International Journal of Advance Research and Innovation
Vol. 9(3), Jul-Sept 2021, pp. 64-69
Doi: 10.51976/ijari.932110
www.gla.ac.in/journals/ijari

Article Info

Received: 04 Jul 2021 | Revised Submission: 28 Aug 2021 | Accepted: 05 Sept 2021 | Available Online: 15 Sept 2021

Bluetooth Low Energy: A Comprehensive Wireless Technology

*Uttpal Raj**

ABSTRACT

BLE, Bluetooth low energy is low power wireless communication technology that is used to connect a number of devices like smartphones, smart watches, wireless speakers, fitness watches, etc. at the same instance of time. Apple was the first phone to introduce BLE into their smartphone iphone4s back in 2011 and after that most of the companies started to include BLE into their devices for a faster reliable and secure connection. The technology was made in 2010 named Bluetooth smart also Bluetooth version 4.0 and then BLE5 was introduced in 2016 and the device versions which could run BLE are windows 8 or above, android 4.0 & above, IOS 5.0 and later, Linux 3.4, and mac OS 10.10 and above.

Keywords: *Wireless; Bluetooth Low Energy; Connection; Communication; Technology.*

1.0 Introduction

Bluetooth is a type of non-wired(wireless) technology that helps in exchanging data for a short range of distances with the use of short wavelengths. The idea behind the development of Bluetooth is to create a setup the can successfully set up the connections with a various variety of other possible peripherals such as mobile phones, computer printer, fax machine, etc. Bluetooth initially came up as an alternative to RS-232 data cable that further helps in building PAN(Personal Area Network) up to 30 feet. The core system employs frequency hopping with a trans receiver to combat interference and fading techniques.

SIG(Special Interest Group) was established in 1998 initially, Bluetooth SIG includes Ericsson, IBM, Intel, Nokia, and Toshiba but later on, it reached nearly 4000 members by the end of the first year. Bluetooth came up in different versions in the past 21 years with different data speed power consumption capabilities and data transmission range. In 1999, Bluetooth 1.0 launched its first version to create new possible ways to enable devices like fax machines, printers, wireless speakers, and headphones. Earlier the speed of data transfer was much slower than the current version. Bluetooth 1.0 was capable of having 1 Mbps data transfer for about 10 meters. Gaussian Frequency Shift Keying(GFSK) in which the carrier shifts between frequencies to attain 1mbps speed. Both 2.0 and 2.1 offer a faster PSK modulation scheme P/4 DQPSK and 8DQPSK that offers 2 to 3 times faster data transmission and attain 2 to 3 Mbps speed. Bluetooth was adopted in 2004 and the second version offers a change in waveform phase to carry the information by opposing frequency modulation which results in easier pairing and enhanced data rate. Bluetooth 3.0 was adopted in 2008 which has 8 times faster than Bluetooth 2.0 with almost 24 Mbps speed up to 30 feet. 2.0 offers have EDR and high-speed options to attain instant information service.

Bluetooth Low Energy(BLE) is a low-power wireless communication technology defined by SIG(Special Interest Group). BLE devices work with interconnections of central that generate command and accept the response of the task while the peripheral receives the command and works on the task. On 30th June 2010, Bluetooth launched its fourth version 4.0 in the market that was linked with various mobile operating systems like ios, Linux, windows phone, and blackberry. Bluetooth sends and receives data with the size 27 to 31 byte at the speed of 1 Mbps up to 10-meter indoor range. BLE 4.0 supports GFSK modulation. In December 2016, Bluetooth launched its most advanced version with better power consumption capability, data rate, and range.

**Department of Electrical, Electronics and Communication Engineering, The NorthCap University, Gurugram, Haryana, India (E-mail: chauahanuttpal@gmail.com)*

Fig. 1: Versions of Bluetooth

BLUETOOTH STANDARD RELEASES & TIMELINE

BLUETOOTH STANDARD VERSION	RELEASE DATE	KEY FEATURES OF VERSION
1.0	July 1999	Draft version of the Bluetooth standard
1.0a	July 1999	First published version of the Bluetooth standard
1.0b	Dec 1999	Small updates to cure minor problems and issues
1.0b + CE	Nov 2000	Critical Errata added to issue 1.0b of the Bluetooth standard
1.1	February 2001	First useable release. It was used by the IEEE for their standard IEEE 802.15.1 - 2002.
1.2	Nov 2003	This release of the Bluetooth standard added new facilities including frequency hopping and eSCO for improved voice performance. Was released by the IEEE as IEEE 802.15.1 - 2005. This was the last version issued by IEEE.
2.0 + EDR	Nov 2004	This version of the Bluetooth standard added the enhanced data rate (EDR) to increase the throughput to 3.0 Mbps raw data rate.
2.1	July 2007	This version of the Bluetooth standard added secure simple pairing to improve security.
3.0 + HS	Apr 2009	Bluetooth 3 added IEEE 802.11 as a high speed channel to increase the data rate to 10+ Mbps
4.0	Dec 2009	The Bluetooth standard was updated to include Bluetooth Low Energy formerly known as Wibree
5	2017	Bluetooth 5 was released in 2017 and provided higher data rates, improved security, the ability to be used for IoT with low current consumption, etc.

Speed of data transmission is up to 2 Mbps, 4 times range i.e. 40 meters indoor environment with large message capacity up to 255 bytes and greater battery life. Now BLE device is capable to support IoT devices. Enhancing the technology Bluetooth took connectivity among the devices to a different level.

2.0 Communication and Security Architecture

BLE known as the Bluetooth low energy is a newly developed protocol which is being developed for its energy-efficient short-range communications, this technology has played a major role in the connectivity of devices because since the last the amount of smart devices that could connect has drastically increased and the connectivity has made been made possible with the BLE due to its low power consumption, faster connectivity and low implementation complexity. If we take look at the power consumption of the BLE technology it's as low as ~5MA, and this also comes with low latencies or minimal delay which means when this technology is made in use there is close to no delay in the exchange of data packets between the connected devices, also the with the updates in the technology of BLE it does not mean that it'll lose connectivity with the previous versions.

The new versions of BLE will just connect fine with the devices having older versions but the major difference is that the connectivity would not be that faster and secure and hence that has made its way to our indoors in the way of smart home devices like the smart home speakers.

The connection of these devices happens in such a way that these Bluetooth devices emit beacon packets, these beacon packets broadcast the data at regular intervals. This communication architecture plays a major role in conserving the energy hence provide higher data transfer rate. This Bluetooth low energy framework has 40 frequency channels 2MHz apart out of which 3 are the primary advertisement

and the rest 37 are the secondary channels. These beacons are the small radio transmitters that transmit BLE signals up to 80 meters and when a device comes in a range of any of the beacons a connection is being established between those devices with the exchange of the passkeys. With the advancement of BLE technology, it's having some security concerns to look upon like the connection speed of 2Mbps, a range that can reach up to 400 meters with connection bandwidth of 800% and this increase band can lead a hacker to access the device from a faraway location and with the speed of 2Mbps, the data can travel at such speed without the owner getting noticed.

A man-in-the-middle attack(MITM) is a kind of cyber attack also known as a wrapping attack in which the attacker can hack the devices having BLE5 and can see the conversation in between the devices here the conversation refers to the data that is being exchanged between the devices and the attacker could do anything with that data as he/she can access that data without getting noticed. The MITM happens when the key that is being exchanged between the devices is identified by the attacker usually the key is 0 but in certain cases, the software is used which tries different keys at a time at a very fast pace which makes the user open a gateway into the crucial data of the users.

Though encryption was made a mandatory step after BL 2.1 that does not imply the pairing of the devices in which BLE falls let's say for eg. We are connected to our system with a wireless keyboard as the wireless keyboard does not have a screen we can't see that is only connected to our system not other. The process of pairing includes the finding of temporary keys with a Bluetooth device and exchanging them in between.The client-side initiates an exchange of safety features where it asks the server, This exchange of features will determine what pairing method to use. Once the key sharing is complete, These keys aren't stored for future use. During this connection, long-term keys can be used later. With Bluetooth 4.2, a definite pairing process exists called LE Secure Connections that alleviate a variety of vulnerabilities associated with passkey pairing and Out of band authentication, there is another method called Numeric Comparison. Numeric Comparison state that a display is there on both the devices and an example of this is the pairing between a cellular device and laptop. In Numeric Comparison a six-digit no. is displayed on both devices and thus if users are having a similar number then this shows that the connection is secure and correct.

3.0 Mesh Networking in BLE Devices(A Step Towards IoT), Applications

Bluetooth low energy has several applications in the modern period or field of communication. It made life easier and flexible communication between the transmitter and the client. There are the following applications:-

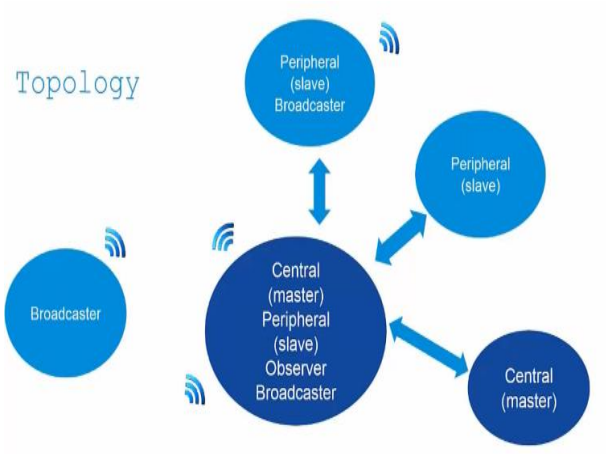
- Wireless charging: Latest smartphones come with a non-wired charging option which is faster than the earlier method. And multiple devices can connect to a Bluetooth charger up to 5 centimeters.
- Agriculture: Gyujo system which is developed by Fujistu is an effective example of an advanced BLE application to figure out of best time to inseminate the cow and helps to improve livelihood. Also, BLE can help in making a smart irrigation system. Irigation is a process of production smart irrigation system consits of water/moisture sensors that catches proportions of moisutre in the soil and supply required amount of water which helps in germonation of seed.
- Automobile: Automobile has updated their vehicle with various Bluetooth adaptive sensors that help in better parking experience, changing of punctured tires, and wireless connection between devices.
- Automation: Bluetooth Low Energy helps to set up automation system in a different level. Nowadays, it is not only linked with home but also with industry as well which helps in production.
- Medical: There are variuos medical devices develpded that transfers the data of patients to the respective hospitas even when the patients are some where outside.

3.1 BLE streetlight controller and sensor networking

Low power wide area network(LPWAN) is a new concept to generate smart city formation. The main ideology is to design and implement a system that is used to control a smart street light and also

gather the data from the installed sensors using the desired BLE devices and give the application by both as software application as well as hardware device that should consume low power(take power from free energy source i.e. solar panel). The communication part aims to utilize 2.4 GHz unlicensed ISM band for LED light fitting and sensor networks and it will make it cost and energy efficient by fulfilling all the requirement of connectivity. This highly relies on BLE and sensor technology that need a small amount of data for a longer range especially in mesh networking and maintaining long battery life.

Fig. 2: Bluetooth Topology



Bluetooth low energy topology consists of various terminology and roles. There is a broadcaster that acts as a transmitter which helps in transmitting the data to the observer that helps in receiving the data. Peripherals of Nordic chip or development board are compatible with Bluetooth devices which further helps in salve roles. Central is the master that supports multiple connection roles and initiates a connection with other peripheral. Further peripheral is divided into further parts like master-slave with their functionality. To help data transfer there is a server and the client. The server is the formation of peripherals that contain the data and further with the client and a client device is a central device that needs the data to access for evaluation. Peripherals contain memory, radio, controller which are connected to the power supply.

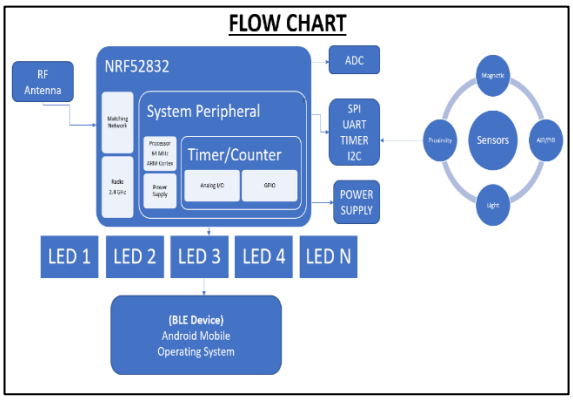
The scope of designing and implementing a system that will be used to control Street Lights as well as gather the data from different Sensors using the BLE devices as a hardware device and an application as software. The system should be low power (can be powered by a coin cell or small solar panel or any free energy source). This project aims to utilize the Bluetooth devices operated in the unlicensed 2.4GHz ISM band for the sensor networks and in the LED light fittings, to make a cost-effective system fulfilling the connectivity and performance requirements of the project.

This flow chart consists of the description of the hardware block by block. There are sets of multiple sensors that contain magnetic, proximity, AIR/ PIR, and the purpose of sensors is to collect data from the environment, digital sensors set straightforward and easy interface with a microcontroller using SPI (Serial Peripheral Interface) bus. Although for analog sensors, either analog-to-digital converter (ADC) or Sigma-Delta modulator is used to convert the data into SPI output. They send analog input to digital output into the next block.

The next block consists of nrf52832(Nordic chip) that works as a development board. Nordic's nRF52832 SoC(System on Chip) provides the Bluetooth Low Energy connectivity from the device to a user's Bluetooth 5.0 smartphone for setup, configuration of a network, and sensor adjustments including time delay, ambient light, and other sensitivity, and motion detection range and sensitivity of the information. The power supply converts 220v ac to 5/3.3v dc. The Nordic chip consists of various peripherals like SPI, UART, I2C that perform different specifications.

There is an RF antenna that has a matching network for data transmission at a particular frequency. It includes an NFC antenna designed for ASICs, ASSPs, FPGAs, microcontrollers, and SoCs which work on 64 MHz processors. Cortex-M cores are commonly that quickly enables the utilization of the NFC-A tag peripheral on the nRF52832. The whole setup sends an output to a smart LED street lights system that can control automatically. It facilitates development by exploiting all features of the nRF52832 SoCs. The ARM Cortex-M family are ARM microprocessor cores that are used as microcontroller chips, but also are set inside of SoC chips as system controllers, power management controllers, Input/output controllers, screen controllers, battery controllers, and sensors controllers.

Fig. 3: BLE Streetlight Flow Chart



For transferring a small amount of data the above set up connected to a BLE device such as an android phone or PC devices that can be used manually.

The strength of the signal can also be increase by following some methods but these methods comes with some drawbacks as well that make the whole system.

- Mesh/ Star topologies: In mesh toplogy there are certain nodes that are acllocated at certain distance which are connected directly, non-hierarchically or dynamically to many other nodes and create mesh like structure and finally it transmits the more data to larger area but due to complications of network sometime security lags and it is also expensive to build.
- Repeater: By using repater it extend the connection distance as it catches the similar data and transfer it accordinlgly it also enhance the signal strength. By using repeater the bandwith decreases. It basically used in broadcasting.
- Amplify the signal: Amplification basically increases the target proportion. It strengthen the recieving signal. But it consume more power and Bluetooth Low Energy (BLE) is based on low power consumtion topology.

4.0 Limitations

Bluetooth have overcome variuos limitations that was faced previuosly. It covers variuos milestones in terms of data transfer and speed. Also, it matches data securities requirements. Bluetooth is a low cost technology available in most of the smartphones and variuos smart devices. Still BLE fails in some aspects mentioned.

4.1 Data limitations

Data throughput of BLE is limited by a layer known as Physical Radio Layer (PHY) rate of data, which is the rate at the radio, transmits the data. This data rate totally depends upon the Bluetooth version used. Considering Bluetooth model 4.2 and earlier, the rate was fixed at 1 Mbps. For Bluetooth version 5 and later on, the rate varies depending on the mode and PHY model. The rate can reach to 1 Mbps like previous versions, and also 2 Mbps when utilizing the high-speed feature.

4.2 Area coverage

Bluetooth or BLE was designed for shorter area coverage applications and that is the reason its range of operation is limited. There are a few factors that limit the range of BLE:

- Bluetooth Low Energy operates in the 2.4 GHz ISM band spectrum which is vastly affected by obstacles that exist all around us such as metal bodies, and various other obstacle (especially human bodies) as it does not support mesh networking.
- Performance and designing of the antenna of the device.
- Physical compatibility of the device, it must match with all the basic requirements such as data transfer and data speed.

4.3 Internet connectivity

Internet connectivity is a major aspect to have Bluetooth transfer. Just like VoIP, BLE need a stable internet connectivity to transfer the data from one place to another. Without internet connection Bluetooth does not work.

5.0 Conclusions

Bluetooth is a kind of wireless technology used to connect devices wirelessly and with the BLE 5, the current boundaries of Bluetooth have pushed its limits to a greater extent. In this research paper, we've covered what's BLE5, how were its previous versions, what modification's been made so far to achieve the BLE5, its versions release timelines, updates, communication architecture, some of its security guidelines, how beacons structure is implemented to achieve the successful interactions with other devices.BLE5 comes with some best-in-class applications like the increased bandwidth,

multiple connections from 1 device have been made possible and many more such applications have been made feasible. At last, the future scope, Low power wide area network(LPWAN) could be a new concept to get smart city formation. This highly relies on BLE and sensor technology that requires a little amount of information for an extended range especially in mesh networking and maintaining long battery life. Bluetooth low energy topology consists of assorted terminology and roles.

References

[1] C Gomez, J Paradells. Wireless home automation networks: A survey of architectures and Technologies. IEEE Commun. Mag. 48, 2010, 92–101.

[2] A Ludovici, A Calveras, J Casademont. Forwarding techniques for IP fragmented packets in a real 6LoWPAN network. Sensors, 11, 2011, 992–1008.

[3] JW Hui, DE Culler. Extending IP to low-power, wireless personal area networks. IEEE Internet Comput. 12, 2008, 37–45.

[4] J Nieminen, B Patil, T Savolainen, M Isomaki, ZShelby, C Gomez. Transmission of IPv6 packets over Bluetooth low energy, draft-ietf-6lowpan-btle-8, 2012.

[5] J Zheng, MJ Lee, M Anshel. Towards secure low rate wireless personal area networks. IEEE Trans. Mob. Comput. 5, 2006, 1361–1373.

[6] JJ Echevarría, J Ruiz-de-Garibay, J Legarda, M Álvarez, A Ayerbe, JI Vázaquez. WebTag: Web browsing into sensor tags over NFC. Sensors , 12, 2012, 8675–8690.

[7] F Callegati, W Cerroni, M Ramili. Man-in-the-Middle attack to the HTTPS protocol. IEEE Secur. Priv. 7, 2009, 78–81.

[8] S Kamath. Measuring Bluetooth Low Energy Power Consumption, Application Note AN092; Texas Instruments: Dallas, TX, USA, 2010.

[9] J Ko, A Terzis, S Dawson-Haggerty, DE, Culler, JW Hui, P Levis. Connecting low-power and lossy networks to the internet. IEEE Commun. Mag. 49, 2011, 96–101.

[10] C Gomez, I Demirkol, J Paradells. Modeling the maximum throughput of Bluetooth low energy in an error-prone link. IEEE Commun. Lett. 15, 2011, 1187–1189.