ENHANCED BLUETOOTH LOW ENERGY 5 AODV-BASED MESH COMMUNICATION PROTOCOL WITH MULTIPATH SUPPORT

MUHAMMAD RIZWAN GHORI

UNIVERSITI SAINS MALAYSIA

2023

ENHANCED BLUETOOTH LOW ENERGY 5 AODV-BASED MESH COMMUNICATION PROTOCOL WITH MULTIPATH SUPPORT

by

MUHAMMAD RIZWAN GHORI

Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

April 2023

ACKNOWLEDGEMENT

All praises are to Allah, the Merciful, the All-Beneficent, by whose Grace and Blessings I have been able to achieve this important milestone. To begin, I would like to express my heartfelt appreciation and gratitude to my supervisor, Associate Professor Dr. Wan Tat Chee, who has led and assisted me in overcoming every challenge with his vast research experience, intellect, and highly matured supervisory skills. He is also a punctual, honest, and disciplined individual, which speaks highly of his abilities and character. I would also like to thank Mr Gian Chand Sodhy, a very kind person who has always supported me and offered me advice whenever I needed it.

My heartfelt gratitude goes to my Father, Grandmother (Late), Mother, Brother, and other close family for all of their prayers, encouragement, and support in helping me earn my PhD.

My most sincere thanks to my wife, Amna Rizwan, who has been there for me during my time in Malaysia with her love, wise counsel, and tender care. With her great willpower, she kept me determined to finish my PhD.

I am grateful to School of Computer Sciences, Universiti Sains Malaysia for providing a stimulating and supportive atmosphere in which to complete my PhD tasks. In addition, I am grateful to the Institute of Postgraduate Studies, Universiti Sains Malaysia, for awarding me the USM Fellowship for the completion of my PhD.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

AC	Advertising Channel
AFH	Adaptive Frequency Hopping
AODV	Ad-hoc On-Demand Distance Vector
ARM	Authenticated Rank and routing Metric
ATT	Attribute Protocol
BATMAN	Better Approach To Mobile Adhoc Networking
BES	Best-Effort Scheduling
BLE	Bluetooth Low Energy
BTCP	Bluetooth Topology Construction Protocol
CbODRP	Cluster-based On Demand Routing Protocol
CBA	Cluster-Based Algorithm
CHA-IDS	Compression Header Analyzer Intrusion Detection System
CSRK	Connection Signature Resolving Key
D-AOMDV	Directional Ad-Hoc On-demand Multipath Distance Vector
DC	Data Channel
DC-BMN	Data-Channel-Based BLE Mesh Networks
DoS	Denial of Service
DREAM	Distance Routing Effect Algorithm for Mobility
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Control Routing
DT	Device Tree
ECDH	Elliptic-Curve Diffie–Hellman
E2SR2	Energy Efficient Secured Ring Routing
FM	FruityMesh
GAP	Generic Access Profile
GATT	Generic Attribute Profile
GLRT	Generalized Likelihood Ratio Test
HAN	Home Area Networks
HCI	Host Control Interface
HHT	Hilbert-Huang Transforms
HIRO-NET	Heterogeneous Intelligent Robotic Network

IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
6LoBLE	IPv6 over BLE
6TiSCH	IPv6 over Time-Slotted Channel Hopping
IRK	Identity Resolving Key
ISFC-BLS	Intelligent and Secured Fuzzy Clustering Algorithm Using Balanced Load Sub-Cluster Formation
JW	Just Work
LESC	Low Energy Secure Connection
LL	Link Layer
LLP	Low Energy Legacy Pairing
L2CAP	Logical Link Control and Adaptation Protocol
LTK	Long Term Key
MAC	Media Access Control
MHTS	Multi-Hop Transfer Service
MITM	Man In The Middle
ML	Machine Learning
MOFCA	Multi-Objective Fuzzy Clustering Algorithm
MRT	Multi-Hop Real Time
MSV	Message Security Value
NC	Numeric Comparison
NDN	Named Data Networking
NFC	Near Field Communications
NFV	Network Function Virtualization
NIC	Network Interface Card
NOC	Network Operation Centre
OLSR	Optimized Link State Routing
OOB	Out of Band
PAN	Personal Area Network
PDR	Packet Delivery Ratio
PKE	Pass Key Entry
PLC	Power Line Communications
RBF	RSSI-Based Bounded Flooding
RFID	Radio-Frequency Identification

SDN	Software Defined Network
SEECH	Scalable Energy Efficient Clustering Hierarchy
SIG	Special Interest Group
SM	Security Manager
SSP	Secure and Simple Pairing
STK	Short Term Key
STR	Shortcut Tree Routing
TDMA	Time-Division Multiple Access
TK	Temporary Key
TTDD	Two-Tier Data Dissemination
UUID	Universal Unique Identifier
VHF	Very High Frequency
WAHN	Wireless Ad-Hoc Network
WPAN	Wireless Personal Area Network

PROTOKOL KOMUNIKASI MESH BERDASARKAN AODV BLUETOOTH TENAGA RENDAH 5 YANG DIPERTINGKATKAN DENGAN SOKONGAN BERBILANG LALUAN

ABSTRAK

Rangkaian ad hoc tanpa wayar (WAHN) sedang berkembang dengan meluas akibat peningkatan teknologi internet pelbagai benda (IoT). Beberapa teknologi WAHN, termasuk *ZigBee, Z-Wave, Threads, Bluetooth Low Energy (BLE)* telah diwujudkan. Walaupun terdapat perkembangan dalam IoT, penghalaan berasaskan rangkaian terus kekal sebagai masalah kritikal yang perlu diatasi. Justeru itu, kajian ini berfokus kepada rangkaian mesh berasaskan BLE. Rangkaian mesh BLE membekal komunikasi fleksibel dan boleh dipercayai antara peranti-peranti IoT. Rangkaian mesh BLE membolehkan peranti-peranti kuasa rendah IoT berkomunikasi menggunakan cara fleksibel dan boleh dipercayai. Sebahagian besar protokol mesh berasaskan BLE dalam kajian literatur dibangunkan sebagai lapisan atas topologi bintang Bluetooth, menggunakan *piconet* dan *scatternet*. Rangkaian mesh BLE tradisional mempamerkan kaedah membanjir untuk komunikasi berbagai hop, yang menyebabkan overhed tinggi akibat daripada penyiaran mesej tanpa mekanisme penghalaan. Protokol Vektor Jarak Atas Permintaan Ad hoc (AODV) merupakan salah satu protokol penghalaan yang paling popular untuk WAHN. Namun begitu, AODV mempamirkan bilangan paket kawalan yang besar khususnya ketika gangguan sambungan,yang menyebabkan kesesakan, overhed dan penangguhan; mengakibatkan nisbah penghantaran paket (PDR) yang lebih rendah berbanding protokol BLE berdasarkan kaedah banjir. Akibatnya, protokol Vektor Jarak Atas Permintaan Ad hoc yang Dioptimumkan (O-AODV) dicadangkan untuk mempertingkatkan prestasi penghantaran data dari segi

overhed dan penangguhan. Sebagai tambahan, untuk mengatasi kelemahan protokol O-AODV sekiranya terdapat gangguan sambungan, ia ditambah-baik dengan sokongan berbilang laluan menjadikannya Protokol Vektor Jarak Atas Permintaan Ad hoc yang Dioptimumkan dan Berbilang Laluan (M-O-AODV), yang dapat mempertingkatkan keteguhan protokol yang dicadang. M-O-AODV dapat mencapai PDR yang tinggi setanding dengan BLE berdasarkan kaedah banjir, tidak seperti protokol lain seperti AODV dan AODV Sonsang Berbilang Laluan (M-R-AODV) yang digunakan sebagai bandingan. Berbanding dengan BLE berdasarkan kaedah banjir, protokol O-AODV melaporkan pengurangan muatan trafik, overhed (dengan pengurangan overhed sebanyak 16% dan 53% masing-masing berbanding dengan AODV dan BLE berdasarkan kaedah banjir), masa lengah hujung ke hujung (1000 ms dan 2000 ms lebih rendah berbanding AODV dan BLE berdasarkan kaedah banjir masing-masing) dan purata masa lengah satu arah setiap lompatan (purata penangguhan setiap lompatan adalah 8% hingga melebihi 20% lebih rendah bebanding protokol-protokol lain). Sebagai tambahan, protokol yang ditambah baik untuk komunikasi berbilang laluan (M-O-AODV) didapati mencapai nisbah penghantaran paket (PDR) sebanyak 88%, setanding dengan nilai PDR 92% untuk protokol BLE berdasarkan kaedah banjir. Selain dari itu, M-O-AODV telah diuji untuk keteguhan dan didapati memberikan masa yang lebih baik iaitu 3700 ms untuk kes kegagalan nod, berbanding dengan protokol-protokol lain yang mengalami tangguhan antara 4800 ms sehingga 6000 ms. Berdasarkan keputusan ini, sekiranya tiada medium komunikasi berdawai, rangkaian mesh BLE berdasarkan protokol M-O-AODV dijangka berkesan untuk diguna dalam persekitaran Industri 4.0.

ENHANCED BLUETOOTH LOW ENERGY 5 AODV-BASED MESH COMMUNICATION PROTOCOL WITH MULTIPATH SUPPORT

ABSTRACT

Wireless Ad-Hoc Networks (WAHN) are growing more widespread due to improvements in Internet of Things (IoT) technologies. Several WAHN technologies, including ZigBee, Z-Wave, Threads, Bluetooth Low Energy (BLE) are available. Despite progress on IoT, network-based routing continues to be a critical problem that has to be tackled. In view of the above, this study focuses on a BLE-based mesh network. BLE mesh networks provide flexible and reliable communication between IoT devices. BLE mesh networks enable low-power IoT devices to communicate in a flexible and dependable manner. The majority of BLE-based mesh protocols in the literature are built as overlays on top of normal Bluetooth star topologies, employing piconets and scatternets. Traditional BLE mesh networks exhibit flooding for multi-hop communication, which results in high overheads due to message broadcasting without a routing mechanism. The Ad hoc On-Demand Distance Vector (AODV) protocol is one of the most popular routing protocols for WAHN. However, AODV exhibits large number of control packets, especially in case of link disruption and hence causing congestion, overheads, and delay; resulting in a lower Packet Delivery Ratio (PDR) compared to the flooding-based BLE protocol. Consequently, the Optimized AODV (O-AODV) protocol is proposed to improve the data forwarding performance in terms of overheads and delays. Moreover, to overcome weaknesses in the O-AODV protocol in case of link failures, it is further enhanced with multipath support to become Multipath O-AODV (M-O-AODV), which significantly increases the robustness of the proposed protocol. M-O-AODV is able to achieve a high PDR which is comparable to flooding-based BLE, unlike other protocols such as AODV and Multipath-Reverse-AODV (M-R-AODV) are used for comparison. In comparison with flooding-based BLE, the proposed O-AODV protocol reduces traffic loads, overheads (with 16% and 53% lower overheads than AODV and flooding-based BLE respectively), end-to-end delays (1000 ms and 2000 ms lower than the AODV and flooding-based BLE respectively) and average per-hop one-way delay (8% to over 20% lower average per-hop delay compared to the other protocols). Additionally, the proposed protocol is enhanced for multipath communication (M-O-AODV) is found to have a PDR of 88%, which is comparable to the PDR of 92% for the BLE-based flooding protocol. Also, M-O-AODV has been tested for robustness and has given a better time of 3700 ms in case of a node failure, as compared to the other protocols that experienced delays ranging from 4800 ms to 6000 ms. Based on the results, in the absence of any wired communication medium, M-O-AODV protocol-based BLE mesh networks are expected to be effective for use in Industry 4.0 environments.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Bluetooth Low Energy (BLE) is a Wireless Ad-Hoc Network (WAHN) protocol which is becoming increasingly popular for battery-powered Internet of Things (IoT) devices. The Bluetooth Special Interest Group (SIG) introduced the BLE standard in Bluetooth version 4.0, and it has been further improved in versions 4.2 and 5. BLE 4.x initially used the traditional Bluetooth Personal Area Network (PAN) paradigm for multi-hop communications and network interconnections. Now, BLE 5 has overcome the shortcomings of previous versions (i.e., supporting only star topology with small network size, lesser range, and short battery life) by implementing a pure mesh architecture to enable increased network coverage, inter-network connection, and security (Darroudi & Gomez, 2017).

The majority of BLE-based apps continue to operate in a star network architecture while employing BLE Beacons in broadcast mode (Gohel, 2018; Sthapit et al, 2018; Yumantoro et al, 2018; Handojo et al, 2018, Sunardy & Surantha, 2018; Mohsin et al, 2018; Giovanelli, 2018). Hybrid mesh topologies extend the master-slave piconet paradigm into diverse interconnected scatternets through the combination of star and mesh links to improve the coverage of BLE 4 networks (Jung et al, 2017). Nonetheless, reliability and scalability are still issues in hybrid mesh networks. A pure mesh topology, on the other hand, eliminates the master-slave limitation by having nodes peer with one another to construct scalable networks. However, so far, there is very little research on the application of BLE 5 pure mesh topologies. Also, the available BLE-based protocols do not provide routing support for message communication (Leonardi et al, 2018).

The vast majority of BLE-based mesh protocols are created as overlays on top of standard Bluetooth star topologies, leveraging piconets and scatternets. Traditional BLE mesh networks, exhibit flooding for multi-hop communication, resulting in large overheads and communication delays due to message broadcasting without a routing mechanism. AODV is a popular and reliable routing protocol for Wireless Ad-Hoc Networks (Zhang & Sun, 2016).

1.2 Use Case

Wireless Ad-Hoc Networks (WAHN) are becoming increasingly popular due to their unique characteristics, such as the lack of infrastructure and consumption of low power for communication. Subsequently, implementation of WAHN shall be beneficial in an Industry 4.0 environment as there are various processes involved in the industry that require access to devices or equipment which are not well supported by wired infrastructure. Many technologies are available, to make WAHN applicable to the Industry 4.0 environment, like ZigBee, Z-Wave, Threads, BLE, and others. BLE 5 can be an efficient solution, in the industrial sector, for facilitating short-range data transmission (Beelde, 2021). Bluetooth sensors and beacons can be used in the most difficult areas where a wired network cannot be established. In the light of foregoing, and extensive literature research, Bluetooth Low Energy 5 (BLE 5) is the best suitable technology for its easy availability in mobile devices (Bluetooth, 2020), low power consumption (Darroudi & Gomez, 2017), low cost, and mesh support (Bluetooth, 2020) characteristics. Consequently, this research will focus on routing-based BLE mesh protocol which is aimed to assist in managing and optimizing the functioning of industrial processes as well as supply chains, by obtaining real-time data for quicker decision-making. This will ultimately enhance the efficiency of the industry's overall operations.

1.3 Problem Statement

Wireless Ad-Hoc Networks (WAHN) are gaining popularity as they require no infrastructure while having the advantage of consuming low power for communication. When it comes to communication in critical areas in the industry, where different manufacturing processes are involved and a wired network is not possible, infrastructure-less communication is very much necessary. Therefore, for the industrial areas, there is a requirement for an efficient BLE-based mesh communication network (Garrido, 2018). Consequently, for the said purpose, there is a strong need for a suitable mesh protocol that can make communication efficient and robust (Jung et al, 2017). During the last few years, researchers have presented different strategies (flooding-based and routing-based) to enable mesh topology for BLE (Darroudi & Gomez, 2017). Flooding is a simple solution because it does not involve the formation of a connection or the routing protocol (Murillo et al, 2017, 2019). Due to the lack of a routing mechanism, it avoids route formation delays and consumes less memory. However, flooding is inefficient because there would be a flood of messages for successful end-to-end communication, which can cause network congestion and overheads and hence consumes more power resources (Dvinge et al, 2019). To address these concerns, the AODV routing strategy is best suited for large networks that require efficiency (Kaur & Kumar, 2012). According to the literature review, researchers have proposed various solutions for the implementation of the BLE mesh routing protocol. However, regarding routing-based mesh solutions, a single BLE-based protocol is available, by (Hussein et al, 2020), which presents an AODV-based solution for BLE Mesh Networks. Nevertheless, there are still issues which need to be resolved such as (a) High overheads and delays due to absence of efficient forwarding mechanism. (b) Lack of multipath forwarding approach in case of link disruption. In contrast to directed forwarding protocols, flooding techniques are more resilient to link disruption since there is no single point of failure and an alternate path is always available (Sharma, Kumar & Kishore, 2013). (c) Low PDR as compared to mesh protocols. Since mesh utilizes a flooding approach for message replication, it has a higher PDR than directed forwarding. The flooding approach enhances the likelihood of message delivery to the destination nodes but incurs more overheads and delays (Mangrulkar & Atique, 2010).

Therefore, the focus of this thesis will be on resolving the issues, faced by the flooding approach, in BLE mesh routing to improve the network efficiency and robustness for efficient communication.

1.4 Research Objectives

The key objectives of this research are as follows:

i) To improve the data forwarding performance of the BLE Mesh network by reducing overheads, and delay compared to the flooding approach using more efficient forwarding techniques.

ii) To investigate the effectiveness of multipath forwarding for improving the robustness of the proposed protocol in terms of link setup time, end-to-end delays, and link recovery time when dealing with link disruptions.

iii) To achieve a PDR comparable to the BLE-based mesh flooding approach using multipath forwarding mechanism, for normal connectivity and when experiencing link disruptions.

1.5 Project Scope

i) The main focus of this research is on enhancing data forwarding performance for BLE Mesh topology with multiple hops.

ii) Other aspects of BLE Mesh configuration such as security and authentication are not addressed and will use the available standards and solutions.

iii) The research will focus on unicast and broadcast traffic only. Multicast traffic forwarding will not be addressed.

iv) Evaluation of actual performance using physical nodes in a testbed is used to obtain experimental data for comparison with existing protocols.

v) Transmission range of the nodes has been minimized through 2-2.5 meters by reducing transmission power.

vi) The experimental testbed is assumed to experience minimum radio frequency (RF) interference.

vii) All the nodes are static.

1.6 Thesis Contribution

BLE devices are Internet of Things (IoT) devices that potentially improve and transform Industry 4.0 situation management and the safety of human lives. Considering the foregoing, this research has focused on optimizing the data forwarding performance of the BLE Mesh network by reducing overheads, delay, and packet loss compared to the flooding approach. This study has also concentrated on strengthening the robustness of the proposed protocol against link disruptions, through multi-path support in order to enable an effective Industry 4.0 communication network, involving the most critical and sensitive sites, requiring better message delivery performance. Consequently, the key contributions of this thesis are as follows:

i) Improved the data forwarding performance with reduced overheads and delays.
ii) Improved the robustness of the proposed protocol in case of link failure.
iii) Achieved the PDR comparable with BLE-based mesh flooding approach.

1.7 Thesis Organization

The thesis is structured in such a way that it should cover all the details in depth. As a result, **Chapter 2** covers the related works on BLE mesh protocols.

Furthermore, in **Chapter 3**, the details of the approach, (including the proposed optimized protocol) for enabling the B5AMPN communication system, are provided.

The **fourth chapter** discusses testbed and the numerous topologies developed for experimentation and analysis. **Chapter 5** provides the experimental results with details, and finally, **Chapter 6** concludes the thesis.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, initially, a comparison of mesh-based IoT technologies has been made. Subsequently, the details of mesh-based IoT technologies are covered in section 2.2 and BLE mesh system architecture are covered in section 2.3. Also, this chapter includes a discussion related to single and multi-path AODV protocols. Moreover, section 2.4 discusses the most recent BLE-based communication protocols as well as related security challenges to grasp the present state of BLE mesh protocol development and open research areas. Finally, the extracted research gaps have been discussed along with BLE mesh networking concepts. Section 2.5 summarizes the chapter.

2.2 Mesh-Based IoT Technologies Comparison

Many mesh-based IoT technologies are available to make WAHN practical, including ZigBee, Z-Wave, Threads, BLE, and others. Therefore, a detailed analysis of various mesh IoT technologies has been done to select the best possible technology.

The summary and comparative analysis are shown in Table 2.1.

Table 2.1. Summary of Various Mesh based IoT Technologies (Yin et al, 2019)

Characteristics	ZigBee	Sub-GHz	Wi-Fi	Classic Bluetooth	BLE
Physical Layer Standard	802.15.4	802.15.4g	802.11	802.15.1	802.15.1
Application Focus	Monitoring and Control	Monitoring and Control	Internet Usage, Web	Short Range Wireless Communication	Monitoring, Control, Low Power, Proximity Control, Accurate Localization
Speed	Up to 250 kbps	Up to 200 kbps	Up to 72 Mbps	2 Mbps	2 Mbps
Battery Life (in days)	200-1000+	1000+	0.5-5	1-7	Up to years
Network Size	100s-1000s	10s-100s	255	7	With Mesh Topology can be more than 1000s
Range (meters)	1-100+	1-7000+	1-30+	1-10+	Long Range with Mesh Topology
Network Architecture	Mesh	Point-Point, Star	Star	Star	Star, Mesh
Optimized for	Reliability, Low Power, Low Cost, Scalability	Low Range, Low Power, Low Cost	Speed	Low Cost and Convenient	Low Cost, Very Low Power, Convenient (Easily available in Mobile devices), BLE Beaconing, Reliability

As shown in Table 2.1, the major parameters for selecting IoT technology are the desired operational range, data transfer speed, power consumption, cost, easy availability, and reliability. According to the analysis, BLE technology addresses all of the aforementioned issues and is well-suited for ad-hoc networks due to its widespread availability in mobile devices, low power consumption, and support for mesh topology.

Due to its simpler routing technique, BLE is better suited for mobile nodes than the Zigbee routing protocol, which necessitates additional network overhead to maintain route tables for mobile nodes. It is essential to consider the use case before choosing one of these technologies. BLE has a few benefits over Zigbee, including less expensive hardware, reliable protocol stacks in widely adopted OS implementations, and smartphone control. Additionally, according to Fafoutis et al, 2016, BLE technology is favored over other 802.15.4 technologies like Wifi, Threads. because it is more widely used in the real world, consumes less power, is more effective for mobile nodes, naturally supports communication with smartphones, and does not need IP support.

2.3 BLE Mesh System Architecture

The BLE Mesh System Architecture is a layer that is added on top of the BLE Network Stack. To describe the various words and concepts used throughout the study, a quick introduction to the fundamental BLE Network Stack and BLE Mesh Layers is provided.

2.3.1 BLE Network Stack

The Host, Controller, and Physical/Radio Layers (Zephyr Projects, 2020) are the three fundamental layers of the BLE Network Stack. This section serves as a reference for the succeeding sections with a brief explanation.

The Host layer, which sits just beneath the application layer, has many non-real-time network and transport protocols that allow apps on different devices to communicate with one another. Generic Access Profile (GAP), Generic Attribute Profile (GATT), Security Manager (SM), Attribute Protocol (ATT), and Logical Link Control and Adaptation Protocol (L2CAP) are among the modules found in this layer.

BLE Link Layer (LL) protocols (low-level and real-time) are implemented by the Controller layer. BLE LL performs packet reception, schedules transmissions, and ensures data delivery (Townsend et al, 2014), in addition to handling control operations and physical layer interfaces via the Host Control Interface (HCI).

The physical layer is in charge of wireless signal transmission. BLE uses the 2.4 GHz ISM (Industrial, Scientific, and Medical) frequency spectrum, with 40 narrowband channels (2 MHz bandwidth) divided into three Advertising Channels (AC) (Ch. 37–39) and 37 Data Channels (DC) (Ch. 0–36) (Yin et al, 2019). Device detection, connection establishment, and the transmission of broadcast messages are all handled by the ACs. DCs, on the other hand, allow two-way data flow between linked devices and rely on Adaptive Frequency Hopping (AFH) for subsequent communications.

Moreover, Figure 2.1 is depicting the BLE Network Stack.

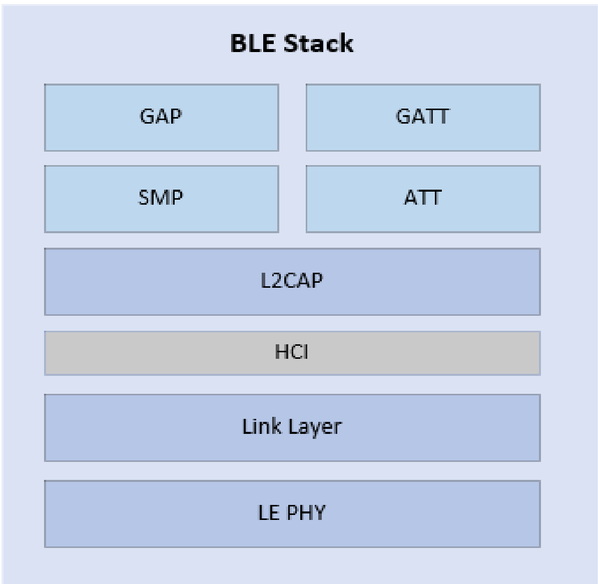

Figure 2.1 BLE Network Stack

2.3.2 Communication Profiles BLE

This section provides a basic overview of BLE Communication Profiles such as GAP, GATT, Security Manager, and Attribute Protocol.

The Generic Access Profile (GAP) offers a standard structure for how Bluetooth Low Energy (BLE) devices link (Tosi et al, 2017). A BLE device can function as a Broadcaster (advertises but does not allow connections), an Observer (sees advertisements but does not initiate connections), a Peripheral (advertises and accepts connections), or a Central (sees advertisements and starts connections) (Darroudi & Gomez, 2017). BLE enables connectionless communications between Broadcasters and Observers through the use of advertisements (called beacons), as well as connection-oriented communications between Peripheral and Central devices.

A BLE Peripheral device, for example, broadcasts its presence at first, while the receiving device, a mobile phone acting as the Central, establishes a connection with the Peripheral to enable two-way communication. Following the formation of the connection, the Central will operate as the master and the Peripheral as the slave. To allow more complicated topologies, devices may also implement multiple roles.

The Generic Attribute (GATT) profile specifies how data is transferred after the GAP has established a dedicated connection. It also specifies node roles, with one acting as the client and the other as the server.

The Security Manager specifies how devices are paired and keys are distributed. It provides secure communications and data transfer services to other layers (Bluetooth, 2020).

Clients' and servers' roles are defined via the Attribute protocol. A client sends requests to the server for reading and writing available attributes (data) that are stored on the server, while the server is in charge of storing the attributes and making them available to the client (Bluetooth, 2020).

The L2CAP profile provides the upper layer with connection-oriented and connectionless data services, as well as multiplexing, segmentation, and reassembly capabilities (Gomez et al, 2012).

2.3.3 BLE Mesh Layers

As demonstrated in Figure 2.2, the BLE Mesh System Architecture is defined on top of the BLE core specifications (Bluetooth, 2020). In the diagram, the Bearer Layer is supported by the BLE Network Stack Host protocols.

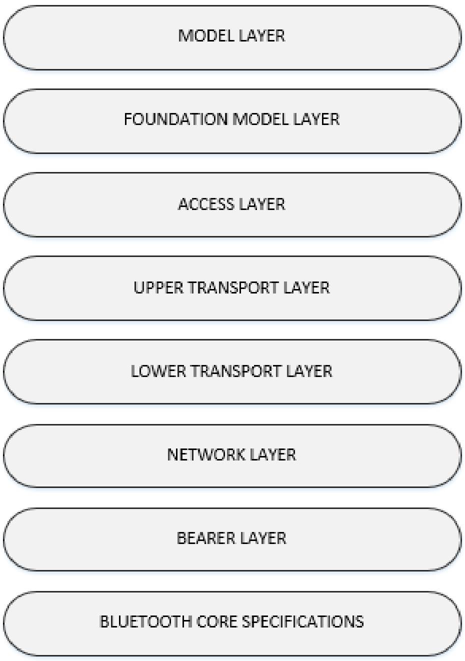

Figure 2.2 BLE Mesh Layers

Models define operations depending on usage scenarios and are found in the Model layer. These models are either defined as Bluetooth Mesh Model Specifications or by vendors (vendor models). The models are recognized by Bluetooth SIG and vendor-defined 16-bit and 32-bit unique identifiers.

The Foundation Model layer defines the states, messages, and models required to configure and manage mesh networks for certain scenarios. The Bluetooth SIG Specification defines two types of models: Configuration Client and Server models and Health Client and Server models.

The Access Layer specifies how upper layers can use the Upper Transport Layer. Furthermore, it is in charge of defining the application data format and implementing encryption/decryption functionalities. Finally, it ensures that incoming data contains the right network and application keys before transferring it to the upper layers.

The Upper Transport layer is in charge of encrypting, decrypting, and authenticating application data, as well as providing access message confidentiality. Furthermore, it defines the control messages used to coordinate the transport layer functions between nodes.

The Lower Transport layer specifies the segmentation and reassembly of upper-layer messages into different lower-layer protocol data units. It also manages segmentation and reassembly control messages.

The Network layer is in charge of addressing, formatting, encryption, and authentication for data communications. This layer is also responsible for message forwarding and dropping decisions.

The Bearer Layer defines the message transport mechanism. There are now two bearers available in the current BLE 5 Mesh standard, namely the Advertising bearer and GATT bearer.

2.3.4 BLE Mesh Networking Concepts

The BLE Mesh System Architecture is a library for enabling mesh functionality in a Bluetooth Low Energy network. It sits on top of the BLE Networking stack, which manages the BLE node's radio communications. A BLE node in a mesh can communicate with any other node in many to many architectures (Bluetooth, 2020).

2.3.4(a) Provisioning and Configuration

An unprovisioned device is one that is not connected to an existing BLE mesh network. If a device wishes to join a specific mesh network, it must first be provisioned (Bluetooth, 2020). After provisioning, the device will turn into a BLE Mesh node capable of communicating with other nodes. Furthermore, the node must be configured based on its functioning. A light switch, for example, must be programmed to operate one or more light bulbs (Bluetooth, 2020).

2.3.4(b) Nodes and Elements

A node is a device that has joined the BLE mesh network and can support varied levels of complexity. A simple LED light bulb, for example, merely emits monochromatic light. Multi-colored LED bulbs, on the other hand, can emit a variety of colors. As a result, each colored LED in a single node is referred to as an element, and every BLE mesh node must contain at least one element. One of the elements in the multi-element node is identified as primary or root, and it contains all of the configuration data (Bluetooth, 2020).

Control or access messages are used to communicate between nodes in a BLE mesh network. The former messages are associated with mesh network operations; for example, a message to check the presence of a specific node in a network. The latter messages are used to control application functionality, such as when a BLE mesh light switch sends a SET message to a group of lights to turn them on (STATE change from off to on). In addition, the node can use a GET message to acquire the state information of particular nodes, which will be returned in a STATUS message.

2.3.4(c) BLE Mesh Models

In the current Bluetooth Mesh Model Specification, 52 Bluetooth SIG accepted client/server models are described, divided into four groups: generics, models for sensors, models for lighting, and time/scene models. The model specifies a set of states as well as their binding, transition, messages, and other associated properties. For the implementation of needed functionality, each BLE node may consist of one or more models of any type (SIG accepted or Vendors models) (Zephyr Projects, 2020 and Bluetooth, 2020).

A BLE Mesh-enabled light bulb that can be turned on and off using a BLE Mesh-enabled light switch is an example of a Generic On/Off Client-Server model. The Generic On/Off Server model will be used by the light bulb, while the Generic On/Off Client model will be used by the light switch.

Furthermore, the Bluetooth SIG specifications' foundation models, namely the Configuration Client and Server models, and the Health Client and Server Models are required for the management of the network, and all the devices participating in the mesh network must implement these models for configuration and health monitoring (Zephyr Projects, 2020; Bluetooth, 2020).

2.3.4(d) BLE Security Features

BLE implemented additional features to strengthen the security of IoT-enabled devices (Bluetooth Mesh Security Overview, 2020). To enable encrypted communications, BLE uses Legacy Pairing or Secure Connection (Bluetooth 4.2).

Moreover, this research has utilized the existing security mechanisms as-is in the proposed solution.

a. Low Energy Pairing

Low Energy Pairing (Connection) is further classified into the following groups:

Low Energy Legacy Pairing (LLP)

In Bluetooth 4.2, Low Energy Pairing (LP) for encrypted connections was renamed Low Energy Legacy Pairing (LLP). In LLP, an LTK is created and distributed first using the Transport Protocol (TP). LLP generates the LTK on one device and securely transports it to other devices during the pairing process, rather than requiring both devices to generate keys independently. Furthermore, because the keys (LTK, Identity Resolving Key (IRK), and Connection Signature Resolving Key (CSRK)) must be transmitted to the other device, an extra step is necessary for their distribution. LLP, on the other hand, uses the same pairing process as legacy Bluetooth and is hence vulnerable to eavesdropping attacks unless Out of Band (OOB) pairing with a 128-bit Temporary Key (TK) is employed (Padgetter et al, 2020).

Low Energy Secure Connection (LESC)

The LTK key in LESC (Bluetooth 4.2) is generated and held locally within each device via mutual key agreement, and hence does not need to be exchanged over a link. Unlike LLP, an LTK is generated during the pairing process rather than a Short Term Key (STK). Following that, the encryption key is obtained from the LTK in order to secure the communication, and the IRK and CSRK are exchanged between the two devices. LESC improves security by employing ECDH public-key cryptography (P-

256 Elliptic Curve) to prevent eavesdropping and MITM attacks (Padgetter et al, 2020).

b. Low Energy Pairing Association Models (LEPAM)

LEPAM is the pairing technique utilized by LLP and LESC (Padgetter et al, 2020).

Out of Band (OOB)

An out-of-band technique is utilized for device discovery and the exchange of cryptographic data to be used in the pairing process, which is commonly accomplished through the use of Near Field Communications (NFC) technology. When compared to the PKE and JW approaches, this is more secure. Nonetheless, the OOB model's security is dependent on the mechanism utilized.

Pass Key Entry (PKE)

The first device will display a 6-digit passkey that must be typed into the second device. In-band eavesdropping attacks are not possible because the passkey is not transferred during the pairing process. Furthermore, the usage of EDCH key agreement methods helps protect it from passive attacks.

Just Work (JW)

This approach provides no security because devices must accept connections without verification. This mechanism is typically used by peripherals such as mice and headphones. It is vulnerable to Man in the Middle (MITM) attacks, but certain passive attacks can be neutralized by using EDCH key agreement methods.

Numeric Comparison (NC)

Both devices display their own 6-digit numbers, and the user confirms whether the numbers match. This differs from PKE in that the 6-digit number is not used to generate link keys. As a result, an eavesdropper who obtains the 6-digit number cannot deduce the encrypted connection key (Padgetter et al, 2020).

2.4 BLE Mesh Communication Protocols

In this section, there will be a discussion on the most recent BLE-based mesh communication protocols, as illustrated in Figure 2.3. Following an introduction of the numerous protocols in each category, a critical review of the cited works is provided, together with their advantages and disadvantages and open issues. Moreover, Table 2.2 summarizes this discussion.

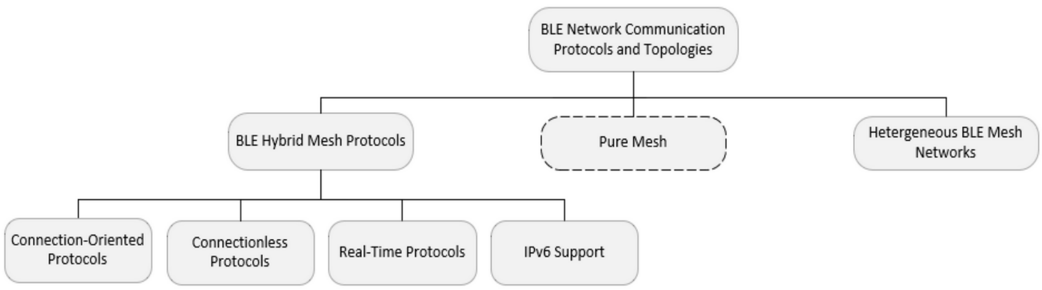

Figure 2.3 Classification of BLE Communication Protocols

2.4.1 Message Forwarding Paradigms

To help the reader comprehend the taxonomy in Figure 2.3, a quick overview of three basic message forwarding paradigms used by various multi-hop forwarding protocols is provided here.

2.4.1(a) Reactive (On-Demand) Protocols

Reactive forwarding schemes use received messages to get information about destination nodes (Zhang & Sun, 2016). Each forwarding table entry is only active for a limited time. The entry will be removed if no traffic for a certain destination was detected during the stated time frame (Saini & Sharma, 2020). If the sender node requests it, a new route discovery procedure is started (Bhushan et al, 2013; Kaur & Kumar, 2012). Ad-hoc On-Demand Distance Vector (AODV) (Perkins & Das, 2003) and Dynamic Source Control Routing (DSR) (Johnson & Hu, 2007) are two examples of reactive forwarding protocols.

2.4.1(b) Proactive (Table Driven) Protocols

All nodes, whether active destinations or not, have explicit forwarding table entries in proactive forwarding protocols. The Bellman–Ford Algorithm is often used to maintain feasible pathways to the respective nodes, and data can be transmitted instantly and without delay to a destination. Babel (Chroboczek, 2011), Optimized Link State Routing (OLSR) (Clausen & Jacquet, 2003), Destination Sequenced Distance Vector (DSDV) (Perkins & Bhagwat, 1999), Distance Routing Effect Algorithm for Mobility (DREAM) (Basagni, 1998), and Better Approach To Mobile Adhoc Networking (BATMAN) (Neumann et al, 2008) are examples of proactive forwarding protocols.

2.4.1(c) Cluster-Based Protocols

Scatternet is a cluster-based forwarding mechanism that was introduced in BLE 4.1 to facilitate multihop communications. Cluster-based forwarding protocols were created originally for mobile ad-hoc networks. It separates a network's nodes into many overlapping disjoint clusters (Jiang et al, 1999). Each cluster is led by an elected cluster head who is in charge of maintaining cluster memberships, which are then utilized for inter-cluster path finding. The clustering of nodes lowers flooding during the path discovery phase.

Furthermore, the protocol tracks any unidirectional links for inter-cluster and intra-cluster forwarding. Two-tier data dissemination protocol (TTDD) (Luo, 2005), Ring Routing (Tunca et al, 2015), Energy Efficient Secured Ring Routing (E2SR2) (Bhushan & Sahoo, 2019), Intelligent and Secured Fuzzy Clustering Algorithm Using Balanced Load Sub-Cluster Formation (ISFC-BLS) (Bhushan & Sahoo, 2020), Scalable Energy Efficient Clustering Hierarchy protocol (SEECH) (Tarhani et al, 2014), and Multi-Objective Fuzzy Clustering Algorithm (MOFCA) (Sert et al, 2015) are examples.

2.4.2 BLE Hybrid Mesh Protocols

Traditional Bluetooth networks used star topologies in master-slave configurations (Leon et al, 2017; Sikora et al, 2018; Garcete et al, 2018). Because such topologies are inefficient for supporting large numbers of IoT devices, contemporary BLE networks have emphasized the usage of Scatternets, which are hybrid star topologies, to improve network efficiency and scalability.

2.4.2(a) Connection-Oriented Protocols

Because of the master-slave relationship within a piconet (cluster), as well as the limited number of inter-cluster communication links between one BLE piconet and another, scatternets often form tree-structured networks. As a result, scatternets use connection-oriented links for data transmission. Because the loss of inter-cluster links results in disjointed clusters, this can lead to fragile network topologies (Balogh et al, 2015).

Mikhaylov & Tervonen (2013) suggested an early BLE mesh system known as MultiHop Transfer Service (MHTS). The researchers used on-demand routing for multi-hop communication of nodes using Texas Instruments' CC2540 SoCs. Furthermore, the proposed approach worked well for 2-hop and 3-hop data forwarding. Nonetheless, due to numerous scalability concerns, additional protocol development is required to enable a greater number of nodes in a larger network.

Wang & Chiang (2017) suggested a BLE-based tree topology protocol that is connection-oriented. The 37 Bluetooth data channels are used by the BLE-Tree Network to construct master-slave chains. Each device has two Bluetooth Low Energy interfaces, one configured as a Master and the other as a Slave. The tree topology is maintained by four processes: Master Agent, Slave Agent, Scan Center, and Sensor Center. The Master Agent establishes links with other devices (slaves) in its vicinity. The Slave Agent broadcasts its UUID in order for surrounding devices' Master Agents to discover it. The Slave interface uses the Scan Center to listen for neighbor broadcasts and deliver messages to its associated Master Agent, whereas the Sensor Center maintains neighbor MAC addresses and transmits data to them. The achieved Packet Delivery Ratio (PDR) was significantly higher than that of connectionless (broadcast) protocols.

Martinez et al (2018) used an existing mesh protocol to construct a mesh topology for office doorbells for the office. To show the efficiency of the BLE mesh network, the system made use of a Nordic Semiconductor board and the Softdevice libraries. Sirur et al (2015) developed an on-demand routing technique for data transmission optimization based on a weight-balancing approach. Their method allows for dynamic node organization for optimal data forwarding.

As per Balogh et al (2015), the scatternet architecture used in BLE 4.1 enables long-distance communications. To circumvent the constraints of the scatternet requirements in BLE 4.1, the authors presented a service mediation concept based on the Named Data Networking (NDN) methodology in the study. Guo et al (2015) created an on-demand multi-hop BLE routing protocol based on the BLE 4.1 scatternet topology. On real hardware, the suggested system was tested, and the protocol functioned well in terms of latency and resource utilization.

Bardoutsos et al (2019) suggested a multi-hop tree-based wireless network with multi-protocol gateways that used heterogeneous technologies, such as Wifi and BLE, to enhance energy efficiency and presented encouraging results. Similarly, Dvinge et al (2019) tested the power consumption of nodes while utilizing the FruityMesh protocol to demonstrate that connection-oriented Bluetooth mesh networks, due to their low power consumption, could be a good solution for off-grid applications. Murillo et al (2019), on the other hand, used a Software Defined Network (SDN) strategy to obtain longer lifetimes for static BLE resource-constrained nodes. The proposed protocol was designed to strike a balance between the number of connection events and the amount of energy consumed.

Ng & She (2019) introduced a unique BLE-based overlay mesh approach to overcome best-effort scheduling (BES) and RSSI-based bounded flooding (RBF) limitations in a BLE beacon-based network to achieve mesh functionality. Twenty Bluetooth Low Energy (BLE) devices and four Android mobile devices were employed to conduct sensing/advertising and receiving activities, outperforming existing methods.

Jung et al (2017) proposed an on-demand multi-hop routing mechanism based on Bluetooth Low Energy. Using an on-demand (reactive) routing protocol, the CbODRP protocol solved topology configuration difficulties (node discovery, piconet, and scatter net creation) and cluster recovery processes. During node discovery, all BLE nodes transmit advertising and update their neighbor count value in order to pick a master device with the most neighbors, with the device id acting as a tiebreaker. Following that, master nodes form piconets with their neighbors. Scatternet formation then takes place in two stages. In stage one, a neighbor node from another piconet with the lowest id is chosen as a relay node, and a link is formed with that piconet. As illustrated in Figure 2.4, in phase two, slave nodes in the current piconet locate neighbors from other piconets that do not have established connections and notify the master of possible relay nodes for new connections. In the event of a master node failure, for cluster recovery, the neighbor count metric is used to select a replacement master for a piconet. By clustering, messages for batch transmission to master and relay nodes, routing overhead is decreased. When compared to traditional on-demand routing systems, the proposed protocol minimizes energy consumption and route discovery delays.

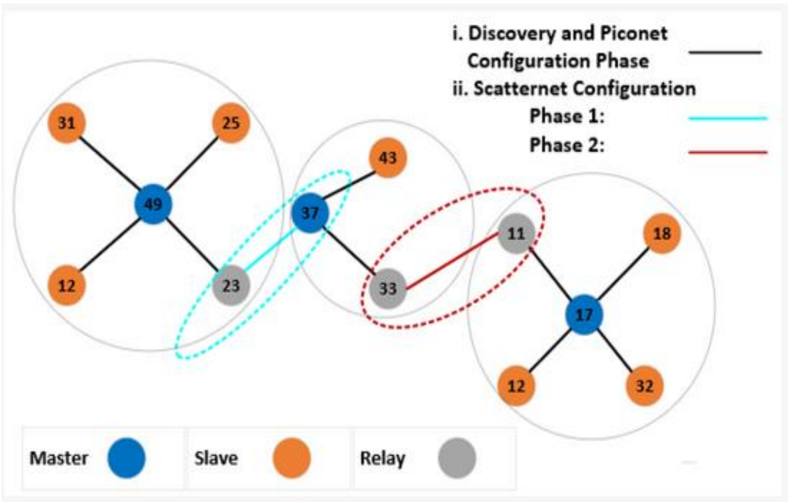

Figure 2.4 Cluster-Based On-Demand Routing Protocol (Jung et al, 2017)

According to Darroudi & Gomez (2018), connectivity is a major element of any wireless mesh network. An analytical model for node connection probability was proposed by the authors. Isolated nodes are regarded as being outside the network in their model. Furthermore, two nodes can only link if they have a suitable amount of time slots for communication. The formula for determining the likelihood of at least one connection between a node and its neighbors, as well as the formula for calculating the chance of node connectivity via k distinct paths, were demonstrated. The developed model was evaluated via simulation and proven to be suitable for analyzing data-channel-based BLE mesh networks (DC-BMN).

2.4.2(b) Connectionless Protocols

Due to the constraints of connection-oriented scatternet-based mesh protocols, the use of connectionless forwarding in BLE Mesh topologies evolved. Connectionless forwarding is accomplished by flooding Broadcast packets throughout the BLE Mesh topology.

Murillo et al (2017, 2019) used the Nordic nRF52 development board to test PDR, end-to-end delay, and power consumption for the Trickle (flooding-based connectionless) and FruityMesh (connection-oriented) protocols, respectively. When compared to a connection-oriented strategy for comparable PDR objectives, the flooding approach produced reduced end-to-end delay at the expense of higher power consumption.

According to Chiumento et al (2018), control parameters must be carefully set in order to establish a reliable and robust interconnected mesh network with the lowest congestion and packet loss probability. Furthermore, Hansen et al (2018) studied the influence of relay node selection on the overall PDR of flooding-based BLE mesh networks. Better overall network performance was achieved despite employing fewer relay nodes; thus, optimal relay node selection is crucial. Among three automated candidate relay selection algorithms, namely Greedy Connect, K2 Pruning, and Dominator, the K2 Pruning approach achieved the greatest performance at the expense of high data storage needs. The Greedy Connect approach, on the other hand, is more efficient in terms of data storage requirements, whereas the Dominator approach allows for rapid network reconfiguration.