting to develop a wireless system.

Keywords: wireless technologies, BLE v 4.0, wireless lock controller.

При обмене данными на малых или средних расстояниях можно использовать следующие беспроводные технологии: NFC (на малых расстояниях); Bluetooth, ZigBee, Thread и др. (WPAN технологии); Wi-Fi (WLAN технология). В большинстве случаев выбор беспроводной технологии передачи данных зависит от особенностей системы, в которой она будет использоваться. Поэтому рассмотрим все на конкретном примере.

В качестве примера возьмём автономную распределенную систему управления запирающими устройствами, которая позволяет управлять замками и защёлками со смартфона. Для выбора беспроводной технологии передачи данных нужно:

1. Проанализировать особенности системы, где нужно применить выбранную технологию.
2. Рассмотреть доступные технологии.
3. Руководствуясь выделенными особенностями системы на основе характеристик беспроводных технологий, выбрать наиболее подходящую из рассмотренных технологий.
4. Проанализировать выбранную технологию на наличие «слабых» мест в контексте рассматриваемой системы.
5. В случае обнаружения «слабых» мест, найти пути их решения или обхода.

К беспроводной технологии передачи данных в системе управления электромеханическими замками можно выдвинуть следующие требования:

- близкая (до 20 м.) дальность действия;
- высокая безопасность (так как происходит управление замками);
- высокая скорость соединения (так как система распределенная предполагается частое соединение/разъединение пользователей с системой);
- скорость обмена не ниже 100 кбит/с (передача данных между контроллером и пользователем не является потоковой, а осуществляется пакетами достаточно малого размера, поэтому требования к скорости относительно невысоки);
- низкое энергопотребление (так как система является автономной);
- наличие топологии соединения «точка-точка» или «звезда».

Наиболее важной из представленных требований в контексте рассматриваемой системы является безопасность обмена данными.

В современных смартфонах существует несколько беспроводных технологий передачи данных, основные из них и наиболее распространённые:Wi-Fi, Bluetooth, NFC. В таблице 1 представлены краткие описания и примеры конкретных решений для Wi-Fi, Bluetooth LE и NFC.

Таблица 1 – Краткое описание и примеры конкретных решений для Wi-Fi, Bluetooth LE и NFC[1]

	Название модуля	Протокол	Дальность[2]	Потребляемый ток	Скорость соединения	Скорость обмена данными	Топология соединения	Цена[3]	Цена на российских ресурсах[4]
Bluetooth									
Общая характеристика	-	Bluetooth Classic	До 100 м.	До 100 мА.	3-4 сек. [1]	До 2,1 Мбит/сек.	«звезда», «точка-точка»	-	-
	-	BLE v. 4.x	До 100 м.	До 5 мА.	1-2 сек. [1]	До 270 Кбит/сек. [2]	«звезда», «точка-точка»	-	-
Примеры pcb модулей	E104-BT02	BLE 4.2	70 м	Sleep mode – 6 мкА Work – 700 мкА	1-2 сек.	270 Кбит/сек.	«звезда», «точка-точка»	2,08$	310 руб.
	E104-BT20	Bluetooth v2.1+EDR	50	Work – 54,4 мА	3-4 сек.	До 2,1 Мбит/сек.	«звезда», «точка-точка»	2.24$	280 руб.
Wi-Fi									
Общая характеристика	-	-	До 100 м.	До 250 мА.	5-6 сек.	До 600 Мбит/сек. [3]	«точка-точка», «звезда»	-	-
Примеры pcb модулей	E103-W01	802.11 b/g/n	100	Sleep mode – 900 мкА Work – от 15 мА до 170 мА.	5-6 сек.	До 54 Мбит/сек.	«точка-точка», «звезда»	1,50$	300 руб.
	ESP-03	802.11 b/g/n	100	Sleep – 860 мкА Work – до 215 мА	5-6 сек.	До 54 Мбит/сек.	«точка-точка», «звезда»	1,50 $	350 руб.
NFC									
Общая характеристика	-	-	До 10 см.	-	Доли секунды [1]	106-424 кбит/с. [5]	«точка-точка»	-	-
Примеры модулей	TRF7970A	NFC-A NFC-B NFC-F NFC-V	До 10 см.	Sleep 1 мкА Work RX – до 10 мА Work RX and TX – до 130 мА.	Доли секунды	106-424 Кбит/сек.	«точка-точка»	1$	620 руб.

[1] Часть показателей в общей характеристики и примеры WiFi, Bluetooth и NFC взяты из беспроводных pcb модулей (BLE и WiFi модули от E-BYTE [6], BLE и WiFi модули от Espressif Systems [7], NFC модули от Texas Instruments (TRF79**A)[8]).

[2] На открытой местности на высоте 2 м. (pcb антенна).

[3] Минимальная цена на Alibaba, AliExpress, eBay

[4] Минимальная цена за шт. на таких ресурсах как ChipDip и Platan.

С точки зрения безопасности, NFC является самой безопасной технологией из рассматриваемых, так как дальность его действия очень мала, из-за чего перехват данных обмена является практически невозможным. Wi-Fi является более защищенной технологией по сравнению с Bluetooth. Более высокая защищенность достигается за счет усложнения протоколов передачи данных и более сложным процессом соединения, что делает его более продолжительным.

Таким образом, исходя из требований, представленных в начале статьи, из рассматриваемых беспроводных технологий передачи данных больше всего подходит Bluetooth LE. Использование NFC неудобно из-за дальности действия (накладываются жесткие требования к расположению контроллера управления замком), несмотря на то, что Wi-Fi более защищен, потребление и скорость соединения также делают его использование неудобным.

Так как система автономная, то использование Bluetooth Classic менее предпочтительно, чем Bluetooth LE. Поэтому, выбирая из рассматриваемых технологий, предпочтительнее всего является Bluetooth LE.

Bluetooth LE удовлетворяет практически всем требованиям, предоставляемым в начале статьи. Так как наиболее важное требование рассматриваемой системы к беспроводной технологии является высокая защищенность обмена информацией, то необходимо рассмотреть вопрос безопасности технологии и возможности «атак» злоумышленников.

Особенности Bluetooth LE

Рассмотрим внутреннюю структуру Bluetooth LE.

Стек BLE состоит из двух основных частей: контроллера (Controller) и узла сети (Host). Контроллер включает в себя физический и канальный уровень и часто реализуется в виде системы-на-кристалле с интегрированным беспроводным трансивером. Часть стека, именуемая узлом сети реализуется программно на микроконтроллере приложений и включает в себя функциональность верхних уровней: уровень логической связи (Logical Link Control — LLC), протокол адаптации (Adaptation Protocol — L2CAP), протокол атрибутов (Attribute Protocol — ATT), протокол атрибутов профилей устройств (Generic Attribute Profile — GATT), протокол обеспечения безопасности (Security Manager Protocol — SMP), протокол обеспечения доступа к функциям профиля устройств (Generic Access Profile (GAP). Взаимодействие между верхней и нижней частями стека осуществляется интерфейсом Host Controller Interface (HCI). Схематично внутренняя структура BLE изображена на рисунке 1.

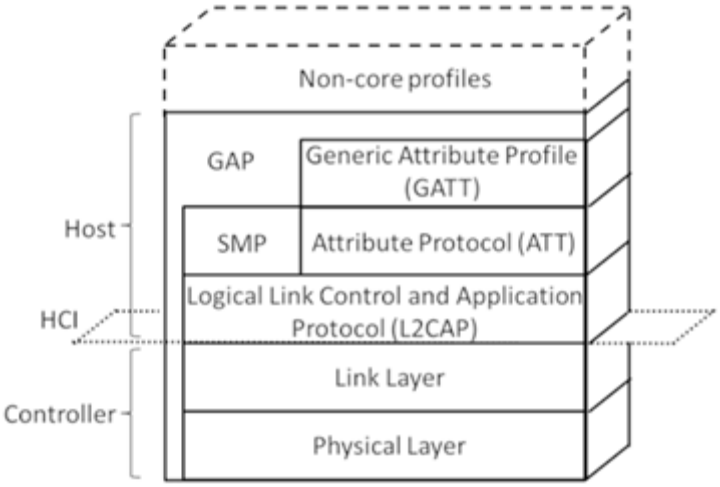

Рисунок 1 – Внутренняя структура BLE

На физическом уровне передача данных происходит в диапазоне частот ISM 2,4 ГГц с использованием частотной модуляции GFSK (Gaussian frequency-shift keying) на полосе частот 2 МГц, разделенной на 40 каналов. Три канала предназначены для широковещательной передачи данных (advertising channels), они выбраны таким образом, чтобы не пересекались с трёмя наиболее часто используемыми каналами в WiFi. Широковещательные каналы используются на GAP-уровне, а остальные 37 предназначены для передачи данных, используются на GATT-уровне [9].

Канальный уровень управляет скачкообразным переключением частоты, «рекламированием» (advertising), сканированием (scanning), инициированием подключения (initiating connections), подключением (connected). Канальный уровень BLE поддерживает шифрование и аутентификацию на основе алгоритма Cipher Block Chaining-Message Authentication Code (CCM) и блочного шифра AES-128. При использовании в соединении шифрования и аутентификации, к полезной нагрузке (PDU) добавляется четырехбайтное сообщение проверки целостности Message Integrity Check (MIC), после чего поля PDU и MIC шифруются. На данном уровне устройства подразделяются на ведомое (slave) и ведущее (master), причем ведомому устройству всегда доступна только топология «точка-точка».

Уровень L2CAP управляет потоком данных (разделяет данные, поступающие «сверху» на блоки нужного размера (22 байта)), реализует при необходимости повторную передачу данных.

GATT уровень представляет из себя иерархическую структуру хранения доступных клиенту данных [10]:

- Сервисы
- Характеристики
- Дескрипторы
- Возможные действия (read, write, notify, indicate)

ATT уровень реализует клиент-серверную архитектуру, предоставлением следующего протокола:

- команды от клиента серверу: Read (прочитать характеристику, сервис и т.п.), Write (изменить значение характеристики);
- команды от сервера клиенту: Notify (уведомить об изменении характеристики), Indicate (уведомление клиента об изменении характеристики и ожидание подтверждения о получении уведомления).

В роли сервера выступает текущее устройство независимо от того ведомое (slave) оно или ведущее (master).

SMP уровень отвечает за сопряжение устройств, обмен ключами при сопряжении и т.п. В общем случае сопряжение BLE устройств происходит в 3 этапа [10]:

1. Обмен данными о возможностях ввода/вывода устройств на канальном уровне.
2. Аутентификация соединения (формирование временного ключа для шифрования дальнейшего процесса сопряжения). Существуют несколько вариантов аутентификации:

a. Out Of Band – передача временного ключа по альтернативным каналам (например, NFC);

b. Presskey Entry – формирование ключа на основе вводимого пользователем пароля (последовательности из 6 цифр);

c. Just Work – не проводить процесс аутентификации (делает возможным атаку «человек посередине» MITM (Man In The Middle)).

3. Каждая из конечных точек соединения может передать другой конечной точке до трех 128-битных ключей, называемых Long-Term Key (LTK) – используется для шифрования на канальном уровне, Connection Signature Resolving Key (CSRK) – для подписи данных на уровне ATT, Identity Resolving Key (IRK) – для генерации частных адресов.

Уровень GAP определяет роль устройства, режим и процедуры обнаружения устройств и сервисов, управляет установлением соединения и безопасностью. В Bluetooth LE уровень GAP выделяет четыре роли для контроллера [10]:

1. Широковещательный (Advertiser). Может только передавать пакеты по рекламным каналам. Не поддерживает соединение с другими устройствами.
2. Наблюдатель (Scanner). Только прослушивает рекламные каналы (способен принимать пакеты, передаваемые Advertiser).
3. Периферийный (Peripheral). Способны поддерживать одно соединение с центральным устройством.
4. Центральный (Central). Способны поддерживать несколько соединений.

Роли центрального и периферийного узла предполагают, что устройство способно выполнять функции ведущего и ведомого, соответственно. Устройство может поддерживать несколько ролей, но одновременно активной может быть только одна из них. Обмен данными между устройствами происходит посредством изменения характеристик.

Исходя из вышесказанного о внутренней структуре Bluetooth LE технологии, можно сделать вывод, что безопасность обмена данными зависит от реализации уровней в тех или иных конкретных решениях.

Возможные «атаки» на Bluetooth LE

Рассмотрим некоторые возможные «атаки» на Bluetooth LE соединение [11]:

- Подслушивание (Sniffer): как следует из названия, подслушивание относится к стороннему устройству, прослушивающему данные, которыми обмениваются два сопряжённых устройства. Соединение между двумя сопряжёнными устройствами означает цепочку доверия. Цепь разрывается при удалении одного из устройств. Компания Nordic Semiconductor выпустила руководство для nRF Bluetooth Smart Sniffer, которое позволяет прослушивать даже зашифрованный канал связи между сопряженными устройствами [12]. Назначением данного устройства является отладка программ.
- Атаки «человек посередине» (MITM). Атаки «человек посередине» включают некоторое стороннее устройство, имитирующее легитимное, обманывая тем самым законные устройства. Имитатор заставляет поверить каждое из них в то, что они связаны друг с другом, когда на самом деле произошло подключение к имитатору (посреднику). Этот тип атаки позволяет злоумышленнику/имитатору получить доступ ко всем данным, которыми обмениваются устройства, а также манипулировать данными, удаляя или изменяя их, прежде чем они достигнут соответствующего устройства. Как было сказано раньше это возможно только при отсутствии фазы аутентификации при сопряжении.

Рассматриваемая система предоставляет высокие требования к безопасности, так как осуществляется управление замками. Из этого следует, что поверх основного стека протоколов необходимо добавить протокол обмена информацией между смартфоном и разрабатываемым устройством, который будет включать в себя свой «канальный» уровень с шифрованием передаваемой информации. Также нужно следить за тем, чтобы скорость обмена и соединения не сильно возрастала.

Вывод

Таким образом, на основе автономной распределенной системы управления запирающими устройствами был продемонстрирован процесс выбора беспроводной технологии передачи данных для управления устройством на малых или средних расстояниях.

В результате анализа доступных для смартфонов беспроводных технологий был сделан вывод, что для рассматриваемой системы оптимальным выбором является Bluetooth LE. Данная технология отличается низким энергопотреблением, близкой дальностью действия, а также приемлемыми скоростью соединения и обмена данными.

Ввиду особенностей рассматриваемой системы и выбранной технологии, необходимо предусмотреть следующие положения при использовании Bluetooth LE в качестве технологии передачи данных:

1. Соединение следует осуществлять без аутентификации, так как она слишком затягивает процесс соединения, который часто производится в распределённой системе.
2. Ввиду отсутствия механизма аутентификации и наличия повышенных требований к защищённости обмена данными, поверх основного стека протоколов следует предусмотреть дополнительный протокол обмена данными между смартфоном и контроллером замка, который будет включать в себя дополнительное шифрование данных перед отправкой по Bluetooth-каналу. Данная тема выходит за рамки текущей статьи.

Список литературы

1. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology [Electronic resource]/ URL: https://www.mdpi.com/1424-8220/12/9/11734/htm (Date of treatment 23.09.2020).
2. Как выбрать лучший протокол Bluetooth для своего приложения [Электронный ресурс] / Режим доступа: https://spb.terraelectronica.ru/ news/6121 (Дата посещения 23.09.2020).
3. WiFi, Bluetooth или Zigbee – какой стандарт лучше? [Электронный ресурс] / Режим доступа: http://ua.automation.com/content/wifi-bluetooth-ili-zigbee-kakoj-standart-luchshe (Дата посещения 22.09.2020).
4. NFC: Разбор технологии Near Field Communication [Электронный ресурс] / Режим доступа: https://habr.com/ru/company/droider/blog/5041 96/ (Дата посещения 21.09.2020).
5. ГОСТ Р ИСО/МЭК 18092-2015 Информационные технологии (ИТ). Телекоммуникации и обмен информацией между системами. Коммуникация в ближнем поле. Интерфейс и протокол (NFCIP-1).
6. URL: http://www.ebyte.com/en/product-class.aspx (Date of treatment 23.09.2020).
7. URL: https://www.espressif.com/ (Date of treatment) (Date of treatment 23.09.2020).
8. URL: https://www.ti.com/ (Date of treatment) (Date of treatment 23.09.2020).
9. Bluetooth low energy technology [Electronic resource] / URL: https://www.compel.ru/wordpress/wp-content/uploads/2012/04/Bluetooth_ low_energy_technology.pdf (Date of treatment 23.09.2020).
10. Для мобильных стражей: беспроводной стандарт Bluetooth Low Energy в системах безопасности [Электронный ресурс] / Режим доступа: https://www.compel.ru/lib/53866 (Дата посещения 23.09.2020).
11. Что такое Bluetooth Low Energy (BLE) и как его взламывают [Электронный ресурс] / Режим доступа: https://hackware.ru/?p=9757 (Дата посещения 23.09.2020).
12. nRF Sniffer User Guide v 1.1 [Electronic resource] / URL: https://infocenter.nordicsemi.com/pdf/nRF_Sniffer_UG_v1.1.pdf (Date of treatment 23.09.2020).

References

1. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology [Electronic resource]/ URL: https://www.mdpi.com/1424-8220/12/9/11734/htm (Date of treatment 23.09.2020).
2. Как выбрать лучший протокол Bluetooth для своего приложения [Электронный ресурс] / Режим доступа: https://spb.terraelectronica.ru/ news/6121 (Дата посещения 23.09.2020).
3. WiFi, Bluetooth или Zigbee – какой стандарт лучше? [Электронный ресурс] / Режим доступа: http://ua.automation.com/content/wifi-bluetooth-ili-zigbee-kakoj-standart-luchshe (Дата посещения 22.09.2020).
4. NFC: Разбор технологии Near Field Communication [Электронный ресурс] / Режим доступа: https://habr.com/ru/company/droider/blog/5041 96/ (Дата посещения 21.09.2020).
5. ГОСТ Р ИСО/МЭК 18092-2015 Информационные технологии (ИТ). Телекоммуникации и обмен информацией между системами. Коммуникация в ближнем поле. Интерфейс и протокол (NFCIP-1).
6. URL: http://www.ebyte.com/en/product-class.aspx (Date of treatment 23.09.2020).
7. URL: https://www.espressif.com/ (Date of treatment) (Date of treatment 23.09.2020).
8. URL: https://www.ti.com/ (Date of treatment) (Date of treatment 23.09.2020).
9. Bluetooth low energy technology [Electronic resource] / URL: https://www.compel.ru/wordpress/wp-content/uploads/2012/04/Bluetooth_ low_energy_technology.pdf (Date of treatment 23.09.2020).

10. Для мобильных стражей: беспроводной стандарт Bluetooth Low Energy в системах безопасности [Электронный ресурс] / Режим доступа: https://www.compel.ru/lib/53866 (Дата посещения 23.09.2020).
11. Что такое Bluetooth Low Energy (BLE) и как его взламывают [Электронный ресурс] / Режим доступа: https://hackware.ru/?p=9757 (Дата посещения 23.09.2020).
12. nRF Sniffer User Guide v 1.1 [Electronic resource] / URL: https://infocenter.nordicsemi.com/pdf/nRF_Sniffer_UG_v1.1.pdf (Date of treatment 23.09.2020).