Multi-hop communication in Bluetooth Low Energy ad hoc network

Seminar I

Branko Skočir

Supervisor:
dr. Franc Novak

Approved by the supervisor: _____________________________

(signature)

Study programme:
Information and Communication Technologies

Master degree

Ljubljana, 2014
Abstract

In this paper an overview of Bluetooth and Bluetooth low energy (BLE) standard is presented which is making a great impact as the lead communication standard in the field of internet of things in home automation. Paper is divided into three parts: in the first part the problem of multi hop data transfer in Bluetooth and BLE is presented. In the second part Bluetooth and BLE are reviewed and ad hoc networks using Bluetooth and BLE are described. In the third part the problems in BLE multi hop data transfer are addressed and possible solutions are indicated. In the last chapters further work is given and some conclusions are drawn.

Keywords: Home automation, Internet of Things, Bluetooth, Bluetooth Low Energy, Piconet, Scatternet, Mesh, Single hop, Multi hop, Single mode, Dual mode
1 Definition of the problem

In our everyday life we come across increasing number of home appliances with smart embedded systems. They can be as simple as temperature reader with display, status reporting interface, timers, counters, etc. More evolved systems have already built in controller functions such as air conditioning, heating, and ventilation. Furthermore, the latest appliances can also have embedded communication systems that can communicate with designated recipient. Such systems are creating an internet of things in our homes, cars, public buildings, transportation, and industry. The systems can be connected by variety of communication interfaces. Bluetooth communication interface is one of the most common communication interfaces. It was standardized by Bluetooth SIG group. Recently the standard focused on energy efficiency resulting in Bluetooth Low Energy (BLE) standards.

Although Bluetooth was initially designed as a replacement for RS-232 wire connections and it quickly evolved and become a standard for connecting devices in short range proximity. The Bluetooth devices can create a personal area network using a piconet and scatternet topologies. The Bluetooth standard evolved to Bluetooth Low Energy (BLE) standard. Standard is primarily designed for wireless sensors. According to BLE standard only point to point or piconet connections are allowed. For example, multiple sensors can connect to a master device like smart phone but cannot be connected with each other or send data over multiple devices using multi hop method. For multi hop communication the data is traveling over multiple routing devices. Every passing of a router is a single hop. The goal is to create a method where a multi hop routing would be possible with BLE devices. The problem occurs because the BLE devices can only take single mode at a time: the master mode (receiver) or the slave mode (transmitter). To solve this problem, a device must perform a switching sequence between the master and slave mode and in the mean time data that needs to be relayed forward must be stored.

Multi-hop methods are presented in [14] and [15]. In the first method [14] the BLE devices are used as a sensors sending data to the gateway in one direction over the network and creating a multi hop data transfer. The second method [15] uses the BLE devices also as a bidirectional routers so the data can travel in both directions. Both methods use a table routing system for relaying the data to desired nodes. In this paper the Bluetooth multi-hop techniques described in [14, 15] are extended to establish the multi-hop data transfer in the BLE environment.
2 Overview of the research

2.1 Home automation

The first experimental home automation was created as a home computer in the 1966. The inventor was James Sutherland and the computer was called Electronic Computing Home Operator or ECHO IV. It was built from surplus computer parts like memory, CPU and I/O units that were enclosed in two wooden boxes weighing over 360kg. It could do different computations like managing the finances, store shopping lists, track family inventory, control home temperature and turn appliances on and off [1] [2].

Home automation derives from building automation and has since then with introduction of the microcontroller evolved into its own branch. The automation of individual controlled appliances and devices is increasing every day. For example the heating system can be controlled in regard to the temperature or the occupancy of the building. The ventilation and the air conditioning can also be controlled and regulated in the same regard. Lighting and multimedia centers can be set up to accommodate the individual needs and wishes. Security and surveillance is achieved with different sensors and modes for notifying the property owner that the intruder is present in the building. If this systems are obtained as standalone systems they must also operate as such, which in turn increase the maintenance effort within the building. So the need for central system that will combine all these sub systems become more and more evident.

Only with the use of computer and information technology the home automation started its breakthrough. All the subsystems can now be integrated in centralized control unit. Control unit receives the data from all the sub systems. For instance inside and outside temperature, humidity, on/off light status, window blinds position, open/closed window status, stocked refrigerator, gas leak, smoke detection, presence of a person etc. The control unit reacts and manipulates the actuator with respect to the received data from sensors. The actuators can be a simple switches to turn the light on or off, they can be electrical valve to turn the water for the sprinklers on or off or it can be a driver for electrical motor that is lifting or lowering the window blinds. More advanced regulation methods like a PID regulators are often used in an air conditioning, ventilation and heating system1.

All these appliances and systems must be somehow connected to the central unit. This can be achieved either through the wired network or through the wireless network. After the connection and communication is achieved we have a network of connected systems called also the internet of things (IoT) [3]. Furthermore the

1 http://en.wikipedia.org/wiki/Home_automation
control unit can now be accessed via remote computer or smart device by appropriate software.

2.1.1 Internet of Things

IoT was first developed as an RFID system in which every object has its own RFID tag. Tracking of the objects was performed through the network of RFID readers. Today we can describe internet of things as a network of interconnected devices that can be aware of their surroundings, collect data, send and receive the data to and from other devices and interact to the surroundings and people, accordingly [4]. In home automation these include various everyday devices such as smart phones, sensors, actuators, home appliances, security systems, heating, ventilation and air condition systems. Depending on the technology they are build with devices that are using different connection options. One common option is also Bluetooth.

2.2 Bluetooth

Bluetooth is a communication standard for creating a personal area network (PAN) that incorporates various communication protocols. It was first developed in 1994 at Ericsson Company. Later the standard was adopted by other companies that formed a Bluetooth Special Interest Group (SIG). Bluetooth operates in a 2.4GHz to 2.485GHz radio frequency range called unlicensed industrial, scientific and medical (ISM) band. A frequency hopping spread spectrum (FHSS) method is used for communication. With this method the communication frequency is constantly changing within the ISM band and hopping between channels reaching up to 1600 hops per second. Each channel can be 1MHz wide so the band is filled with 79 channels. This method provides security and reduces the interference.

Bluetooth protocol stack is composed from various layers that are broadly divided into the controller and host stack as shown in Figure 1. The lowest control layer is a radio frequency layer (RF). It is responsible for the radio transmission of the data between the master and the slave. It operates in the 2.4GHz ISM band in the range of 10 meters and performs frequency hopping with 1600 hops/s. Second layer is a baseband (BB) layer that manages the frequency hopping, error correction, flow control, security and connection modes. Two links can be established between Bluetooth master and slave device. The synchronous connection oriented (SCO) link and asynchronous connection less (ACL) link. The audio is transferred directly from baseband to the application layer through SCO link while the data is transmitted over the ACL to the link manager protocol (LMP). LMP is responsible for link setup, authentication and configuration. Next is the host controller interface (HCI) that provides the communication between the controller.

---

2 http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum
and the host stack. It incorporates different HCI transport layer standards like USB and UART. The lowest layer in the host stack is logical link control and adaptation protocol (L2CAP). It is responsible for communication through the ACL link and used for data transmission to the upper layers. The L2CAP provides data multiplexing, segmentation and reassembly of packets and quality of service (QoS) to the upper layers. Three layers after the L2CAP are radio frequency communication layer (RFCOMM), service discovery protocol (SDP) and telephony control protocol specification binary (TCSBIN). RFCOMM is a serial port emulation protocol providing a serial port connectivity. SDP provides the information of services available from and to other devices. TCSBIN provides the instructions for establishing the calls between two Bluetooth devices. From here the upper layers define the applications and profiles in the host stack.

#### Applications/Profiles

- RFCOMM
- SDP
- TCSBIN
- L2CAP
- HCI
- LMP
- BB
- RF

**Figure 1: Bluetooth protocol stack**

Bluetooth is an excellent communication standard for transferring data between devices that have sufficient energy supply, however for devices relying on a lower capacity energy source a new standard was introduced. This is Bluetooth Low Energy (BLE) or Bluetooth Smart.

### 2.2.1 Bluetooth low energy – Bluetooth Smart

Bluetooth Low Energy (BLE) is a Bluetooth wireless technology that enables communications in a wireless personal area network. It was specially designed to have very low power consumption and thus suitable for coin-cell battery devices such as watches, toys, sport and fitness devices, health care devices and entertainment devices. BLE uses the same radio frequency range as the classic Bluetooth, although each channel is 2MHz wide, this in term reduces the number of channels to 40. Communication is established through advertising, scanning and initiation. BLE devices use three channels for the advertising their presence and scanning for other devices. Once the connection initiation is sent, the advertiser
must switch to slave mode and the initiator is switched to the master mode. Like classic Bluetooth, BLE also uses the FHSS method to allow previous Bluetooth version compatibility, minimize the interference and maximize security. To minimize the power consumption the BLE was developed for small data transfer. Consequently the data throughput of the BLE is quite smaller compared to the data throughput of a classic Bluetooth that can reach up to 24Mbps. The BLE throughput is reach up to 100 kbps. Due to the low power consumption of BLE devices they are suitable for battery operated sensor networks and IoT in home automation.

Another difference between classic Bluetooth and BLE is their protocol stack shown in Figure 2. The BLE stack is divided into two parts: controller for the lower layers and host for the upper layers. First layer from the bottom control part is physical layer (PHY) that incorporates the RF transceiver and manages the physical data transfer between devices. Next is link layer (LL) which is responsible for packet structure and control and third the host controller interface for the controller and host stack connectivity. The lowest two layers in the host stack are generic access profile (GAP) and logical link control and adaptation protocol (L2CAP). GAP is an interface for the applications responsible discovery of other BLE devices and enabling different modes of operation like advertising and scanning. L2CAP is responsible for data multiplexing, segmentation and reassembly of packets. Above the L2CAP layer are security manager protocol (SMP) and attribute protocol (ATT). The SMP is used for pairing and creation and distribution of the AES-128 keys. The ATT profile exposes and recognizes the attributes to and from other BLE device. Next layer that is bounded to GAP, SMP and ATT is generic attribute profile (GATT). On the base of ATT attributes GATT determines the framework for the attribute exchange from one device to another and transmits the meaningful data through application profiles to the user applications [6].

![Figure 2: Bluetooth low energy protocol stack](image-url)
Connected Bluetooth devices form different ad hoc network topologies like piconet, star or scatternet topology described in one of the next sections.

2.2.2 Single mode and dual mode bluetooth devices

Most of the devices today only support the classic Bluetooth communication and cannot benefit from new technology. For this purpose single and dual mode functionality of the Bluetooth devices was introduced. Single mode devices support only one type of Bluetooth either Classic or BLE. Dual mode devices are equipped with dual mode module and can communicate with classic Bluetooth devices or BLE devices. Latest technology allows also simultaneous communication with classic and BLE devices. New marking was introduced in this regard where dual mode devices are marked as Bluetooth Smart Ready and BLE devices are marked as Bluetooth Smart3.

2.2.3 Available technology

Although the technology today in BLE is still evolving a selection of suitable BLE modules for further work research in multi hop routing was created. They are presented in Table 1.

<table>
<thead>
<tr>
<th>BLE112</th>
<th>BLE113</th>
<th>BTM800</th>
<th>AMB2620</th>
<th>PAN1026</th>
<th>OBS421</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Classic Bluetooth</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Master/Slave mode</td>
<td>✓</td>
<td>✓</td>
<td>/</td>
<td>✓</td>
<td>/</td>
</tr>
<tr>
<td>Added OS support</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>Android</td>
</tr>
<tr>
<td>UART Interface</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Transmit power</td>
<td>+3dBm to -23dBm</td>
<td>+0dBm</td>
<td>Up to +7,5dBm</td>
<td>4dBm</td>
<td>4dBm</td>
</tr>
<tr>
<td>RX sensitivity</td>
<td>-85dBm to -91dBm</td>
<td>-93dBm</td>
<td>-92,5dBm</td>
<td>Up to -93dBm</td>
<td>-87dBm</td>
</tr>
<tr>
<td>Simult. slave connections</td>
<td>4+</td>
<td>Up to 8</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Power supply</td>
<td>2V to 3,6V</td>
<td>2V to 3,6V</td>
<td>1,8V to 3,6V</td>
<td>2V to 3,6V</td>
<td>2,7V to 3,6V</td>
</tr>
<tr>
<td>Average TX consumption</td>
<td>27mA@3V</td>
<td>18,2mA@3V</td>
<td>16mA@3V</td>
<td>&lt;25mA@3V</td>
<td>46mA@3V</td>
</tr>
<tr>
<td>Minimal consumption</td>
<td>0,4μA@3V</td>
<td>0,4μA@3V</td>
<td>&lt;0,5μA@3V</td>
<td>&lt;0,3μA@3V</td>
<td>Idle 7,8mA@3V</td>
</tr>
<tr>
<td>Class</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1: Selection of single and dual mode BLE modules (/ - no data available)

---

Even though the Bluetooth Class 2 is more suitable for use in home automation because of its medium transmit power, Class 1 module OBS421 and Class 3 BLE113 were also presented in the table for comparison purposes between classes. All modules support the BLE and UART communication. All of them can be powered with the CR2032 button battery that has 3V nominal voltage with 225mAh typical capacity\(^4\). Another important feature that the module must support is capability of operating in both master and slave mode. That information is only available for four modules and which makes them more suitable for the network implementation. It is obvious that the dual mode modules have significantly bigger average transmit power consumption then single mode and added OS support with the development package. The transmit power of the modules also varies with respect to the module Class shown in Table 2. The only deviation is the case of BTM800 module which should be classified as Class 1 module but it is advertised\(^5\) as Class 2. Taking into account that Class 2 transmit power is more suitable choice for home automation the BTM800 would be less appropriate for the application.

<table>
<thead>
<tr>
<th>Class</th>
<th>Permitted power</th>
<th>Typ. range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100mW</td>
<td>20dBm ~100m</td>
</tr>
<tr>
<td>2</td>
<td>2,5mW</td>
<td>4dBm ~10m</td>
</tr>
<tr>
<td>3</td>
<td>1mW</td>
<td>0dBm ~1m</td>
</tr>
</tbody>
</table>

Table 2: Bluetooth classes

2.2.4 Piconet

A piconet is a network of two or up to eight Bluetooth devices communicating with each other on the same channel. One master device and seven active slave devices. In BLE environment the devices are in either the advertising mode or the scanning mode. Device that is advertising its presence assumes the role of a slave device and the device that is scanning will assume the role of master device. The master device is responsible assigning each slave with its own transceiver timeframe and determining the FHSS in order to avoid collision and overlapping\(^6\).

In BLE the device identification in the piconet network is performed with a 32-bit address. With respect to the time between the start of the consecutive connection event, which is between 7,5ms and 4s, the number of connected slaves are from 2 to 5917 [6]. As mentioned before master can have up to seven active slaves. All slaves that have been recognized by the master and are not in the active connection can be put into park state by the master but still maintain synchronization. When slaves are in park state all ACL and SCO traffic is stopped. Only small data transmission is enabled for maintaining the synchronization. Master

\(^4\) [Link](http://en.wikipedia.org/wiki/CR2032_battery)
\(^5\) [Link](http://www.lintech.de/entwicklung/bluetooth-oem-module/)
\(^6\) [Link](http://en.wikipedia.org/wiki/Piconet)
can activate parked slave after sending an initiate message to the slave and receives a request message. After receiving a request message the message is sent to the slave with the unpark procedure\(^7\).

Multiple piconets can be connected together through a mutual slave or a master/slave node. That kind of topology is called a scatternet.

2.2.5 Scatternet

If piconet is a group of slave nodes connected to one master node then scatternet is a group of piconets connected together forming a network tree [10]. Piconets are connected together through a common slave node or a node that is a master to one piconet and slave to another. In the scatternet there is no direct connection between two master nodes and data relaying between piconets can only be managed through the common slave node. Though there are many solutions for classic Bluetooth scatternet [11] [12] [13] there are none for Bluetooth low energy. Bluetooth scatternet is shown in Figure 4.

---

\(^7\) [Link to Data Transport Page](https://developer.bluetooth.org/TechnologyOverview/Pages/DataTransport.aspx)
2.3 Wireless mesh network

In wireless mesh network every node can be connected to its surrounding nodes. Every node is aware of its surrounding nodes and every node can relay the data from a surrounding node to another surrounding node. Such nodes are called routing nodes. In this kind of connection every node can participate in data distribution\(^8\).

In wireless mesh network is constructed from strategically positioned routing nodes. When routing nodes are not known in advance or the nodes are mobile, a dynamic mobile ad hoc network structure is formed.

2.3.1 Mobile ad hoc network

A mobile ad hoc network (MANET) has its origins in defense advanced research project agency (DAPRPA) pocket radio network (PRNet) from 1972. Survivable adaptive radio network (SURAN) was introduced in 1983 to improve the PRNet. In the 1994 DARPA started a global mobile information system program (GloMo) for exploration and research of MANET [7] [8].

Today we can describe mobile ad hoc networks as wireless interconnected device network in which each device can be a transceiver and a router. MANET is network formed out of necessity and does not need any support from existing network infrastructure. Network is formed arbitrary and heterogeneous [9].

Mobile ad hoc network allows spontaneous changes in routing if the network formation is changing. For example if one node in the network changes position or is not available any more the routing protocol must be changed accordingly. Data transfer between nodes can be accomplished with single hop data transfer or with multi hop routing.

2.3.2 Single hop and Multi hop

In a network nodes are connected through the various routers and gateways. When information is destined to a remote node in the network it must pass certain number of routers and gateways. Every pass over router is a hop\(^9\). In a Bluetooth ad hoc network like scatternet topology the data transfer is also performed with a hop if it goes through a slave node with two masters. However if the scatternet is more complex even multiple hops are possible. The route of multiple hops in a scatternet can be determined by the use of different protocols and techniques [11] [12] [13]. There has been however only one suggestion [14] for multi hop data transfer for the

---

\(^8\) [http://en.wikipedia.org/wiki/Mesh_networking](http://en.wikipedia.org/wiki/Mesh_networking)

3 Related work and critical judgement

As mentioned in previous section only one proposal and one application of that proposal was already developed for BLE multi hop routing. The suggestion by [14] is to build the routing table from gateway (GW) up if the nodes are connecting one by one to the network. Nodes are constructed from Arduino template and BLE112 module and have a function of a sensor. Nodes are programmed to send an advertising broadcast of their presence and information of the metric distance with received signal strength indication (RSSI) every 30 seconds. Advertising node then receives a confirmation from the closest neighboring node that it is connected to the network with the information of primary node route to the GW according to the RSSI information. The broadcast is then repeated every 30 seconds with same basic information about the node and a routing table is updated accordingly. GW on the other hand is constructed with the IP network interface and it sends the data received from the sensors to the database. All the data is travelling from the sensors to the GW as shown in Figure 5 thus creating a data flow towards the GW. The implementation however was not realized due to the technology limitations at that time. However there are various scenarios and suggested methods of a mobile ad-hoc network in the work.

![Figure 5: Suggested information flow from [14]](image)

In [15] similar hardware was used but different approach for route discovery called multi hop transfer service (MHTS). It was implemented on top of the GATT layer. The route is created on each node separately with assumption that the address of the destination node is known to the initiator node. Communication in this case is bidirectional so they use two more routing tables. In the implementation four nodes were used. The total time that includes the route searching and 13 byte data transmission was 25 seconds on average. When the route was discovered data transfer time was from 6 to 9 seconds. Main two disadvantages that [15] acknowledges are the realization of the switching between the master/slave mode and the shortage of the RAM available on the modules.
In the first method the network is designed as a sensor network. This means that the communication will be mostly one way from the sensor to the gateway. This kind of network is primarily useful in the environment where only monitoring is required, e.g. monitoring the vital functions of a patient. In home automation where bidirectional communication is needed the second method is more applicable. Although the method is using the bidirectional communication the main problem is in establishing the connection which leads to the significant increase in total time of data transmission.

4 Further work

Both the above methods for creating a multi hop data transfer have their advantages and disadvantages as described in previous chapter. Our goal is to take the advantages of both methods and create a new method. With the new method all the data will still be traveling towards the gateway (GW) such as smart phone but the GW will be also capable of communicating with the distant devices. So the data transfer will be bidirectional. The routing table will be created from the GW and informing the nodes about the routing. In this case the nodes are not preoccupied with the routing table creation. GW will collect necessary data for creating a routing table from each node and calculate the best route for data transfer. Best route will then be transferred to the nodes but each node will only receive the routing table of first hop direction to the main device and first hop direction to the next device in a line from the opposite direction. This way we will try to minimize the routing data stored on the nodes. The sent data from GW will incorporate the recipients address so each node will check if it is the recipient, otherwise it passes the data forward until it reaches the recipient. The acknowledgement of data transfer will only be carried out between directly connected nodes.

Future work will be initially dedicated to further research of BLE communication protocols and data stack. After that the purposed method will be further developed and analyzed. Next step will be the selection of the proper BLE module from the currently available technology in regard to its capability, price and availability and test the method in practical implementation.
5 Conclusion

Bluetooth low energy is an increasingly growing technology for the personal area network and sensor network today. Although the standard has been present for over four years the technology is only recently started to gain the momentum\textsuperscript{10}. By the year of 2018 more than 90 percent of smart phones are supposed to be Smart ready devices\textsuperscript{11}.

In this paper we have presented an overview of the research in the Bluetooth and Bluetooth low energy technology. The protocol stacks of both standards were introduced. Different topologies that are used in both Bluetooth standards and other wireless communication standards were described. Differences between Bluetooth and BLE standards are presented and currently available technology overview is shown. The most significant difference is however the lack of research in multi hop data transfer on BLE for which suggestions are presented and discussed in related work and critical judgment chapter.

In the last part of the paper future work is presented with two suggestions that have yet to be investigated. From the available technology section the comparison of the different available modules will be used for selection of the suitable device and creation of the network in the practical implementation.

\textsuperscript{10} http://en.wikipedia.org/wiki/Bluetooth_low_energy
\textsuperscript{11} http://www.bluetooth.com/Pages/Mobile-Telephony-Market.aspx
References


[7] Lu Han, Wireless ad hoc networks, October 8, 2004

[8] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges


[15] Konstantin Mikhaylov and Jouni Tervonen, Multihop Data Transfer Service for Bluetooth Low Energy