A Survey on Bluetooth 5.0 for Internet of Things

Jathin Sreenivas
Faculty of Computer Science and Engineering
Frankfurt University of Applied Sciences
Frankfurt, Germany
Jathin.Sreenivas@stud.fra-uas.de

***Abstract*—The most common challenge faced in IoT large-scale deployments is to enable a wide range of use cases in applications. There are a numerous number of communication technologies such as 4G, WiFi, WPAN, and the latest technology 5G. But now the Bluetooth Special Interest Group (SIG) has released Bluetooth 5.0 and claims to be for IoT specifically, by enhancing all the features of Bluetooth 4.2. Further, three relevant queries such as what is better about Bluetooth 5.0, why does it matter, and how it affects the IoT industry and its applications. With this context, a survey can be made on why Bluetooth 5.0 would be ideal for IoT applications, how Bluetooth 5.0 - IoT interact with each other, is Bluetooth 5 a valid technology candidate for implementation of Internet of Things applications, provided the security threats of Bluetooth.**

I. Introduction

Bluetooth is a technology that was developed more than 20 years ago. The first version of Bluetooth came up in 1994 when it was just used as a form of data transmission, in the current era this technology is one of the pillars of the Internet of Things (IoT). In the past years, the Internet of Things (IoT) has seen major improvements in the number of deployments, sensors, automation, and smart devices. IoT are being researched extensively for a wide range of application areas, such as private and commercial, industrial and logistic, or public sectors. In such areas, communication technology is considered accurately as there are varying requirements. For IoT use cases, they require a higher communication range, more speed, and large messaging capacity. Bluetooth 5.0 promises all these features and are has been introduced for IoT purpose, due to which the number of IoT application has significantly increased and reached to smart factories, smart home, and buildings as shown in Figure 1. The term Internet of Things (IoT) was first used by Kevin Ashton in 1999 in the context of supply chain management. In the current days, IoT areas include covering a wide range of applications like healthcare, transport, and other utilities, etc. IoT vision where anything in the physical world can be digitally represented and connected together for communication. The interaction with sensors, actuators, wireless connectivity, people, and smart objects is creating a significant improvement in IoT for intelligent devices.

II. Bluetooth Evolution

In the evolution of Bluetooth as illustrated in Figure 2, the first generation of Bluetooth started with providing the Basic Rate(BR) for basic functionalities. The next generations that came along added new features or improved the existing performance. In Bluetooth 2.x and 3.x, Enhanced Data Rate (EDR) and High Speed (HS) was introduced to further improve the performance. In generation 4.x Bluetooth Low Energy(BLE) was introduced for applications of Bluetooth which required low power. And the Bluetooth 5.x has improved the performance of Bluetooth 4.x significantly. Bluetooth 5.0 achieves

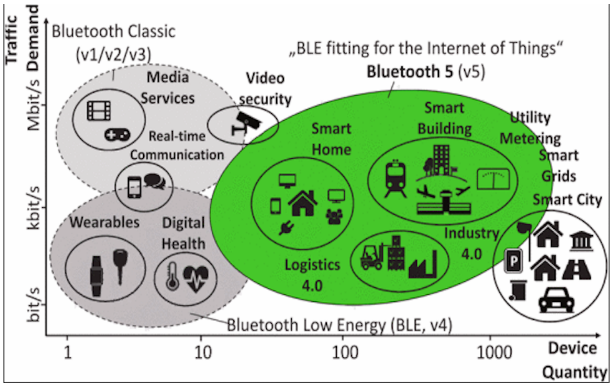

Fig. 1. Expansion of Bluetooth for the Internet of Things [6]

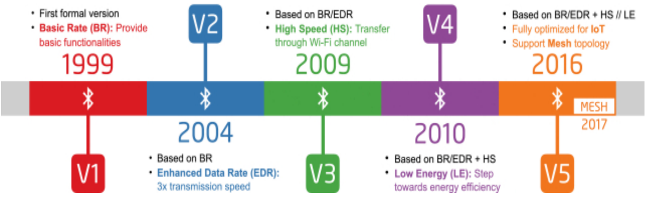
First formal version
Basic Rate (BR): Provide basic functionalities
1999
V1
V2
2004
Based on BR
Enhanced Data Rate (EDR): 3x transmission speed
Based on BR/EDR
High Speed (HS): Transfer through Wi-Fi channel
2009
V3
V4
2010
Based on BR/EDR + HS
Low Energy (LE): Step towards energy efficiency
Based on BR/EDR + HS // LE
Fully optimized for IoT
Support Mesh topology
2016
MESH
2017
V5

Fig. 2. Bluetooth Evolution [9]

A. Improvements of Bluetooth 5.0 over Bluetooth 4.2

1) Larger Advertising - Bluetooth 5.0 has a major increase in its messaging capacity, the capacity that can be transferred is 8 times the capacity of what Bluetooth 4.2 achieves.
2) Increased Range - The transmission range of Bluetooth 5.0 is increased by 4 times the range of Bluetooth 4.2. With this increasing range, IoT devices can be extended far away beyond the walls of a typical home.
3) Improved Speed - Bluetooth 5.0 achieves two times the transmission speed of Bluetooth 4.2.

4) Stronger Robustness - Bluetooth 5.0 establishes much more stable connections.
5) Mesh Topology - With the mesh topology in Bluetooth 5.0, now Bluetooth can be deployed massively in many variety topologies.

All of the above points certainly prove that Bluetooth 5.0 is enhanced significantly. These enhancements make it possible for Bluetooth to now transfer information much faster, further by establishing a much more stable connection with a lot more content. For all these reasons Bluetooth 5.0 is an important technology for the IoT area. The Bluetooth mesh is not restricted to just Bluetooth 5.0, Bluetooth 4.0 and above are supported as well. The network structure has been improved using the mesh structure, making it possible for a group of devices to connect rather than just an end-to-end connection. Bluetooth 5.0 will transform the IoT experience by making it simple, seamless, precise, and accurate.

III. Bluetooth5-IoT Architecture

The architecture of Bluetooth 5 IoT can be divided into six layers.

1) The hardware Layer - This is the bottom layer comprising the hardware components of IoT, such as sensors or sensors in smartphones which includes weather sensors, environment sensors, home appliances, and other physical components. The hardware layer covers up abstraction to leverage information about its periphery to the above layer the microcontroller layer.
2) Microcontroller Layer - This layer comprises of the microcontrollers that are required for automatically controlled devices such as office machines, home appliances, and other embedded systems. Few instances of what layer comprises of are The Raspberry Pi, AT Mega, Edison, etc.
3) Bluetooth Connectivity Layer -This layer contains the wireless standard for exchange, Bluetooth which uses a variety of protocols. The Bluetooth stack is divided into two segments. Firstly, the Controller - the controller is implemented in low-cost silicon devices which contains a time-critical radio interface that is the Bluetooth radio and a microprocessor. The second segment is the Host which deals with high-level data, the host is implemented as a package on top of an operating system or a part of an operating system itself. For EDR devices such as Bluetooth earphones, both the host and the controller are present on the same microprocessor which reduces the production costs. These devices are known as hostless systems. However, the host stack also comprises the protocol for communication between the host and the controller. Host Controller Interface (HCI) is a pseudo protocol for standardized communication between the two stacks. Link Manager Protocol (LMP) is used to control the connections between the devices, which include creation, modification, and releasing logical transports or logical links. As well as, to query any device capabilities and power control. The final protocol that is the Link Control Protocol (LC) communicates the flow control, acknowledgment, and retransmission requests. This protocol is embedded in the header of the Link Manager protocol.
4) Connectivity Layer - There are two pathways that can be taken in this layer, Internet Connectivity or Smart Phone OS. Internet Connectivity is the central part of the whole stack. IoT specific communication protocols are added here for energy efficiency, resource constraints, and lightweight information processing. MQTT, CoAP, IPv6, UDP, AMQP, LLAP, XMPP, and DDS protocols perform the following tasks: publish/subscribe messaging, multicast support, real-time messaging, packet-switched networking, message queue for middleware, lightweight local automation, and direct addressing publish/subscribe based communication for real-time embedded systems. The other pathway is the Smart Phone OS: The Wireless Personal Area Network (WPAN) technology which is designed for application in health care, fitness, security, and home automation. Current Mobile devices are always released with hardware and software support for Bluetooth. There are already Bluetooth Profiles present in mobile devices, such as the Blood Pressure Profile (BLP), and many other Fitness profiles.
5) Infrastructure Layer - The infrastructure layer is the most valuable layer of all. This layer comprises of four different compositions of 1. IoT business cloud services 2. Big Data Services, and 3. Bluetooth Host API/protocol. The IoT Business Cloud - an abstraction for business-specific services. Various business transactions and activities are served here by SaaS, PaaS, and IaaS cloud solutions. This modular architecture, as well as packet business APIs, eases the performance of any business-related operations. Parallelly also performs resource definition, abstraction, orchestration, and optimization of its external ecosystem. These business clouds reduce the organization's overhead of operational activities by providing a common layered approach with necessary supports provided. The Bluetooth Host API/Protocol - The host and controller stacks is divided into various subcategories. The General Access Profile (GAP) defines the topology being used by the Bluetooth network stack. The one-to-one, one-to-many, or many-to-many mechanisms which are means to connect to the other devices fall under the mechanism of GAP. During a one-to-one connection, there should be an explicit connection and here handshake is required to transfer data. The Generic Attribute Profile (GATT) describes the detailed description of the transfer attributes once the devices are connected. The Object Exchange (OBEX) is a communication protocol that facilitates the exchange of binary objects between devices. For example, file transfers require simple data exchange. The OBEX is bound to Radio Frequency Communication (RFCOMM), which is a set of transport protocol which is commonly used for its widespread support and publicly available API on most operating

systems. The Low energy attribute protocol is adapted for BLE since this protocol allows the client to read and write certain attributes with a lot more ease. The Big Data Services, these services make it possible for Big Data and IoT to work in conjunction. These services can be used for providing optimizations, statistical analysis, predictions, etc. By using these services, the network disks and computer power are impacted. The stack for big data processing must be done in consideration of the influx of data that IoT will deliver.

6) Application Layer - This layer is designed to disseminate the user experience via the software in applications that are performed over Bluetooth Connectivity. Bluetooth 5.0 with IoT can help solving numerous problems in fields such as health care, agriculture, sensors in smart phones, watches, home automation and many more.

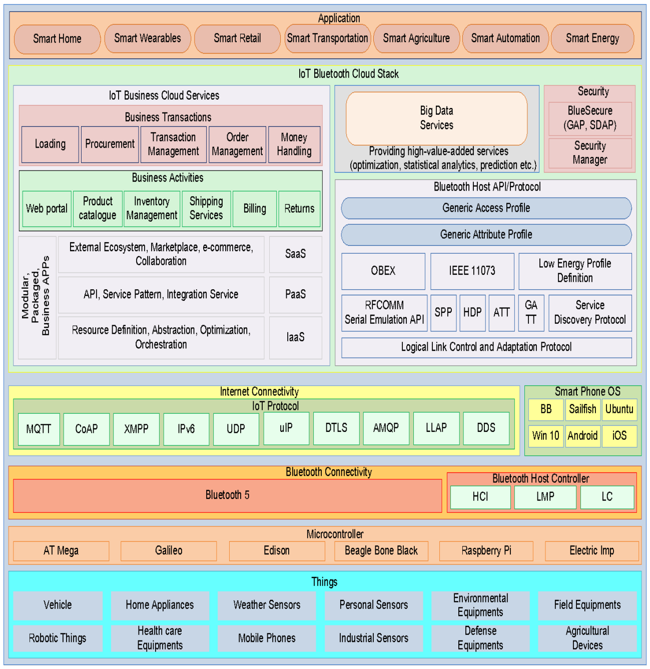

Fig. 3. Bluetooth-IoT (BTIoT-5) Architecture [5]

IV. Application Scenarios

Due to all the enhancements to Bluetooth, Bluetooth has a significant influence in the IoT area. Normally Bluetooth is used between two devices and broadcasting, which are the one-to-one and one-to-many applications. With the support of Mesh topology, now the application can use Bluetooth in form of many-to-many topology. The effects on the existing applications by Bluetooth 5.0 are

A. One-to-One: Paired Devices

This is the most known form of Bluetooth communication, which is being experienced from the first version of Bluetooth. This form of topology can be seen in all smartphones, wearable devices such as wireless earphones, smartwatches, etc. The typical Bluetooth mode used in these applications is the BLE or EDR. For applications using BLE such as IoT devices, smartwatches, Bluetooth 5.0 can be enjoyed as the data rate is doubled and range-extended, and the time required is cut down by half. Therefore needing a very less active time for the same amount of work, which leads to increased battery life. For the EDR applications such as wireless headphones where data that needs to be transferred is a lot more, the Bluetooth 5.0 can now transfer the same data for even more further range with clearer data. Therefore applications that use one-to-one communication now can send data in a faster way for a longer range while keeping the performance quality uninfluenced and also getting a much more stable connection.

B. One-to-Many: Proximity Beacons

A classic example of a one-to-many topology using Bluetooth is the beacon-based proximity. These devices continuously broadcast their IDs and information to all its neighbors. Any devices that are based on the distance and the angle can collect these IDs and information. Beacons also can carry large advertising capacity which enables them to carry detailed information along with its IDs. Now using Bluetooth 5.0 the same process can be done more efficiently. And also an added advantage of the location feature in Bluetooth 5.0, beacon devices can provide various context-rich location based services.

C. Many-to-Many: Meshed Objects

The main feature of Bluetooth 5.0, which allows many-to-many devices communication. Smart homes/offices and industrial controls make a huge profit using the Mesh topology of Bluetooth. In Smart Homes/offices - Smart home appliances serve the users seamlessly and intelligently. These devices require a reliable strong connection among IoT devices within and across rooms. The data that is being transferred ranges from kilobytes to megabytes. And for certain appliances, they need to operate on low power. However, Bluetooth was not the first preference for these applications. Due to the reason the star topology of Bluetooth, Bluetooth cannot cover a conference room when there are more than seven applications. And creates a lot of complexity. Now with Bluetooth Mesh, Bluetooth has finally had an edge to used in these appliances as well. Bluetooth is now a competitive player. The ZigBee is considered ideal for home automation, but Bluetooth may take over for the reason being Bluetooth is available in all laptops, mobile phones, and easy for a user to control and manage the home offices on their smart devices using Bluetooth.

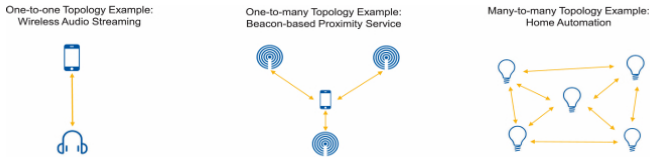
One-to-one Topology Example:
Wireless Audio Streaming
One-to-many Topology Example:
Beacon-based Proximity Service
Many-to-many Topology Example:
Home Automation

Fig. 4. Three examples of three kinds of topologies of Bluetooth [9]

V. Security and Reliability Threats in Bluetooth

Bluetooth devices are exposed to malicious intervention during the pairing process with another Bluetooth device, this is due to the flaw in the link key establishment protocol, which is required for pairing the device. Encryption in the process of pairing is optional and created at the end of the pairing process, meaning that attacks can be performed well before pairing is complete. Bluetooth transmissions can be deliberately jammed, denied, intercepted, and manipulated. False information can be passed to the devices by malicious users. Security and Reliability threats in Bluetooth can be classified into three categories:

- Disclosure threat: There can be an eavesdropper in between the source and the target, and the eavesdropper is not authorized for the information which is being transferred.
- Integrity threat: The information that is being transferred can be deliberately manipulated.
- Denial of Service (DoS) threat: The users can be blocked from gaining access to a service by making it either unavailable or severely limiting its availability to an authorized user.

These weaknesses are the flaws in the link key establishment protocol which is required for devices to pair as session encryption is not mandatory. Attacks can occur even before the pairing completes. A summary of the attacks that can occur on a Bluetooth network before and after the pairing process is summarized in Table I.

TABLE I
List of Bluetooth attacks. [4]

Type of issue	Description of the issue
Attacks Prior to Pairing	
PIN cracking	The attacker uses a brute force algorithm to identify the PIN. After cracking the pin, the attacker can pair with the target device and access information illegally.
BlueJacking	Attacker makes uses of the Bluetooth technology to send unauthorized messages to Bluetooth enabled device.
Man-In-The-Middle	Attacker acts as a legitimate user to establish Bluetooth connections to both victims' devices and to initiate the IO phase.
BlueSnarfing	Attacker hacks the node in order to access devices files, documents, etc.
MAC spoofing	Attackers could impersonate an alternative client and end connections or modify data during transmission
BlueBugging	The intruder gets illegal access to a device and can then implement unauthorized actions such as making phone calls etc.
BlueBorne	This attack allows an attacker to exploit some insecure implementations of Bluetooth.
Fuzzing	This intrusion involves sending malicious data to a device's Bluetooth radio and observes how the device reacts.
BluePrinting	A method to remotely extract information from Bluetooth enabled devices.
Attacks after Pairing	
Backdoor	This attack involves establishing a trust relationship through pairing but ensuring that it no longer appears on the target's device.
Denial of Service (DoS)	In this attack, the attacker prevents valid users from accessing the service by sending a large number of messages to the Bluetooth device.
Worm	The Cabir worm is a malicious software that uses Bluetooth technology to search for available Bluetooth devices and send itself to them.
Bluesmack	This attack is the Bluetooth equivalent of the Ping-of-Death DoS attack
MultiBlue	A MultiBlue dongle, a Bluetooth capable 4 GB drive, is utilized to take control of the target device.
BD_ADDR	The attack occurs when a bug is kept within coverage area of a Bluetooth device. The bug duplicates the BD_ADDR of the target device.
Reflection/Relay	An intruder need not be aware of any confidential data as only relays sensitive data from one node to the other in the authentication phase.

VI. Conclusion

Bluetooth has been in the industry for over two decades and in this time there is a significant improvement and the Bluetooth market has continued to expand at an exponential rate. The evolution of Bluetooth, wherein each version has bought many improvements and new features. The Bluetooth 5.0 aims at addressing the requirements of the IoT industry. The Bluetooth IoT architecture makes a strong impact on how IoT end users can be benefited from using Bluetooth. Bluetooth has officially come into the battle with its other competitors of communication technology of the IoT industry. It can be concluded that Bluetooth has made a strong competitor for the communication technology for the IoT applications and provides complete solutions for meeting the communication demands of the IoT industry.

References

[1] P. McDermott-Wells, "What is Bluetooth?," in IEEE Potentials, vol. 23, no. 5, pp. 33-35, Dec. 2004-Jan. 2005, doi: 10.1109/MP.2005.1368913.

[2] M. Collotta, G. Pau, T. Talty and O. K. Tonguz, "Bluetooth 5: A Concrete Step Forward toward the IoT," in IEEE Communications Magazine, vol. 56, no. 7, pp. 125-131, July 2018, doi: 10.1109/MCOM.2018.1700053.

[3] M. B. Yaakop, I. A. Abd Malik, Z. bin Suboh, A. F. Ramli and M. A. Abu, "Bluetooth 5.0 throughput comparison for internet of thing usability a survey," 2017 International Conference on Engineering Technology and Technopreneurship (ICE2T), Kuala Lumpur, 2017, pp. 1-6, doi: 10.1109/ICE2T.2017.8215995.

[4] S. Zeadally, F. Siddiqui, and Z. Baig, "25 Years of Bluetooth Technology," Future Internet, vol. 11, no. 9, p. 194, Sep. 2019.

[5] P. P. Ray and S. Agarwal, "Bluetooth 5 and Internet of Things: Potential and architecture," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 1461-1465, doi: 10.1109/SCOPES.2016.7955682.

[6] S. Böcker, C. Arendt and C. Wietfeld, "On the suitability of Bluetooth 5 for the Internet of Things: Performance and scalability analysis," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-7, doi: 10.1109/PIMRC.2017.8292720.

[7] https://medium.com/jaycon-systems/bluetooth-technology-what-has-changed-over-the-years-385da7ec7154 Accessed On: 06/12/2020

[8] S. Raza, P. Misra, Z. He and T. Voigt, "Bluetooth smart: An enabling technology for the Internet of Things," 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, 2015, pp. 155-162, doi: 10.1109/WiMOB.2015.7347955.

[9] Junjie Yin, Zheng Yang, Hao Cao, Tongtong Liu, Zimu Zhou, and Chenshu Wu. 2019. A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT. ACM Trans. Sen. Netw. 15, 3, Article 28 (August 2019), 29 pages. DOI:https://doi.org/10.1145/3317687