Bluetooth within Internet of Things

Internet of Things (IoT) generally refers to embedded devices that connect to the internet in order to complete specific tasks, and this has significantly flourished in recent years (Aftab, M.U, 2017). Devices and products of IoT can include, according to the category they fall under, smart sensors which, for example, adjust the temperature and lightening in a room (Rouse, M, 2018) and Alexa, Amazon's Bluetooth speaker which can be turn on and off and change songs only by speaking it out loud. Other IoT products, such as Google Home which can answer questions, are more functional and enable people to send messages to friends or call them.

On this basis, IoT requires a communication method to connect with smarter devices which enables them to complete the given tasks. A notable and important communication method which has been significantly developed throughout recent times in IoT devices is Bluetooth. In 1994, Bluetooth was invented by Ericsson and has been ever since a fundamental part in technological devices. Moreover, Bluetooth is found nowadays in devices ranging from phones, computers and game consoles to smart devices such as smart watches and smart Home system.

As a short-range method of communication, Bluetooth exchanges data such as files, or individual data such as time. This is further done by the Master/Slave communication method between Bluetooth connected devices. This is where a Master Bluetooth device is responsible for initialising to embedded systems connected to it, which are referred to as Slave devices. (Altium, D, 2017). A Master Bluetooth device can send and/or receive data from a Slave device connected to it, whereas a Slave device can only send and/or receive data from its Master device and is unable to communicate with other Slave devices. A Slave will normally begin by advertising and broadcasting their data, meaning that this will allow other devices to find its IP address. The next step is to wait for the devices which want to communicate with it. This process is being regulated by the Generic Access Profile (GAP), which "is responsible for managing connections, advertisements, discovery and security features", as Afaneh explains (Afaneh, M. 2017). Further in this process, a Master or a Slave will try to connect to the device and then the connection is completed by the Master device, which will allow the devices to communicate with each other in private (Townsend, K., 2019). This is done by the Generic Attributes Profile (GATT).

GATT defines the way Bluetooth devices transfer data between themselves. It must be noted that connections made via GATT are exclusive connections, meaning that a Slave device can be connected to a Master device one at a time (Townsend, K, 2019). For instance, if the Slave device wold be a heat sensor, this would be broadcasting its data to the Master device in order for it to read it. Then the Master device will apply the data processed from the Slave device as it sees fit.

In contrast with the GATT connection, in Bluetooth connections a Master device can connect to eight Slave devices at a time. When two or more Slave devices are connected to a Master device, this is called a Piconet (Techopedia, 2019). Additionally, when two or more

Bluetooth-enabled devices are networked by at least two or more piconets, this is called a Scatternet (Techopedia, 2019). This becomes sufficient in Bluetooth 5, as well as in the use of IoT products which will further be discussed in this paper.

Within the IoT products, a subsection of Bluetooth 4 has been developed, namely Bluetooth Low Energy (BLE). BLE was specifically designated to provide significantly lower consumption, in contrast with the classic Bluetooth, and it is commonly used for the transfer of small amounts of data between nearby devices and to interact with proximity sensors, which allows users to get a customized experience based on their current location (Android Developers, 2019). In the structure of a BLE device, there are 3 main software levels which need to be noted: Application, Host and Controller. The Application level interfaces with the stack and helps implement the specific user application. The Host is the higher level of the stack, while the Controller is the lower level of the stack and they communicate with one another via the Host Controller Interface (HCI) (Afaneh, 2017).

Another innovative networking has been introduced in Bluetooth 5.0, more specifically Bluetooth Mesh (BM). The way in which BM works is that scatternets allow piconets to communicate with each other and this further allows multiple Bluetooth devices to reliably and securely communicate with each other (Kolderup, K. 2017). Harrel provided the following example as BM: "When you unlock your front door, the lights in the foyer come on, the motion sensors on your alarm system turn off, the thermostat starts the air conditioning and your entertainment system starts playing your favourite music – all before you put your keys down!" (Harrel, W. 2017). Before BM, devices had to be nearby in order to connect to each other. However, this is not the case anymore as BM connects to their destination via nearby devices, which now makes the devices to be able to become both Master and Slave devices, thus allowing Mesh to function.

Bluetooth has become a well-known method of networking nowadays and, as already mentioned, can be used to send information from a device to another, for example from your phone to a smart device or vice versa. Within a BLE device, data can be sent periodically within a distance varying between 30 to 100 meters and the respective data can include the temperature, the time or the heart rate (Afaneh, M. 2017). Crucially, the introduction of Bluetooth 5 makes Bluetooth much more accessible by including an increased packed size over a wider range and with a higher speed. Bluetooth 5 has a doubled speed of 2mb/s in contract with BLE which stands at 1mb/s. That being said, Bluetooth 5 was designed bearing in mind the IoT and therefore keeping the low energy and low value that enabled BLE to be a viable option in the first place (McClelland, 2017).

From a security perspective, Bluetooth is considered to be rather secure, although it has its occasional flaws, like any other popular communication method. Two of the main reasons for which Bluetooth is considered to be a fairly secure form of communication between devices are that it requires the devices to be relatively nearby and that it required both devices to accept to communicate to each other, thus making it harder for hackers to gain access over any of the devices. There are three basic means of providing Bluetooth security, namely Authentication, Confidentiality and Authorisation. However, the security measures provided by the Bluetooth specifications detail 4 Bluetooth security modes. Mode 1, is a non-secure mode which has no authentication and allows you to connect to any device. Mode 2 has some authentication and encryption mechanisms, but they are implemented at the LMP layer (below L2CAP). Mode 3

initiates the security procedures before any physical link is established. This can be done, for example, by copying of confirming a number shown on one device on the other device. Mode 4 goes beyond this and uses Elliptic Curve Diffie Hellman (ECHD) techniques for key exchange and link key generation (Electronics Notes, 2017). Taking this into account, the older the device is, the more unlikely to be secure. However, as the majority of IoT devices are now modern, they will be using the latest Bluetooth security system, which is either BLE or BM (Electronics Notes, 2017).

Nonetheless, one concerning security problem which can commonly arise within a Bluetooth connection is hacking one or both of the connected devices. Hacking in these regards can come under three shapes, respectively Bluejacking, Bluebugging and Car Whispering. Bluejacking is not considered as a malicious security problem, although it involves the misleading of the recipient into reading messages as they appear to be from a supposedly known contact (which is not). Bluebugging allows hackers to access a connected device, for example a phone, and use all of its features. This can include sending messages or placing calls while the owner is not aware that his/her phone has been hacked. Car Whispering is a less encountered form of Bluetooth hacking, but involves the use of a software which enables hackers to send and receive audio to and from the Bluetooth enabled car stereo system (Electronics Notes, 2017).

From the competitive point of view, it can be argued that Bluetooth has competition on the basis of close-by methods of communication between devices in IoT. Currently, Wi-Fi is considered to be the most realistic competitor of Bluetooth, as the amount of throughput of Wi-Fi is considerably higher than the one in Bluetooth. Some advantages of Wi-Fi are that Wi-Fi is configured in more devices as standard, it has a low cost of infrastructure and devices and it can easily be deployed. It is sometimes the obvious choice for IoT connectivity; however, this does not necessarily mean it is the best option (Parekh, J. 2017). In contrast, due to the lower amount of energy that requires, the cost of Bluetooth seems more appealing to users. BLE an BM use a considerably less amount of energy in comparison to Wi-Fi, and more specifically, the introduction of BM makes Bluetooth connectivity between devices a better option. This is because Bluetooth allows a network to expand if a device is nearby in order for a signal to be sent, whereas Wi-Fi connected devices need to be close to the access point, or else the speed might be affected and this can further affect the ability to perform the given task (Parekh, J. 2017).

Another technological device that can be argued to compete with Bluetooth is a Low Power Wide Area Network (LoRaWAN). For the purposes of this paper, LoRaWAN and LoRa will be used interchangeably. LoRa is intended to be a low cost, open standard with a wide range of up to 10 miles and this has seemed to be well received by the users (Farnell, 2017). Other advantages of LoRa include the fact that LoRa has up to 10 years' battery life, it considerably improves the robustness to the interference, noise and jamming, has high accuracy with regards to localisation and ranging and, crucially, that the sensors can be placed across a large area, without any other sensors in proximity to send back signal to the initial target (Farnell, 2017). LoRa claims to provide a secure, bi-directional data transfer at the end-point and to be license-free, however the non-implementation in many devices nowadays makes it a less appealing option to developers (Farnell, 2017). In contrast, Bluetooth connectivity and its increased implementation in devices makes Bluetooth a more tempting option to use, despite its lower range.

In conclusion, IoT has become an increasingly developed field of technology, as well as Bluetooth within it. As one of the core principles of Bluetooth, BLE has enabled connected devices such as smart phones or smart watches to perform the way they do now and helped developers consider BLE as one of the best options due to its low cost and low energy. The establishment of Bluetooth 5 and BM has allowed the IoT industry to think and develop new possibilities within connected devices, such as adjusting an entire building's lighting and temperature from your phone, unlike what can be seen with Wi-fi application. From the security perspective, Bluetooth connectivity has never been stronger provided the security steps are followed, which makes it harder for the hackers to take control over the devices. Although there are some other communication devices which can be able to compete with Bluetooth, the aforementioned has deeply bonded with IoT and became one of the fundamental standards in an IoT device, thus making it more complicated for other ways of device communication to compete with it.

Bibliography

Afaneh, M. (2017) Bluetooth Low Energy (BLE) and Internet of Things (IoT) Available from: https://www.linkedin.com/pulse/bluetooth-low-energy-ble-internet-things-iot-mohammad-afaneh/ / [Accessed 30th March 2019]

Aftab, M.U. (2017) Building Bluetooth Low Energy Systems: Packet Publishing.

Altium Design (2017) Embedded System's Master/ Slave Communication Model Available from https://resources.altium.com/pcb-design-blog/important-considerations-in-your-embedded-systems-master-slave-communication-model [Accessed on 30th March 2019

Android Developers (2019) Bluetooth Low Energy Overview. Available from https://developer.android.com/guide/topics/connectivity/bluetooth-le [Accessed on 30th March 2019]

Electronics Notes (2017) Bluetooth Security. Available from https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php [Accessed on 1st April 2019]

Ericsson (2012) Bluetooth inventor nominated for top European honor. Available from: https://www.ericsson.com/en/news/2012/6/bluetooth-inventor-nominated-for-top-european-honor [Accessed 30th March 2019]

Farnell (2017) The LoRaWAN as an IoT Network Solution. Available from https://uk.farnell.com/lorawan-as-an-iot-network-solution# [Accessed on: 1st April 2019]

Harrel, W. (2017) In a world saturated in Wi-Fi, there's still room for Bluetooth Mesh. Available from: https://www.digitaltrends.com/computing/bluetooth-mesh-networks/ [Accessed on: 1st April 2019].

Kolderup, K (2017) Introducing Bluetooth Mesh Networking. Available from https://blog.bluetooth.com/introducing-bluetooth-mesh-networking [Accessed on 1st April 2019]

McClelland, D. (2017) 5 ways Bluetooth 5 will drive the Internet of Things. Available from: https://www.computerweekly.com/blog/Inspect-a-Gadget/5-ways-Bluetooth-5-will-drive-the-Internet-of-Things [Accessed on: 2nd April 2019].

Parekh, J. (2017) WiFi's evolving role in IoT. Available from: https://www.networkworld.com/article/3196191/wifi-s-evolving-role-in-iot.html [Accessed 2nd April 2019].

Rouse, M (2018) IoT Devices (internet of things evidence) Available from https://internetofthingsagenda.techtarget.com/definition/IoT-device [Accessed on 30th March 2019]

Techopedia (2019) Piconet. Available from https://www.techopedia.com/definition/5081/piconet [Accessed on 30th March 2019]

Techopedia (2019) Piconet. Available from https://www.techopedia.com/definition/5087/scatternet [Accessed on 30th March 2019]

Townsend, K. (2019) Introduction to Bluetooth Low Energy – GAP. Available from https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gap [Accessed on 30th March 2019]

Townsend, K. (2019) Introduction to Bluetooth Low Energy – GATT. Available from https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt [Accessed on 30th March 2019]