Internet Of Things Technology: Low Energy Communication

Brian Kelein Ngwoh Visas
Electronics Engineering
Hamm-Lippstadt University of Applied Sciences
Lippstadt, Germany
brian-kelein-ngwoh.visas@stud.hshl.de

***Abstract*—Internet of things describes physical objects that are embedded with sensors, processing ability, software, and other technologies, and that connect and exchange data with other devices and systems over the Internet or other communications networks.In this paper we would be looking at IoT devices using Low energy to aid in their communication with each other.In recent years Internet of Things has developed rapidly and has a wide range of applications. A study is carried out on the differences between devices using Low energy and those that do not use Low Energy, and an example of how Low Energy used in our every day processes.**

***Index Terms*—Internet of Things, Low Energy, Bluetooth Low Energy**

I. Introduction

Internet of Things (IoT) was established by a member of the RFID development community in 1999, and it has just lately become more significant in the real world, thanks to the emergence of smartphones, embedded and widespread connectivity, cloud computing, and data analytics.Consider a society in which billions of items can detect, communicate, and exchange data over public or private Internet Protocol (IP) networks. Data is gathered, evaluated, and regularly used to start acting on these networked items, offering a wealth of insight for planning, management, and decision-making. This is the Internet of Things (IoT) world (IoT).According to the most prevalent definition, the Internet of Things (IoT) is a network of physical items. The internet has been transformed from a network of computers to devices of all types and sizes. This includes cars, smartphones, home appliances, toys, cameras, medical instruments, industrial systems, animals, people, buildings.

All connected, all communicating and sharing information based on predetermined protocols, to achieve intelligent re-organizations, positioning, tracing, safety, control, and other goals. Internet of Things is an idea and a paradigm that examines the ubiquitous presence of a range of things/objects in the environment that may communicate and collaborate with one another. These objects collaborate to create new applications/services and achieve common goals using wireless and wired connections and unique addressing schemes. However, the research and development hurdles to creating an intelligent world are immense in this setting. A universe in which the physical, electronic, and simulated worlds mix to create creative surroundings that enhance energy, transportation, cities, and various other industries.

Fig. 1. Internet Of Things 1 [1]

A. What is Internet of Things(IoT) Technology?

IoT refers to a broad concept of things, particularly daily items, that are readable, identifiable, locatable, accessible through information sensing devices, and/or controllable over the Internet, regardless of communication means (whether via RFID, wireless LAN, wide area networks, or other means). Everyday objects comprise not just the electronic gadgets we meet or products of more significant technical advancement such as automobiles and equipment, but also items we don't often consider to be electronic at all, such as food, clothing, chairs, animals, trees, and water. The Internet of Things is a new Internet revolution. Objects gain intelligence and recognise themselves by creating or facilitating context-related decisions, owing to their ability to transmit information about themselves. For example, they might access data that has been gathered by other systems, or they can be components of more complicated services. This revolution is occurring in tandem with the advent of cloud computing capabilities and the Internet's move to IPv6, which has a nearly limitless routing capacity.

The main aim of IoT is to allow things to connect with anything, anybody at any time, anywhere, and utilize any

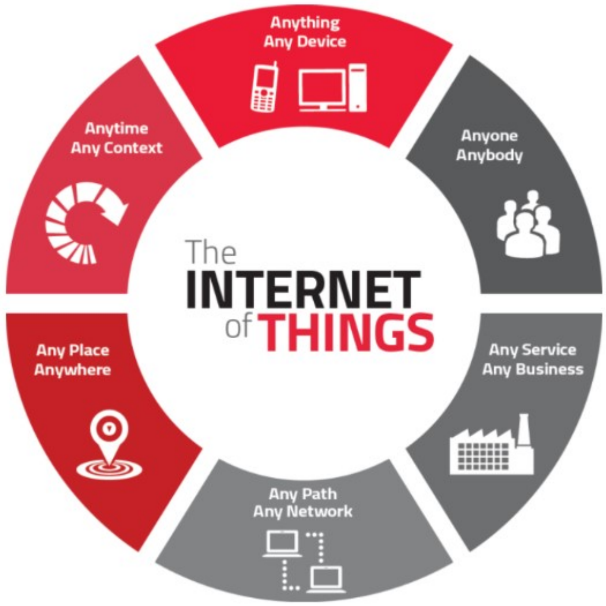

Fig. 2. Internet Of Things 1 [1]

path/network and service.

B. What is Low Energy?

Low-power wide-area (LPWA) networks enable low-power IoT devices to effectively and successfully communicate across long distances at low power costs. These networks are intended to transmit tiny payloads such as sensor data, alarms, and status updates. However, low power is necessary for many remote devices to save battery life, and with the variety of devices predicted to grow dramatically, the environmental effect must be addressed [2].

II. Communication Interfaces for IoT Systems

1) Bluetooth Low Energy: Bluetooth Low Energy (BLE) was recently designed to upgrade Bluetooth 4.0 and above. As the name implies, BLE is a Bluetooth power-saving communication technique developed for low-power devices such as sensor terminals. BLE has a maximum bandwidth of 1 megabit per second (Mbps) and an adequate bandwidth of 270 megabits per second (kbps). The most recent BLE Enhancement, Bluetooth 4.2, has a sufficient bandwidth of 650 kbps (kbps). On the other hand, Classic has a maximum and effective bandwidth of 3 (Mbps) and 2.1 (Mbps), respectively. As a result, BLE is inappropriate for sending vast amounts of data [3].

Because Bluetooth LE is a personal area network (PAN), its range is significantly reduced compared to ZigBee. The goal is to connect to devices that are close to the user. Although Bluetooth LE has a lesser capacity than ZigBee, it offers a significantly faster data rate. Bluetooth LE has a data rate of 1 Mbit/s for brief bursts, compared to 1 to 3 Mbit/s for traditional Bluetooth [4]. In addition, it ”sleeps” in-between such shots, which is a feature ZigBee lacks, using fewer data and power.Bluetooth was created under the IEEE 802.15.1 standard, used for wireless communication via radio transmissions. Bluetooth supports frequencies ranging from 2.4 GHz to 2.483 GHz. It has a shorter range than Zigbee. The GFSK modulation technology is utilized in Bluetooth [5].

2) zigBee: The network infrastructure necessary for wireless sensor network applications is provided by ZigBee and IEEE 802.15.4, which are standards-based protocols. The physical and MAC levels are defined by 802.15.4, whereas the network and application layers are defined by ZigBee. Long battery life, low cost, compact footprint, and mesh networking are primary design criteria for sensor network applications to facilitate communication between large devices in an interoperable and multi-application environment [6].ZigBee is a mesh network technology for transporting tiny quantities of data across short to medium distances. It uses a mesh topology network, which means that data from a single sensor node flows via a series of modes (or ”mesh”) until it reaches the gateway. In addition, because ZigBee is a local area network (LAN), it is not meant to connect to devices near the user, unlike Bluetooth LE. Instead, it links to devices that require a more fantastic range of communication. As a result, it’s an excellent choice for home automation and intelligent lighting [4].

3) WiFi: A WiFi network is basically a network device that allows several devices in a house or company to share an internet connection. The router connects to your internet modem instantly and functions as a hub, broadcasting the internet signal to all of your wireless connections. So as long as you’re inside your network’s service area, you’ll be able to stay in touch on the internet.It stands for nothing, ironically. Wifi, often known as wifi, or wifi, is not the same as Wireless Fidelity. The word was coined by a marketing company in response to the wireless industry’s need for a more user-friendly moniker for the IEEE 802.11 standard.

Wi-Fi transmits data from your wireless network to Wi-Fi-enabled devices such as your TV, smartphone, tablet, and computer via radio waves. Your equipment and confidential info are exposed to hackers, cyber-attacks, and other hazards since they interact over the airwaves. This is especially true while using a public Wi-Fi network at a coffee shop or an airport. Connecting to a password-protected wireless network or a personal hotspot is preferable whenever feasible [7].

A. Low energy interfaces

1) Bluetooth Low Energy: Bluetooth has many applications in the smart home, such as home automation, device tracking, remote control and many more. Home automation which is also a branch of IoT is one of the primary driving force behind the concept of BLE. Applications in this domain are usually deployed within a limited range of short distance to each other(less than 15m) but with more frequent interactions between sensors, actuators, and gateways. [9] BLE shines when it comes to local services and can make it much easier for people to interact with buildings and other infrastructure in their surroundings actively. Such BLE- services are more

Fig. 3. WI-FI Communication [8]

responsive, even without Internet connectivity such as assets and people tracking in a facility. BLE is also available In the domain of intelligent vehicles network, VANETs(Vehicular Ad Hoc Networks), which is considered a very effective and safe technology for modern transportation systems. BLE was first proposed as an alternate V2V(Vehicle-to-Vehicle) communication 2014 [9].

Bluetooth communication has become valuable since the Bluetooth Special Interest Group(SIG) developed Bluetooth Low Energy in Bluetooth v4.0. The Bluetooth Low Energy technology is designed for the low-powered operation in which it sacrificed its range from 100m to 50m as against the Bluetooth classic. One exciting thing about the BLE is that a master node can be connected to hundreds of slave nodes [10], unlike the Bluetooth Classic piconet where a master node can only be connected to seven slave nodes.

BLE has 40 channels that operate in the 2.4 GHz ISM band and uses three channels for advertising, which allows device discovery. With a successful device discovery and connection, the remaining channels serve as a data transmitter. Basically, in Bluetooth LE, hundreds of slave nodes can be connected to a master node [10].

BLE uses connection-less communication for BLE beaconing. Beacons act as advertisers and continuously broadcast a specific packet containing information for several purposes. The advertising process consumes very little energy. Theoretically, a coin cell battery-powered BLE beacon can last up to 14 years [9].

For the remaining chapters, we will talk about how the Bluetooth LE, its architecture is used in the smart home with the case scenario of Bluetooth location services focusing on Real-Time Location Systems(RTLS) for asset tracking and Indoor Positioning Systems.

2) Bluetooth Low Energy Architecture: The Architecture comprises three main parts; application, host and controller

The application layer is where the application interface and logic and the overall application is contained.

Access Profile (GAP): This layer defines the communication and access protocol between Bluetooth LE devices. BLE devices can connect by either acting as a broadcaster or an observer [11].

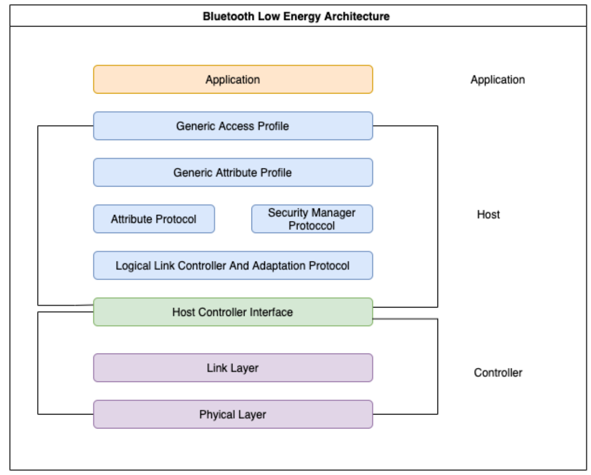

Fig. 4. Bluetooth Low Energy Architecture [11]

- Broadcaster: A BLE device advertises or broadcasts information packets in this protocol. It is also referred to as peripherals.
- Observer: In this protocol, the device continuously listens for the packets and decides based on the situation whether to start a connection or not. This is also referred to as central.

Attribute Protocol: This protocol defines rules for accessing data on a device. This protocol also explains the practices that any data on a server will have; a 16-bit attribute handle, set of permissions, value, and UUID.

Generic Attribute Profile (GATT): GATT defines how connected BLE devices communicate with each other. Like GAP, it has two roles, the client and server. The server's role is to store data or attributes and make them available whenever requested. The client requests data from the server, retrieves it and interprets and manipulates it.

The Host: defines the essential specifications that enable BLE devices to communicate and identify each other.

The controller facilitates the transmission of a signal. It has two parts, the Link Layer and the Physical Layer.

Link Layer: It is used for creating, scanning, advertising and maintaining links between the BLE devices. It has five states: standby, scanning, initiating, advertising and connection between master and slave. The Physical layer transmits and receives data, and the coating consists of analogue circuits.

3) Central Peripheral Architecture for Bluetooth Low Energy: Understanding Bluetooth Low Energy architecture in terms of Central and Peripheral roles is essential to understand how Bluetooth Low Energy devices advertise and connect to each other. A Central is a device that scans for Bluetooth devices, connects to them, and extracts their hosted information. Ideally, Central devices are richer in computing power than Peripheral devices.

On the other hand, Peripherals are devices that advertise their presence, and it is under this advertisement that the

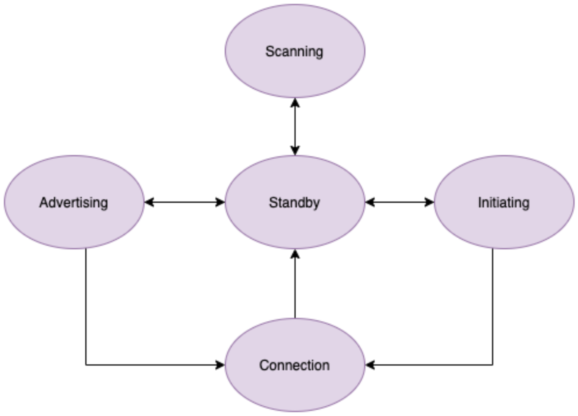

Fig. 5. Link Layer State [11]

Central knows that a Peripheral device is nearby. It can connect to enquire about its data.

If the Peripheral is responsible for advertisements, then the Central is responsible for the following:

- Initiating a connection
- Establishing a connection
- Retrieving information from the peripheral (Discover Services, Characteristics, Descriptors and finally read the data)
- Terminating a connection

Based on the above points, it can be concluded that the Central is always in control of the information exchange process and the actual connection. For a one-to-one relationship, depending on whether it is connected to a Central or not, a Bluetooth Low Energy Peripheral can be in either one of the following two states: * Advertising * Connected When the Peripheral is in an Advertising state, it broadcasts Bluetooth Low Energy advertising packets. Before delving into the details of advertising packets, it is essential to understand the general packet structure that BLE follows.

4) Bluetooth Low Energy Meshes and Beacons: BLE mesh networks allow reliable and flexible communication for IoT devices requiring low power for the Internet of Things (IoT). Most Bluetooth LE-based mesh protocols are implemented using piconets and scatter nets as overlays on standard Bluetooth topologies similar to the star topology [12]. Mesh networking transforms each Bluetooth Low Energy node into a hub, where the node/hub can also transfer data to nearby devices. This changes the network topology from a traditional star network to a Mesh as shown as follows:

This means that each node on the network can accept and send data to neighbouring nodes, allowing the network to scale more easily by simply adding new nodes. A mesh network exhibits the following characteristics:

Self-forming / organized: As soon as a new node joins the network, all its adjacent nodes are notified so that an optimized route for data packets is dynamically configured.

Self-healing: If a node on the network fails, the surrounding nodes notice it immediately, and an optimized route is dynamically configured for the remaining data packets. A single node cannot cause the entire network to fail. The network continues to operate without downtime as long as the density of devices is sufficient to maintain communication.

Self-optimization: the network can optimize itself to obtain the highest possible coverage.

The Beacon is another piece of pre-existing hardware technology that will benefit significantly from Bluetooth Low Energy 5. Beacons are small-sized Bluetooth low-energy devices that transmit information.

Bluetooth low energy beacons are mainly used for proximity broadcasting or advertising. The most popular use case for beacons is to transmit/publish contextual information to nearby smartphones and portable devices that support nearby Bluetooth Low Energy. Beacons are also used for internal movements: Because GPS does not operate indoors, Bluetooth Low Energy beacons can be placed at specific areas (home/office) to provide indoor navigation. Object tracking: Bluetooth low energy beacons/beacons can be attached to items that may be misplaced, such as keys, to serve as trackers. These variables may then be tracked using a smartphone app. Personal Supervision: Monitoring patients, the elderly and young children within the home.

B. Zigbee

The Internet of Things (IoT) has grown in popularity in recent years. As a result, IoT device security becomes more critical, especially since many devices have access to highly individualized and sensitive data. As a result, many large firms, including Samsung and Philips, have chosen Zigbee as one of the most frequently used protocols for wireless communication between different IoT devices. Zigbee is a low-power, low-cost wireless personal area network that connects devices primarily for personal usage. The goal of the standard is to offer a two-way, reliable communication protocol for applications with a limited range, usually between 10 and 100 meters. Zigbee is utilized in various applications, including home automation, intelligent energy, remote control, and health care, and is implemented using several application standards [13]. Even though Zigbee was created with security in mind, compromises were made to maintain the devices low-cost, low-energy, and highly interoperable. Unfortunately, some of the security safeguards in the standard are inadequately applied, resulting in security issues. The critical security issues and outcomes of attempted attacks on a few IoT devices using the Zigbee standard are highlighted in this study [13].

ZigBee devices use unlicensed frequency channels such as 2.4 GHz (globally), 868 MHz (Europe), and 915 MHz (North America) (America). The maximum data rate for each band is different. 250K bits per second may be obtained in the 2.4 GHz frequency range, 40K bits per second in the 915 MHz frequency band, and 20K bits per second in the 868 MHz frequency band. Its range can range from 10 to 100 meters depending on the frequency, power, and ambient factors [14].

Offset-quadrature phase-shift keying (O-QPSK), binary phase-shift keying (BPSK), and amplitude-shift keying are the three types of modulation used by ZigBee (ASK). There is one channel in the 868 MHz band and ten in the 915 MHz band (1 through ten), whereas there are 16 ZigBee channels (11 through 26) in the 2.4 GHz spectrum, each with a bandwidth of 2 MHz and a channel spacing of 5 MHz [14].

C. Zigbee Architecture

Application (APL) Layer: This top layer comprises an Application Framework, a ZigBee Device Object (ZDO), and an Application Support (APS) Sublayer.

Application Framework: Provides instructions for adding a profile to the ZigBee stack (to verify that profiles are created consistently). It also defines a set of standard data types for profiles and descriptors for service discovery, frame formats for transmitting data, and a significant value pair construct for quickly creating simple attribute-based profiles.

Application Objects: The ZigBee device is controlled by software on an endpoint. Up to 240 application objects can be supported by a single ZigBee node. Endpoints 1 to 240 are supported by every application object (with endpoint 0 designated for the ZigBee Device Object(ZDO)).

ZigBee Device Object (ZDO): Defines a device's position in the network (coordinator, router, or end device), sends and receives binding and discovery requests, and creates a secure connection between network devices. It also offers a comprehensive set of administration commands described in the ZigBee Device Profile (used in ZigBee commissioning). Endpoint zero is always the ZDO.

ZigBee Device Object Management Plane: Enables communication between the ZDO and the APS and NWK levels. The ZDO handles network connectivity and app security requests using ZDP (ZigBee Device Profile) messages.

Application Support(APS)Layer: The application and ZigBee device profiles rely on the data service provided by this component. It also includes a management service for keeping binding connections and the table itself up to date.

Security Service Provider(SSP): Provides encryption-based layers with security measures (NWK and APS). The ZDO was used to set up and configure the system.

Network Layer(NWK): Handles network address and routing by invoking actions in the MAC layer. Its tasks include starting the network (coordinator), assigning network addresses, adding and removing network devices, routing messages, applying security, and implementing route.

Medium Access Control Layer (MAC): Provides reliable communication between a node and its near neighbours, reducing collisions and increasing efficiency. The MAC layer is also in charge of putting together and breaking down data packets and frames.

Physical Layer(PHY): The interface to the actual transmission media is provided (e.g. radio). The PHY layer comprises two layers that operate at different frequencies. For example, the 868MHz European and 915MHz bands utilized in nations like the United States and Australia are covered by the lower frequency PHY layer. On the other hand, the relatively high PHY layer (2.4GHz) is almost universally employed.

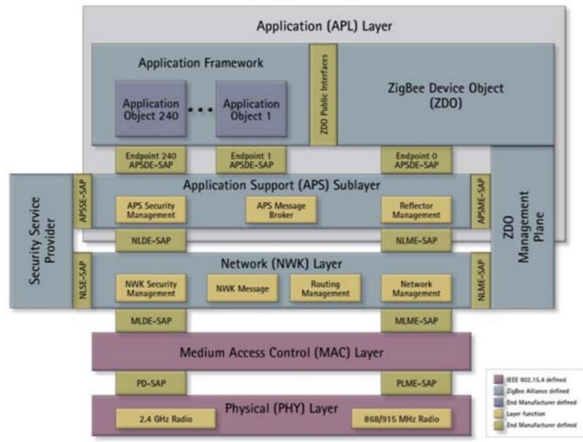

Fig. 6. Link Layer State [6]

1) Non-Low energy interfaces:

III. Internet of Things Application in Low Energy

IV. Conclusion

References

[1] K. Patel, S. Patel, P. Scholar, and C. Salazar, "Internet of things-iot: Definition, characteristics, architecture, enabling technologies, application future challenges," 05 2016.

[2] "Mqtt anywhere data and low-power iot efficiency — u-blox," https://www.u-blox.com/en/blogs/insights/low-power-iot-mqtt-anywhere, (Accessed on 12/21/2021).

[3] N. Kajikawa, Y. Minami, E. Kohno, and Y. Kakuda, "On availability and energy consumption of the fast connection establishment method by using bluetooth classic and bluetooth low energy," in *2016 Fourth International Symposium on Computing and Networking (CANDAR)*, 2016, pp. 286–290.

[4] B. Ray, "A Bluetooth & ZigBee Comparison For IoT Applications | Blog | Link Labs." [Online]. Available: https://www.link-labs.com/blog/bluetooth-zigbee-comparison

[5] "Difference between Bluetooth and Zigbee," Jun. 2019, section: Computer Networks. [Online]. Available: https://www.geeksforgeeks.org/difference-between-bluetooth-and-zigbee/

[6] "Getting started with zigbee and ieee 802.15.4," (Accessed on 12/22/2021).

[7] "What is Wi-Fi? | Definition, Meaning & Explanation | Verizon Fios." [Online]. Available: https://www.verizon.com/info/definitions/wifi/

[8] "What is wi-fi? - definition and types - cisco," https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html, (Accessed on 12/28/2021).

[9] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, "Beyond beaconing: Emerging applications and challenges of ble," *Ad hoc networks*, vol. 97, p. 102015, 2020.

[10] M. Collotta and G. Pau, "A solution based on bluetooth low energy for smart home energy management," *Energies*, vol. 8, no. 10, pp. 11 916–11 938, 2015.

[11] M. Bhargava and J. Wilson, *IoT projects with Bluetooth low energy: harness the power of connected things*. Birmingham Mumbai: Packt, 2017, oCLC: 1043899880.

[12] M. R. Ghori, T.-C. Wan, and G. C. Sodhy, "Bluetooth low energy mesh networks: Survey of communication and security protocols," *Sensors*, vol. 20, no. 12, p. 3590, 2020.

[13] "17.pdf," https://courses.csail.mit.edu/6.857/2017/project/17.pdf, (Accessed on 12/22/2021).

Comparisons between Bluetooth Low Energy and ZigBee		
Attribute	Bluetooth Low Energy	ZigBee
Network type	Personal Area network(PAN) supports few nodes(max 8 cell nodes)	Large Area Network(LAN) supports many nodes(up to 65000 nodes)
Connection Range	Can connect over distances as long as 77 metres	Connects over distances as long as 291 metres
Operating System compatibility	Android, iOS, Windows 8, OS X	Not compatible at the moment
Topology Type	Operates with Mesh and Star Topology Network	Operates with Mesh Only
Data Transfer	Transfers 270 kbps	Transfers 250 kbps
Modulation	Frequency-hopping spread spectrum (FHSS) varies between 2.4GHz to 2.483GHz	Direct-sequence spread spectrum (DSSS) only 2.4GHz worlwide
Power Transmission	10 mW could be transmitted at a time	100mW could be transmitted at a time
Bandwidth	Bluetooth requires low bandwidth.	While zigbee also requires low bandwidth but greater than Bluetooth's bandwidth most of time.
IEEE Standard	Bluetooth was developed under IEEE 802.15.1.	Whereas it was developed under IEEE 802.15.4.

TABLE I
COMPARISON BETWEEN BLE AND ZIGBEE [5] [4]

[14] F. Cayci, "Fpga assisted zigbee communication for low-power home automation design," https://udspace.udel.edu/bitstream/handle/19716/5715/Furkan$_Cayci_Thesis.pdf?isAllowed=ysequence=1,(Accessedon12/22/2021)$.