Beyond Beaconing: Emerging Applications and Challenges of BLE

Jian Yang[a,*], Christian Poellabauer[a], Pramita Mitra[b], Cynthia Neubecker[b]

[a] *Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN 46556, USA*
[b] *Research and Advanced Engineering, Ford Motor Company, Dearborn, MI 48121, USA*

Abstract

As an emerging technology with exceptional low energy consumption and low-latency data transmissions, Bluetooth Low Energy (BLE) has gained significant momentum in various application domains, such as Indoor Positioning, Home Automation, and Wireless Personal Area Network (WPAN) communications. With various novel protocol stack features, BLE is finding use on resource-constrained sensor nodes as well as more powerful gateway devices. Particularly proximity detection using BLE beacons has been a popular usage scenario ever since the release of Bluetooth 4.0, primarily due to the beacons' energy efficiency and ease of deployment. However, with the rapid rise of the Internet of Things (IoT), BLE is likely to be a significant component in many other applications with widely varying performance and Quality-of-Service (QoS) requirements and there is a need for a consolidated view of the role that BLE will play in applications beyond beaconing. This paper comprehensively surveys state-of-the-art applications built with BLE, obstacles to adoption of BLE in new application areas, and current solutions from academia and industry that further expand the capabilities of BLE.

Keywords: Bluetooth Low Energy, BLE, Communication, Applications, Low Power, Low Latency.

1. Introduction

Bluetooth Low Energy (BLE), also known as Bluetooth Smart, is an emerging short-range wireless technology aiming at low-power, low-latency, and low-complexity communications. With its deep market penetration (e.g., Bluetooth is available on almost all laptops, tablets, and smartphones), BLE has become an attractive alternative to many existing wireless communications technologies [1]. A new implementation of the Bluetooth protocol stack allows BLE to operate for very long time periods using only a coin-cell battery [2]. BLE also provides new approaches to wireless communications compared to the Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) supported by Classic Bluetooth, as described later in the paper.

One of the most popular BLE applications is its use in *BLE Beacons*, which is a class of devices that continuously broadcast an identifier to nearby BLE receivers [3]. This has enabled a multitude of *proximity detection* solutions, i.e., the beacons allow devices such as smartphones and tablets to perform certain actions when in close proximity to a beacon. Examples of using BLE Beacons include indoor positioning [4, 5], activity recognition [6, 7], and vehicle network wake-up system [8] .

However, in addition to proximity detection, BLE-based systems are also used to connect wireless sensors and receivers in a variety of healthcare and smart home applications. Because of its ubiquitous presence in commercial devices and low-energy requirements, recently a few less traditional domain of applications are investigating the use of BLE, such as Vehicular Ad Hoc Networks (VANETs) [9, 10], smart infrastructure [11, 12, 13], multimedia streaming devices [14, 15, 16], mobile payment systems [17, 18], etc. However, such emerging applications are often unable to utilize BLE without modification or enhancements. Obstacles to the widespread adoption of BLE (besides beaconing) include the lack of support for large and dynamic data transmissions, mesh networking, inter-

[*] Corresponding author

Email addresses: jyang9@nd.edu (Jian Yang), cpoellab@nd.edu (Christian Poellabauer), pmitra3@ford.com (Pramita Mitra), cneubeck@ford.com (Cynthia Neubecker)

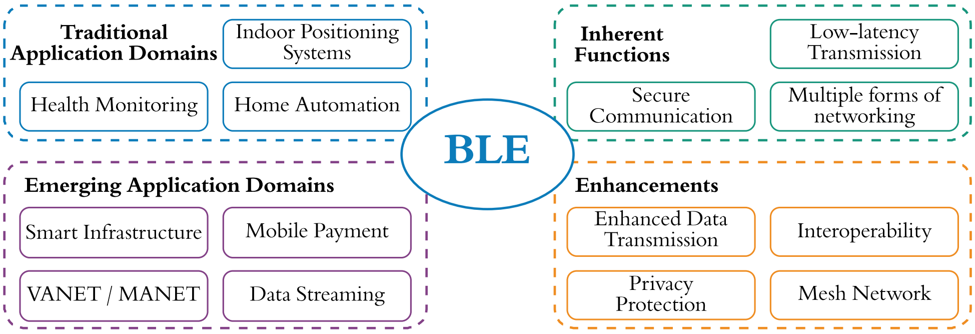

Figure 1: Taxonomy of BLE applications and their challenges and solutions.

operability with other wireless technologies, and security/privacy protection.

While there have been solutions proposed, both in academia and industry, to address these challenges, there are still many remaining opportunities to ensure BLE's success in different domains. This paper provides a comprehensive review of emerging application domains of BLE, the challenges BLE faces in these domains, and solutions that have been proposed. Figure 1 presents a taxonomy of BLE applications and their supporting techniques that will be discussed in this paper. The inherent functions of BLE provide the basis for both *primary* and *emerging* applications, while emerging applications often require enhanced features that have not yet been developed. Therefore, we will first introduce the inherent functionality of BLE, including the *low-latency* capability, *security* consideration for communication, and basic *network topology* that BLE supports. For each of the application domain, we review several typical examples. Then we focus on recent proposed BLE enhancements regarding challenges in the areas of *data transmission*, *mesh networks*, *interoperability*, and *privacy protection*.

The rest of this paper is structured as follows. In Section 2, we introduce the primary functions of BLE and highlight its most important features provided by various protocol revisions. Section 3 summarizes and discusses emerging application domains and their characteristics. Then in Section 4, we present a comprehensive survey of existing modifications and enhancements of BLE for specific application scenarios and discuss open challenges and issues for future BLE applications. Finally, we conclude the paper with a review of our insights in Section 5.

2. BLE: Current Functions and Revisions

BLE was first introduced in 2010 by the Bluetooth Special Interest Group (SIG) as part of the Bluetooth 4.0 specification [19], which defined the overall architecture and implementation details of BLE. Since then, there have been several revisions of the Bluetooth core specification: Bluetooth 4.1 [20], Bluetooth 4.2 [21], Bluetooth 5.0 [22], and Bluetooth 5.1 [23]. Major improvements by these revisions address power management, throughput, communication range, latency, and security issues with BLE. This section describes the primary architecture, current functions, and major evolution of BLE.

2.1. BLE Stack

The protocol stack of BLE maintains a similar lower layer structure as Classic Bluetooth, but also provides revised implementations and a few new layers, such as the *General Attribute Profile (GATT)* and the *Attribute Protocol (ATT)*. Figure 2 shows the simplified stack for three major types of Bluetooth chipsets: Classic Bluetooth, Dual Mode, and BLE-only. For compatibility reasons, the *Bluetooth Dual Mode* chipsets were introduced to support both Low Energy and BR/EDR communications, which are commonly seen on phones and tablets. BLE-only chipsets are typically installed on cost- and resource-constrained devices.

The implementation of the BLE stack layers focuses on low-latency and low energy consumption. Several highlights of the stack layers can be summarized as follows. First, the *Physical (PHY) Layer* of BLE defines 40 Radio Frequency (RF) channels in the 2.4 GHz band, among which three channels

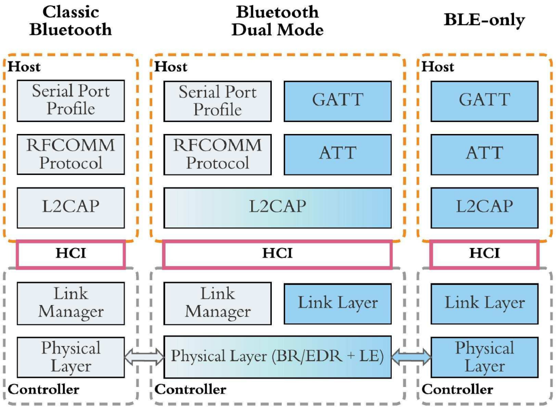

Figure 2: A simplified protocol stack for three types of Bluetooth chipsets (adapted from [24]).

are defined as advertising channels for disseminating data and 37 data channels are used for bidirectional exchange of messages in established connections. The *Link Layer (LL)* defines two interaction patterns between two devices: 1) *connectionless* communication, i.e., two devices act as *advertiser* and *scanner*, where the advertiser broadcasts data packets and the scanner can receive them; 2) *connection-based* communication, i.e., the scanner and the advertiser are able to establish a bidirectional connection and adopt the role of *central* and *peripheral*, respectively. The Host Controller Interface (HCI) is a standard protocol that takes care of the communication between the *Host* and *Controller*.

On top of the HCI sits the *Logical Link Control and Adaptation Protocol (L2CAP)*, which is a protocol in common with Classic Bluetooth. It handles the data from lower layers and encapsulates them into the standard BLE packet format for upper layers' use and vice versa. The serial port protocols (*Serial Port Profile* and *RF Communication Protocol*) in Classic Bluetooth are replaced by two novel layers in BLE stack: the *ATT* and *GATT*. These two layers handle the data interaction between application and stack layers when connection-based BLE communications are used (Section 2.2.1). Furthermore, the *Generic Access Profile (GAP)* and *Security Manager Protocol (SMP)* (not shown) handle the general link management and security functions in BLE communications.

2.2. Built-in Functions

BLE was originally designed for applications in the rising IoT industry where Classic Bluetooth may be found less efficient. The new implementation of the BLE stack protocol inherently provides novel features with respect to data transmission, networking, and security. In this subsection, we discuss these built-in features of BLE and how they can be used to support various application domains.

2.2.1. Data Transmission

The Link Layer defines one packet format (Figure 3) used for both advertising packets (also known as *advertisements*) and data channel packets, which support connectionless and connection-based communication, respectively. These two types of communication dispense with the slow and low-responsive pairing mechanism used in Classic Bluetooth, which makes the protocol more attractive to several novel application domains.

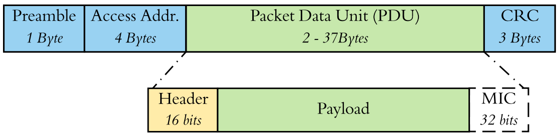

Figure 3: The data packet format.

The *Preamble*, *Access Address*, and *Cyclic Redundancy Check (CRC)* fields are defined for easy control by the Link Layer, with regard to different communication scenarios. Data is transmitted via the *Packet Data Unit (PDU)* payload, with the *Header* identifying its type and size.

In connectionless communications, data is broadcast directly via advertisement payloads and all neighbors (i.e., nodes in wireless range) can receive it. Since the payload is limited to a certain size (31 bytes in Bluetooth 4.1), a single advertisement can transmit only very short messages. Splitting and reassembling data for multiple advertisements can help with large data transmissions, but there will be a trade-off between data volume, transmission overhead, and packet loss. Therefore, connectionless communication is typically used for BLE beaconing, where beacons operate as advertisers and continuously broadcast a specific packet containing information for various purposes. The advertising process consumes very little energy and the theoretical life of a BLE beacon powered by a coin cell battery can be up to 14 years [25].

An advertiser is able to announce its availability for connections by setting the PDU header in outgoing advertisements accordingly, so that the receiving scanner can initiate a connection request. A connection will be established once the advertiser receives and accepts the connection request, and then the advertiser becomes a peripheral and the scanner becomes a central. The data exchange will then be processed based on the GATT rules via one of the 37 data channels.

Connection-based communication uses the same packet format, with the *Message Integrity Check (MIC)* field used for encrypted transmission checks. The *adaptive frequency hopping mechanism* is applied to data channels, with the purpose of minimizing channel interference and maintaining a low loss rate. The GATT further defines the rules of exchanging data. The peripheral acts as a *GATT server* that stores data in the form of a set of services. Each service contains a number of characteristics that take the length of a single PDU. The connected central device, known as *GATT client*, is able to discover, read, and write to the services and characteristics according to their permissions. As an example, if we have a heart rate monitor acting as a peripheral, its GATT server will contain a *Heart Rate Sensor* service with a *Heart Rate* characteristic. This characteristic will include the sensor data and the access permissions (e.g., [60bpm, Read Only]).

2.2.2. Networking

The central-peripheral relationship of connection-based BLE communications is similar to the master-slave relationship in BR/EDR communications, where a central device is allowed to connect to multiple peripherals. Therefore, this communication mode supports the most basic network topology, a *piconet* that is composed of one central and multiple peripherals. Unlike BR/EDR slaves, BLE peripherals do not share a common physical channel with the central, i.e., each peripheral communicates on a separate physical channel with the central. Since Bluetooth 4.1, each device has the capability to operate simultaneously in both roles in different piconets, thus providing opportunities to form larger *scatternets*.

Furthermore, the connectionless communication operates on different physical channels (three advertising channels), and can coexist with connection-based communications (on data channels). On one hand, advertisers and scanners can form a broadcast network on advertising channels; on the other hand, the central or peripheral in an existing piconet or scatternet are also able to advertise and scan, resulting in a scatternet that involves both advertising and data channels. There could be multiple combinations of such scatternets.

A more complex network topology, which offers path diversity that can cope with radio propagation impairments and node failures, is the mesh network. This type of network has been introduced in BLE specifications starting from version 4.2, where a node can act as central and peripheral simultaneously. In late 2017, the Bluetooth SIG released a set of specifications and profiles that define BLE mesh networking on top of current BLE stacks [26]. However, no implementations or tests of mesh networks have yet been provided by the group. Related problems, such as dynamic address allocation, network topology mapping, and routing, also require further exploration.

2.2.3. Security

In general, Bluetooth has potential vulnerabilities that fall into three categories: 1) passive eavesdropping, 2) man in the middle (MITM) attacks, and 3) identity tracking.

Passive eavesdropping is the process where a third device listens to the data being exchanged between two connected devices. BLE addresses this by encrypting the data being transferred using AES-CCM encryption at the Link Layer. The AES-CCM encryption is considered secure as long as the key is unpredictable.

MITM attacks occur when a malicious device impersonates two other legitimate devices, in order to fool these devices into connecting to it. In this scenario, both the central and peripheral will connect to the malicious device, which in turn routes the traffic between the two other devices. This gives the legitimate devices the illusion that they are directly connected to each other when in fact their connection has been compromised. This setup not only allows the malicious device to intercept all the data being sent, but also allows it to inject false data into the communication or remove data before it reaches its intended recipient. LE Secure connections were introduced in version 4.2 to address this problem, where three steps are required before exchanging data: 1) a pairing feature exchange, 2) key generation via Elliptic Curve Diffie Hellman (ECDH) encryption, and 3) authentication.

Finally, identity tracking is where a malicious entity is able to associate the address of a BLE device with a specific user and then physically track that user based upon the presence of the BLE device. BLE addresses this by periodically changing the device address to make it untraceable.

2.3. BLE Versions

Since the release of version 4.0, several revisions of the Bluetooth specification have been published, with enhancements in data rate, payload, power consumption, and security. Table 1 summarizes the major differences between these versions.

Table 1: Comparison of Bluetooth versions.

Version	**4.0**	**4.1**	**4.2**	**5.0 & 5.1**
Multi-Roles	No	Yes		
PDU Payload	Up to 31 bytes		Up to 255 bytes	
LE Secure	No		Yes	
IoT Support	Limited		Medium	High
Advertising Channels	3 Channels			3 Primary Ch. 37 Secondary Ch.
Data Rate	1 Mbps			2 Mbps
Effective Range	50 m (Line of Sight) 10 m (Indoor)			200 m (Line of Sight) 40 m (Indoor)
Battery Life	Shorter			Longer

Bluetooth 4.0 explicitly prohibits a peripheral to participate in multiple connections (or assume multiple roles) simultaneously with other central devices. Version 4.1 and later incorporate a fundamental change with regard to the roles each device can play when multiple connections are present. That is, a device, regardless of its Link Layer role, can run multiple Link Layer instances simultaneously without limitation. Therefore, a peripheral is allowed to be simultaneously connected to more than one central device.

Version 4.2 introduces major enhancements where the maximum PDU payload can be up to 255 bytes, compared to only 31 bytes in previous versions. This version also provides additional support for IoT capabilities, such as low-power IP [27] and Internet gateways [28]. In terms of security, the *LE Secure Connections* were introduced in this version, which utilize the ECDH algorithm for key generation, in order to protect against MITM attacks.

Bluetooth 5.0 is regarded as a significant leap forward compared to previous versions, with claims such as “twice the speed” and “four times the range” [22]. This version also defines two types of advertising channels: *primary* and *secondary*. The primary advertising channels are the same three advertising channels available in previous versions, while the secondary advertising channels use the remaining 37 BLE channels (formerly defined solely as data channels). The secondary advertising channels can exploit frequency hopping, just like data channels. The recently released Bluetooth version 5.1 provides further improvements in connection latency and location services to better support indoor localization services. Both versions 5.0 and 5.1 were designed for IoT applications, e.g., by using more advanced power management designs to maximize the life time of battery-powered devices.

3. Application Domains

BLE’s low-energy performance and widespread deployment in mobile devices makes it an excellent candidate for a variety of applications, including many emerging application domains. Traditional application scenarios can take advantage of all inherent BLE functionality immediately and include examples found in Indoor Positioning Systems (IPS), health monitoring, and home automation. In contrast, many emerging applications cannot readily use BLE and thereby may require further modifications or enhancements, including applications in smart infrastructure, vehicular networks, mobile payments and data streaming. In this section, we briefly summarize the traditional application domains of BLE, and review some attempts of using BLE in emerging domains.

3.1. Traditional Application Domains

BLE was designed specifically for static applications with low-energy requirements. In order to support quick and simple development, each BLE chipset comes with a built-in list of uniform type identifiers, which cover some basic services or data types for IPS, health monitoring, and home automation. These are the three main application domains where BLE has increasingly been deployed and evaluated. Table 2 summarizes the built-in BLE features used in these domains.

IPS are systems that can determine the position of an object or a person in a limited physical space [40]. A simplified structure of an IPS is based on the periodical execution of two steps: 1) sensors or receivers receive signals from transmitting devices and 2) distributed devices or a central unit

Table 2: Summary of Traditional BLE Application Domains.

App Domain	BLE Built-in Features	Range of Interest	Examples
IPS	connectionless communication, low energy	$< 30m$ (workspace)	[5, 29, 30, 31, 32]
Health Monitoring	GATT profile, piconet networking, privacy protection	$< 1.5m$ (body area)	[33, 34, 35, 36]
Home Automation	GATT profile, piconet networking, privacy protection	$< 15m$ (living area)	[37, 2, 38, 39]

estimate parameters to calculate the approximate position of the object [41]. The Received Signal Strength Indicator (RSSI) is usually collected for distance estimation. The RSSI values can be part of the metadata transmitted with BLE advertisements, thus supporting the positioning system in a simple manner. Such applications only rely on connectionless BLE communications and therefore consume very limited energy. Typically, a set of BLE Beacons deployed in a workspace can support positioning services for several years without the need to change battery.

The advent of BLE has also attracted considerable interest in the development of personal or human-centric networks. The continuous transmission of body sensor readings usually requires low latency and low power. Figure 4 shows the general structure of a wireless health monitoring system, where BLE can easily connect a set of body sensors to the smartphone by forming a piconet. For easier development, the GATT profile provides a list of identifiers specifically for health service data, such as *blood pressure*, *glucose*, *heart rate*, and *pulse oximeter*. For the health monitoring applications that are primarily interested in body area ($< 1.5m$) communications, the inherent BLE features satisfy most of the technical requirements with regard to latency, energy consumption, and privacy protection.

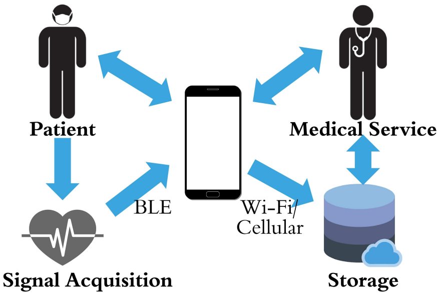

Figure 4: Wireless health monitoring system structure [42].

As a sub-domain of IoT, home automation is one of the major drivers for the design of BLE. Applications in this domain are usually deployed in a limited area ($< 15m$) with more frequent interactions between sensors, actuators, and gateways. BLE also defines a set of GATT services related to home monitoring data, providing simple and direct data extraction for common data types. By virtue of its low-power consumption, BLE has been implemented by many sensors and actuators [37], replacing other wireless technologies, such as Wi-Fi or ZigBee. Some architectures [2, 38, 39] also apply BLE as a key part of the gateway in smart homes, where BLE will play a central role in coordinating operation of sensors and actuators.

3.2. Emerging Application Domains

Apart from the above applications that can be directly supported by BLE, there are numerous other applications that can benefit from BLE-based communications. Most applications in these domains are currently supported by other wireless technologies, but BLE can provide complementary features to, or expand functionality of systems using hybrid networking technologies.

3.2.1. Smart Infrastructure

Smart infrastructure is the cornerstone for future smart city development. It intelligently connects energy systems, buildings, and industries to adapt and evolve the way we live and work. We have reached a state of “infrastructure maturity”, especially in developed economies, where the value of new infrastructure is far outweighed by the value of existing infrastructure [43]. Applying digital technologies to existing infrastructures offers the potential to use our assets more intelligently, and better meeting social needs. Wi-Fi and cellular solutions have provided stable and robust services in this field, but when it comes to local services, BLE can make it much easier for people to actively interact with buildings and other infrastructure in their surroundings. Such BLE-based services are more responsive, even without Internet connectivity. Examples include: 1) identifying certain groups of people in public areas [11], 2) logging and managing the usage and service status of power grids [44], and 3) monitoring extreme weather conditions for farming automation [12].

Take smart buildings as an example; here, a proof-of-concept work called NomaBlue [45] uses buildings as databases for spatial exploration in smart city scenarios. This system utilizes both beacons and regular BLE transmitters for data dissemination and device detection. Buildings equipped with BLE beacons and servers act as the knowledge base that stores spatial knowledge from users. Users with BLE transmitters can share spatial knowledge with other users or buildings when in their proximity. Spatial knowledge is then shared and propagated via numerous meet-ups, allowing the system to provide on-demand knowledge requests for local users. The system has been tested and evaluated without Internet connection, and has been proven effective. Google's Sidewalk Lab has also implemented similar ideas in the city of Toronto [46]. The city-wide deployment of BLE transmitters allow citizens to be aware of people and events in the neighborhood, thus providing opportunities for more social connections.

Using BLE in smart infrastructures can complement other wireless technologies by providing easy and low-cost data transmission in localized areas, even without Internet connection. In case of emergency, for example, BLE may offer an alternative low energy consumption solution monitor peoples location inside buildings and guide evacuations, as everyone will be trying to save battery on their devices and will theoretically have no communication. We therefore see the potential of BLE to be used widely in future infrastructures to build a dynamic and low-cost connected ecosystem.

3.2.2. Vehicular Ad Hoc Networks (VANETs)

VANETs are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. In a VANET, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication have attracted a lot of interest in the research community. In 2014, Frank et al. [47] first proposed to use BLE as an alternative technology for V2V communications. The idea was to utilize connection-based BLE communications, where each vehicle is initially assigned a role of either central (C) or peripheral (P) and exchanges data with neighbors via C-P connections. For the same role communication (i.e., C-C or P-P), one of the vehicle will alter its role to set up the connection. This idea has been implemented with a prototype [9] using BLE-equipped phones, and tested for single-hop and multi-hop communications.

Yang et al. [10, 48] further proved and validated a feasible approach (called BlueNet) for a dynamic and self-organized vehicular network. Their method encapsulated metadata into BLE advertisements so that each node in the network can decide whether to initiate a connection based on the received metadata. BlueNet also applied a dynamic role switching mechanism to provide each node with a higher chance of being connected into the network. Their work also discusses the potential of transferring BlueNet to V2I communications.

The wide deployment of Bluetooth chips in vehicles would greatly lower the cost of large-scale deployment of V2V and V2I systems based on BLE, when compared to technologies such as Dedicated Wireless Short-Range Communication (DSRC). Therefore, BLE will be more prominent in resource-constraint situations, such as Vehicle-to-Pedestrian (V2P) and Vehicle-to-Drones (V2D) communications. Some preliminary models [49, 50] have been developed recently for pedestrian protection using connectionless BLE communication. In these models, the GPS, speed, and direction of pedestrian and vehicles will be broadcast via BLE advertisement, and algorithms are developed based on the received data to predict collision risk. Based on these promising efforts and results in VANETs, BLE can now also be a candidate for communication between other devices such as drones [51, 52] and robots [53], e.g., in the context of Mobile Ad Hoc Network (MANET) applications.

BLE may not be able to outperform other wireless technologies due to its limited communications range and lack of diversity in supported types of network topology, but it can serve as a decent complementary technology in a system that utilizes a hybrid networking approach. Table 3 shows a comparison between several existing wireless technologies in VANETs. Though facing challenges in communication range and data rate, the newly released BLE mesh specification [26] still makes BLE competitive with respect to low cost and easy deployment when compared to Wi-Fi and DSRC.

3.2.3. Mobile Payments

Current mainstream mobile payment methods (i.e., Near Field Communications (NFC), chip cards, carrier billing, etc.) are typically limited to contact-based or very short range contact-less authentication, while BLE can provide more flexible payment experiences for consumers. For instance,

Table 3: A Comparison of VANET Technologies [47].

	BLE	Wi-Fi	DSRC
Bandwidth (MHz)	2	20/40	10
Num. of Ch.	40	11	7
Data rate (Mb/s)	1	600	27
Max Power (mW)	10	100	2000
Range (m)	50	100	1000
Latency (ms)	6	50	1

using BLE beacons it is possible to determine the customer's location in a store. From the seller's perspective, it is useful to be aware of a customer's activity - entering the store or checking out. Based on current BLE functions, three different payment scenarios can be presented, of which the second scenario is based on an actual implementation by PayPal:

- Replacing NFC with BLE - pay at cashier with agreement on handset.
- PayPal Beacon Hands Free [17] - pay at cashier with verbal confirmation.
- "Take and Shake" - scan and pay on your own, no cashier needed.

Unlike the simple scheme of establishing a BLE connection, BLE-based mobile payment requires a more secure process of authentication, which applies to most BLE payment scenarios. Take the approach in [18] as an example, where the payment process usually consists of the following steps: 1) the merchant terminal receives BLE identifiers from the product and the customer, then transmits merchant information related to the product back to the customer device; 2) the customer device sends a request for making a payment; 3) the merchant terminal initiates a transaction based on the product and customer information; 4) the customer device receives and sends back a confirmation to authorize the transaction and the amount; 5) the merchant terminal replies with the confirmation once the transaction is completed. Certain systems may also include two factor authentication approaches to secure the process. The recently opened Amazon Go store is believed to incorporate BLE as part of the solution for automatic checkout [54].

As BLE has already been applied in VANET applications, it may also be adapted for scenarios where vehicles can be utilized for mobile payments (e.g., parking fees, fueling, tolls, etc.). The VANET application layer exchanges the vehicle's information with pay station, and then the quick transaction can be processed by a secure BLE transaction layer. While some attempts of using DSRC in such systems have been shown successful [55], it would be possible to build such solutions also with BLE.

3.2.4. Multimedia Streaming

There is also an increasing interest in BLE in applications that require larger data exchange. The data payload limit of BLE in connectionless mode is 31 bytes in version 4.1 and 255 bytes in version 4.2 and after. Although the connection-based mode does not have such a limit on data packets, large amounts of data may still need to fit into the GATT service and characteristics format. For certain applications, such as multimedia streaming, the ability to efficiently stream large amounts of data is an important criterion.

Giovanelli et al. [14] proposed a data streaming design that adds a service composed of two specific characteristics, one for regular data exchanges and the other is used to control the data stream from the central side, enabling it when set to 1 and disabling it when set to 0. In this case, the central device will only need to check the payload from second characteristic to decide whether or not to receive the next regular incoming data packet, thus narrowing the gap between each packet transmission.

The size limit of data frames at the Link Layer was also tested and explored in [15], where it was shown that with proprietary modifications at upper layers, BLE throughput can go as high as 300 kb/s, which is sufficient for most speech and music transmissions. In another study [16], the potential for BLE beacons to transmit complex data, e.g., images, was demonstrated. The proposed method segments an image into multiple smaller units for beaconing, while utilizing a retrieval algorithm on the receiver end to rebuild the images.

In most data streaming use cases, BLE is inferior to other wireless technologies, such as Classic Bluetooth, Wi-Fi and cellular radios, primarily in terms of achievable data rate. However, it still shows great potential as a back-up method, especially for resource-constraint scenarios, such as emergency communication in a natural disaster.

4. Solutions and Challenges

The examples discussed so far strongly benefit from various BLE features, but also present challenges and additional requirements that need to be addressed for the successful adoption of BLE in emerging application domains. Based on our review of various examples from emerging application domains, we further categorize four major and urgent challenges or additional requirements for BLE: 1) the need of *enhanced data transmission*, 2) *mesh metworking* support, 3) *inter-operability* with other wireless technologies, and 4) more reliable *privacy and security* protection.

The spider web map in Figure 5 demonstrates the significance of these challenges for each of the emerging application domains we reviewed in Section 3. Smart infrastructure applications usually require interactions and cooperation with other wireless devices, and also need some protection for the transmission of sensitive data. VANET applications, in contrast, exhibit a strong need for mesh networking capabilities, e.g., to connect as many vehicles as possible and to exchange information between these vehicles in a timely fashion. An enhanced data transmission mechanism is expected to further accommodate the rapidly growing vehicular networks, while also improving their throughput. For mobile payments, a main challenge for BLE is privacy protection, where the simplicity of the BLE design can lead to a vulnerability to attacks. Multimedia streaming applications require higher data rates and lower latencues for BLE, while also having a need for inter-operability for use cases where BLE works as an auxiliary approach for other technologies.

While some of these challenges have been addressed by prior work, not all have yet received attention or have been fully resolved, indicating the necessity of further research into these areas. In this section, we summarize and analyze some solution approaches to the challenges mentioned above.

4.1. Enhanced Data Transmission

The two types of BLE communications between two devices (i.e., connection-based and connectionless) have enabled simple and quick data exchange for many novel designs and applications. However, there are still some challenges found in application domains such as IPS and VANETs, where BLE encounters several limitations in device discovery and role assignment. We list and analyze several typical solutions below.

4.1.1. Efficient Device Discovery

In most prior studies, it is assumed that the advertisements are processed immediately as long as they are received by a scanner, which means there is no collision when discovering BLE devices. However, in practice, there exist contentions among multiple BLE devices during the device discovery process, especially in a crowded environment. With an increasing number of BLE devices, discovery latency and energy consumption will rise exponentially [56], which will degrade the achievable performance and QoS of many applications. Solutions for low-latency device discovery fall into two categories: 1) *Adaptive Parameter Settings* and 2) *Channel Sensing*, which are further explained below.

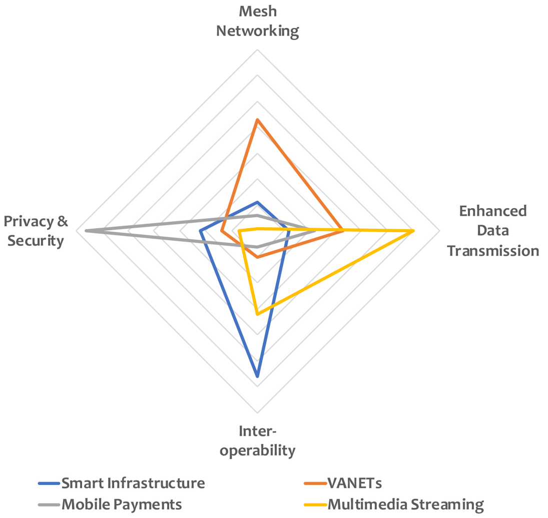

Figure 5: Critical Challenges for Emerging BLE Application Domains.

Adaptive Parameter Settings: There are four major timing parameters that may affect the performance of BLE device discovery:

- *AdvInterval*: total time of an advertising event on three advertising channels;
- *AdvTimePerChannel*: advertising period per channel;
- *ScanWindow*: time length of a scan event;
- *ScanInterval*: delay between two consecutive scans.

Although the BLE standard has enabled the ability for BLE devices to operate with a wide range of these parameters, it is somehow hard for them to fine tune these parameters automatically, as neither the scanner nor the advertiser can be aware of the existence of contentions on advertising channels. The adaptive parameter setting method adjusts some of these parameters based on certain observations to achieve a more efficient device discovery. The authors in [57] presented a model that utilizes the advertisement payload to reflect contention situations. The main idea can be summarized as: 1) advertisers piggyback connection reports (containing *AdvInterval* and the current count of advertising intervals) in the advertisement payload; 2) scanners use the reports to evaluate the current contention situation and adjust certain parameters (*ScanWindow* and *ScanInterval*) accordingly. However in practical use, especially when the parameters are changing fast, the advertiser needs to frequently update the payload, which may lead to high system overhead.

Park et al. [58] provided a parameter adjustment scheme based on the discovery time ratio ρ $(= T_{actual}/T_{reference})$. The reference discovery time is defined according to empirical settings. Advertisers and scanners will then adjust *AdvInterval* and *ScanWindow*, respectively, depending on ρ. This approach allows advertisers to actively join the parameter adjustment, which makes it easier to be applied to general use cases.

Channel Sensing: The latency in the BLE device discovery is partly caused by the unawareness of channel traffic. Therefore, the main idea of the Channel Sensing method is to sense the channel traffic before advertising or scanning. When the channel is busy, an advertiser will execute a deferral and random backoff and retry the sensing until the channel is idle [59]. A similar scheme can also be applied to scanners so that they can decide whether to initiate a connection to neighbors based on channel traffic [60]. The channel traffic can be evaluated by the density of the received packets, but may experience heavy fluctuations in highly dynamic networks. While promising, this method still requires a better definition of the channel traffic and the decision-making algorithm for each role.

The two types of methods mentioned above have shown the effectiveness in reducing latency caused by collisions in certain cases. However, the common problem with these solutions is the lack of tests and validation on physical BLE devices. Device discovery is primarily conducted in the physical layer and link layer, which means that the enhancements will need to manipulate the BLE stack and must be useful for various common applications. Further, the schemes described above are mainly designed and tested for dense networks and the trade-offs when applied to sparse networks have not been investigated.

4.1.2. Role Assignments

In many applications, independent devices will be expected to find ways to coordinate, access each others sensor data, share communication channels, or process and fuse data from multiple sources. Self-organization and self-management of these devices, e.g., the ability to decide when to establish or tear down a connection, is one of the defining characteristics of IoT and VANETs. However, BLE was built for deployment scenarios that have well-defined roles for the connected devices, e.g., it is defined that only a central device can initiate a connection to peripherals. This design may limit the self-management of BLE device and the efficiency of data propagation. Existing solutions to this limitation focus on providing alternatives for the role assignment in BLE connections.

Bronzi et al. [9] proposed an event-based role switching scheme to switch the role of central and peripheral that a BLE device can play, so that each device can be in the accessible role when there is a need to transfer data. The scheme is designed in the context of multi-hop V2V communications, where every node (vehicle) is initially set as a central and will activate its peripheral role manually on the device itself or upon receiving a message to rebroadcast. In a multi-hop scenario, the relay node will stay active as both central and peripheral roles for a certain period of time to ensure the data integrity, and will resume the initial role once the data transmission is finished. However, the transmission latency may increase aggressively as the network size and the amount of data grows.

Following a similar idea of role switching, Yang et al. [10, 48] further developed a more self-organized mode of role switching, which is called *Dynamic C/P Switching*. This approach addresses the problem by allowing BLE devices to continually and frequently switch their roles. In general, if the roles are switched at random times, two devices will eventually have different roles, allowing them to establish a connection and communicate. In this mode, a device may be initially be set as either central or peripheral and after a random period of time, its role will be switched to the other. The *active time* for each role is randomly chosen, possibly from a range of minimum and maximum active times. At any given time, devices with the same role are not able to make a connection and a connection can only be established if one device is central, while the other is peripheral. Once a connection has been established, the role switching process can be paused to allow the newly connected devices to exchange their data. When the data transfer has finished, the connection will be torn down and the switching approach will resume. This method allows equal opportunities for each device to play as central or peripheral, but the frequent role switching may also bring high overhead and low energy-efficiency.

Similar ideas were also applied to the data flow between parent nodes and child nodes in a BLE-based tree networks [61]. However, these role switching schemes face some common challenges: 1) how to provide an efficient parameter settings (e.g., the time interval for each role) according to different network contexts; 2) how to minimize the overhead caused by role switching, particularly in dense networks; and 3) how to ensure the consistency of data transmissions.

4.2. Mesh Networking

The limited range of BLE is one of its major drawbacks, especially for use cases in health monitoring, IoT, and VANETs. BLE was originally designed based on the star network topology. However, other wireless technologies, such as ZigBee and Z-Wave, support mesh networks, which provides them with an advantage in these domains [62]. Therefore, to further extend the network coverage of BLE, solutions have been proposed, both by the community and the Bluetooth SIG.

In mid-2017, the Bluetooth SIG released a set of specifications defining the architecture of the BLE mesh topology [26]. These specifications outline the implementations and requirements to enable an interoperable many-to-many mesh networking solution on top of Bluetooth 5.0 and later. Apart from the official support for mesh networking, many solutions from academia have also been proposed based on Bluetooth 4.0 through 4.2 to fit into multiple application domains. Based on the type of routing protocol, these solutions can be categorized into three classes: 1) *Flooding routing*, 2) *Table-driven routing* and 3) *On-demand routing.* While all of them resolve the routing problems in BLE mesh networks, the target application domains may vary. Smart infrastructure applications are usually deployed in a static environment, where flooding and table-driven routing may exhibit high performance. Similarly, built on a pre-defined and well connected network, health monitoring applications can easily benefit from table-driven routing methods. However in VANETs use cases, the network is usually of high mobility and flexibility, where flooding and table-driven routing are less efficient but on-demand routing can provide more dynamic routes.

We review and analyze typical solutions from each category. The main objectives and approaches for each of the solutions are explained below.

4.2.1. Flooding Routing

This type of routing protocols are based on connectionless broadcast, where every node that receives a broadcast will rebroadcast until the message has been received by the destination node. *BLESSED* [63] is an example that utilizes the BLE advertisement for flooding packets. It defines three superstates for each participating node, so that every node will be able to broadcast, receive, and update identifiers of advertisements. However, the BLESSED method needs to be implemented and tested with the assistance of Wi-Fi hotspots.

BLEmesh [64], proposed in the same year, is a pure BLE-based mesh solution. In BLEmesh, packets carrying data from a specific source-destination couple are aggregated in batches. Data, together with control fields, which are used to decide which nodes will participate as broadcasters, are carried in the advertisements. The control fields include two lists: 1) *Forwarder List* and 2) *Batch Map*, which are used to keep track of a prioritized set of intermediate nodes and the last nodes that have broadcast data to a corresponding batch, respectively. These control fields are designed to minimize the overhead caused by unnecessary rebroadcast. The authors compared their protocol with a conventional flooding protocol and show that BLEmesh requires fewer transmissions.

4.2.2. Table-driven Routing

Table-driven routing is a typical type of routing in MANETs. In such protocols, each node maintains one or more tables containing routing information to every other node in the network. *MHTS* [65] is known as the first attempt to construct a multi-hop BLE network. This approach is based on BLE GATT profiles, which stores the routing entries (including data, source address, and destination addresses). The route discovery is carried out by broadcasting the *Seek Table* in advertisements and constructing a *Route Table* for each receiving node. Then connections will be established based on the

Route Table. Since Bluetooth 4.0 does not allow scatternet formations, current connections must be torn down before the intermediate node transfers data to the next hop. MHTS can transfer packets over up to five hops for a file size of 1 kB.

BMN [66] was later proposed as an improved table-driven routing protocol. BMN uses Directed Acyclic Graph (DAG) as the basis for routing. The network formation starts with BLE advertisements of DAG information and an arbitrarily selected root node. Then a DAG will be formed by a series of connection establishments, and each connected node will maintain a table that stores its parent, alternative parent, and its children. The data forwarding will then retrieve its referenced path from the table maintained by each node. However, this approach may suffer from intermediate node failure and network congestion.

NDN-BLE [67] is a variation of table-driven routing protocol, which uses the Named Data Network (NDN) to build BLE mesh networks. NDN names every chunk of data with an appropriate Uniform Resource Identifier (URI), and operates over a distributed database, which determines how an endpoint can retrieve data of interest. A Mediation Service is introduced to manage and aggregate distributed databases, so that multi-hop transmissions are actually conducted via these mediators. While this approach has been verified from various angles, the authors did not provide any physical or simulation tests to evaluate its performance.

4.2.3. On-demand Routing

On-demand routing is another type of routing protocols in MANETs. In contrast to table-driven routing protocols, routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send data to a destination, it invokes the route discovery mechanisms to find a path to the destination. The route remains valid until the destination is not reachable anymore or until the route is no longer needed. Guo et al. [68] present a typical example of this type of routing based on BLE. In their method, the route discovery is conducted based on scatternets: a source node first sends a route request to its master. If the destination node is not in the slaves list, then the master starts a Breadth-First Search by forwarding the request to its slaves that are also in other piconets. Such slaves will continue the same procedure until the destination node is found. The source node will exploit the shortest path once all possible routes are obtained. This approach may waste network resources as only one route is used and no other nodes benefit from it.

Therefore, *CORP* [69] was proposed to provide a more effective routing procedure. The scatternet formation in CORP is based on a device's degree (i.e., $\#neighbors$) so that the each piconet will be connected with the smallest number of connections. The routing protocol is executed similar to the previous method, but due to the simplification of scatternets, the route discovery is now more efficient. The authors also design a mechanism to locally reconstruct the scatternets when encountering a single-node failure.

RT-BLE [70] and *MRT-BLE* [71] stabilize the routing by putting limitations on each node: 1) a node can establish a connection with up to two masters and 2) a master can establish a connection with at most one other master, and, in this connection, the former shall play the slave role. In the route discovery process, these two models use the Client Characteristic Configuration Descriptor (CCCD), a descriptor available in the GATT layer, to maintain connections. CCCD only allows one connection to be active at a time, while the rest are kept inactive. Such models show improvements in power consumption, while achieving the goal of multi-hop transmissions. Other variations (e.g., Dual-Ring Tree [72]) follow similar approaches to on-demand routing, but use tree topologies to construct the network, which have also been proven useful in some cases.

4.2.4. Comparison

Table 4 summarizes the typical solutions for each of the afore mentioned routing classes and also lists several key characteristics for each solution. Since each work uses different metrics and different hardware/chipsets for evaluating the performance, the comparison may vary depending on the actual test environment. Generally, the Latency in Table 4 refers to the general latency for multi-hop transmissions, while the Dissemination Efficiency reflects the average packet delivery ratio in a mesh network. These key characteristics are generally acknowledged factors that need to be considered when designing a network-based application. There is no solution that fits into all design criteria, but we can see from the table that the BLESSED in flooding routing, BMN in table-driven routing and CORP in on-demand routing stand out for delivering on most

Table 4: A comparison of BLE mesh network solutions.

Routing Type	MajorApplication Domains	Solution Name	Year	Bluetooth Version	Key Characteristics				
					Latency	Energy Efficiency	Dissemination Efficiency	Mobility	Scalability
Flooding	Smart Infrastructure,	BLEmesh [64]	2015	4.2		✓	✓		
		BLESSED [63]	2015	4.2		✓	✓	✓	✓
Table-driven	Smart Infrastructure, Health Monitoring	MHTS [65]	2013	4.0	✓				
		NDN-BLE [67]	2015	4.1			✓		
		BMN [66]	2015	4.1	✓	✓	✓	✗	
On-demand	VANETs	N/A [68]	2015	4.1	✓			✗	
		CORP [69]	2017	4.1	✓	✓	✓	✓	✓
		RT-BLE [70]	2016	4.1	✓			✗	✗
		Dual-Ring Tree [72]	2018	N/A			✓	✓	✓
		MRT-BLE [71]	2018	4.1	✓		✓		

✓: theoretically or experimentally proved to be good; ✗: weakness or proved to be below average; blank: not considered or explained explicitly.

of the criteria. We suggest developers should refer to the best fit based on their actual goal/needs.

In summary, BLE mesh networking is an emerging area with the potential to expand the BLE applicability space. The above solutions can address various application scenarios, but many of them still suffer from trade-offs between latency, network traffic, and power consumption when applied to general cases and, therefore, this area requires further exploration.

4.3. Inter-operability

Although cheap and convenient, BLE cannot yet fully replace other existing wireless technologies. In practical uses, it will be more common to see BLE co-exist or even integrate with technologies that share the 2.4 GHz frequency band. This brings up the problem of inter-operability, i.e., approaches to co-existence and integration with other technologies that minimize inter-technology interference. Next, we discuss such challenges in terms of co-existence and integration.

4.3.1. Co-existence

BLE shares a similar frequency band with Wi-Fi, ZigBee, and many other wireless technologies. Silva et al. [73] have performed comprehensive tests on co-existence and interference among BLE, Classic Bluetooth, Wi-Fi, and ZigBee in a full anechoic chamber. RSSI and Bit Error Rate are measured as the main criteria for the level of interference. The results show no obvious interference between BLE and Wi-Fi, but Classic Bluetooth and ZigBee do collide occasionally with BLE, as shown by the increased RSSI and Bit Error Rate. Kalaa et al. [74] presented a general evaluation of BLE in realistic wireless environments such as a sports facility, a university's food court, and a hospital's Intensive Care Unit (ICU). Their results revealed that the probability of failed BLE connections and transmissions increases sharply when the wireless environment become extremely complex and dense. The PHY layer of BLE stack utilizes an adaptive channel hopping scheme to avoid interference, and it has been shown effective in most cases. However, the evaluation results above also point out that there is a need for additional research to develop enhanced schemes for more critical and complex scenarios.

4.3.2. Integration

We expect that, due to its limitations with respect to data rate and communication range, BLE will often be used together with other wireless technologies to achieve certain goals and functionality.

A common method of integration is to utilize the simple and fast connection process of BLE to set up connection between devices, while the actual data transmissions are performed via another wireless technology. For example, this approach has been implemented and tested for Wi-Fi P2P communications [75], where a pair of nodes exchange Wi-Fi MAC addresses and service lists over BLE advertisements. Nodes then decide whether to establish a Wi-Fi P2P connection based on the contents of the received BLE messages. Once a connection has been established, all data exchange occurs via the Wi-Fi P2P channels. This approach can significantly shorten the latency of connection establishment, while maintaining a high transmission rate. A similar approach could also be based on Classic Bluetooth.

Another type of integration is to transmit non-BLE data packets over BLE networks. One popular idea is to transmit Internet Protocol version 6 (IPv6) packets over BLE. The Internet Engineering Task Force (IETF) published the "IPv6 over

Bluetooth Low Energy" specification in 2015 [76], formally defining a complete protocol stack that integrates BLE (Bluetooth version 4.1 or greater) and IPv6. This stack is based on the *IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN)* standard, which is also maintained by IETF and intended for transmitting IPv6 packets over low-power networks. The IPv6 stack (including 6LoWPAN, IPv6, and UDP/TCP) and GATT stack (including GATT and ATT) work in parallel on top of the BLE L2CAP layer. The 6LoWPAN and L2CAP layers provide address configuration, header compression, fragmentation, and reassembly services to translate IPv6 packets into transferable packets for the BLE PHY layer and vice versa. Based on this concept, several architectures were proposed that yield high throughput [27] or seamless transitions between different protocols [77].

Overall, integrating BLE with existing wireless technologies is a method that can be used to overcome certain weaknesses of each technology, while also offering better compatibility among different types of devices. However, there is still a dearth of work on effective and efficient solutions using this concept, including efforts to standardize such solutions.

4.4. Privacy and Security

Security is of the utmost importance in many application domains. Although recent revisions of BLE were designed for better security and have fixed several vulnerabilities [78, 79], security still remains as a significant challenge for many current and future BLE applications.

Ray et al. successfully performed a series of attacks on Bluetooth 4.2 devices [80] and revealed the weaknesses that have not yet been covered by the LE Secure scheme. They conducted three major attacks on BLE: MITM, Flooding, and Fuzzing attacks. The MITM attack easily breaks a BLE connection and successfully modifies the data packets. The Flooding and Fuzzing attacks do not significantly crash the target BLE device when numerous connection requests and GATT requests are sent to it, but still cause the target device to be "stuck" for a certain period of time. Similar attacks have also been conducted to sniff data from BLE devices (such as keyboards [81]).

Due to the insecure channels and the simplicity of connections, there is a lack of countermeasures that can protect BLE devices from MITM attacks. However, some attempts have been made to secure the transmitted packets, e.g., Perrey et al. [82] proposed a key exchange approach that complements the ECDH algorithm to provide secure connections. This approach applies Merkle's Puzzle to the key generation process, where all puzzles are generated and encrypted depending on the functionality of the devices (i.e., fully functioning or reduced functioning). The encrypted puzzles are then broadcast via BLE advertisements for key distribution, so that further connections will be securely established based on the key. Another attempt, called *Black BLE* [83], applied AES-EAX encryption to both meta-data and payloads of PDUs in each transmission. The encryption method is robust, but it also raises the problem of symmetric key management and reduced payload efficiency.

5. Discussion and Conclusion

BLE is an emerging wireless technology with great potential in many application areas. Ever since its release, it has been successfully applied in many different domains. This paper surveys several BLE applications and describes the challenges and existing solutions regarding data transmissions, mesh networking, inter-operability, and security.

Among traditional application domains, IPS can directly build upon the connectionless BLE transmission, while health monitoring and Home Automation applications rely on connection-based communications and basic BLE network topology. Emerging application domains require more advanced features, such as the inter-operability and mesh network support for smart infrastructure and VANETs, privacy protection for mobile payments and more robust data transmission for multimedia streaming applications. With recent enhancements proposed by the research community, we see that there is great potential for BLE and its use in more emerging domains, especially with the rise of Industrial IoT as its ubiquitous applications in static sensor networks as well as in mobility and transportation industries. While the investigations of current solutions show that some progress has been made, we still witness many opportunities and unsolved problems. Specifically, we propose that the community start with the following directions:

5.1. From Traditional to Emerging

With the release of Bluetooth 5.1, many BLE features have been improved, providing even more opportunities for traditional BLE applications. Bluetooth 5.1 brings two positioning systems to BLE: Angle of Arrival (AoA) and Angle of Departure (AoD). Since they are implemented at the hardware level, BLE-based IPS will then provide more convenient and accurate positioning services even with very few BLE beacons. Based on the location information, home automation can also benefit, e.g., smart home devices can now precisely detect nearby users and take actions accordingly.

Thanks to its low-cost, BLE-based sensors have been widely deployed under various settings, and a lot of data have been generated by these sensors. Utilizing the data and applying machine learning approaches, many more applications could emerge, e.g., attempts have been made to learn and predict moving patterns [84] and distances [85] from the collected data. Similar technologies can also be applied in the Geo-spatial domain, where BLE positioning services and learning models can be used to draw high definition maps for complex road intersections.

5.2. From Small to Large

As BLE technology is now being deployed as a key part in smart city implementation, scalability of the solutions is going to be of paramount interest to the industry. Mesh networking support can apparently expand the range of BLE networks, but there are many other issues that are not fully considered, such as the discovery scheme, connection robustness, support for large payload size of data packets in multi-hop transmission, etc. Since multicast is not supported by connection-based BLE communications [86], system latency is expected to increase significantly as the network scales. Therefore, methods that address many of these issues under one holistic solution architecture design, are currently considered to be the most promising ones to scale the BLE deployment.

5.3. BLE in the era of 5G

It is expected that the arrival of 5G will provide many new opportunities and although 5G communication supports large bandwidth and high data rate communications, BLE can still play a significant role alongside 5G. For example, applications such as bike sharing and station planning services, last-mile delivery services, brain-machine interfaces, etc., can benefit from BLE's ability to provide localized communications, while 5G can handle any required large-scale data transfers for these applications.

With the rise of the Industrial Internet of Things (IIoT) and other technologies such as edge computing, a seamless integration of multiple wireless technologies will often be essential for many deployment environments. IP-based methods [76] are the most popular approaches to connecting constrained devices to the Internet, and it is expected that this will continue to grow due to the ability to provide scalability and simple application development. We therefore expect that BLE will also be used alongside other radio technologies, such are LTE ad 5G, to address the needs of IIoT applications.

Acknowledgment

The project was supported through a Ford Motor Company University Research Program (URP) grant.

References

[1] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, D. Formica, Performance evaluation of bluetooth low energy: A systematic review, Sensors 17 (12) (2017) 2898.

[2] M. Collotta, G. Pau, Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes, Computers & Electrical Engineering 44 (2015) 137–152.

[3] M. S. Gast, Building applications with IBeacon: proximity and location services with bluetooth low energy, " O'Reilly Media, Inc.", 2014.

[4] X.-Y. Lin, T.-W. Ho, C.-C. Fang, Z.-S. Yen, B.-J. Yang, F. Lai, A mobile indoor positioning system based on ibeacon technology, in: Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE, IEEE, 2015, pp. 4970–4973.

[5] R. Faragher, R. Harle, Location fingerprinting with bluetooth low energy beacons, IEEE journal on Selected Areas in Communications 33 (11) (2015) 2418–2428.

[6] D. De, P. Bharti, S. K. Das, S. Chellappan, Multimodal wearable sensing for fine-grained activity recognition in healthcare, IEEE Internet Computing 19 (5) (2015) 26–35.

[7] K. Židek, J. Pitel, Smart 3d pointing device based on mems sensor and bluetooth low energy, in: Computational Intelligence in Control and Automation (CICA), 2013 IEEE Symposium on, IEEE, 2013, pp. 207–211.

[8] T. Takahashi, Y. Shibata, S. Imata, N. Suzuki, Evaluation of wake-on-demand accurate activation and in-vehicle wireless connecation control, in: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015 10th International Conference on, IEEE, 2015, pp. 143–149.

[9] W. Bronzi, R. Frank, G. Castignani, T. Engel, Bluetooth low energy performance and robustness analysis for inter-vehicular communications, Ad Hoc Networks 37 (2016) 76–86.

[10] J. Yang, C. Poellabauer, P. Mitra, Using bluetooth low energy for dynamic information-sharing in vehicle-to-vehicle communication, SAE International Journal of Passenger Cars-Electronic and Electrical Systems 10 (2017-01-1650) (2017) 240–247.

[11] J.-E. Kim, M. Bessho, S. Kobayashi, N. Koshizuka, K. Sakamura, Navigating visually impaired travelers in a large train station using smartphone and bluetooth low energy, in: Proceedings of the 31st Annual ACM Symposium on Applied Computing, ACM, 2016, pp. 604–611.

[12] G. Rajagopal, V. M. Lodd, A. Vignesh, R. Rajesh, V. Vijayaraghavan, Low cost cloud based intelligent farm automation system using bluetooth low energy, in: Humanitarian Technology Conference (R10-HTC), 2014 IEEE Region 10, IEEE, 2014, pp. 127–132.

[13] M. Vochin, A. Vulpe, G. Suciu, L. Boicescu, Intelligent displaying and alerting system based on an integrated communications infrastructure and low-power technology, in: World Conference on Information Systems and Technologies, Springer, 2017, pp. 135–141.

[14] D. Giovanelli, B. Milosevic, E. Farella, Bluetooth low energy for data streaming: Application-level analysis and recommendation, in: Advances in Sensors and Interfaces (IWASI), 2015 6th IEEE International Workshop on, IEEE, 2015, pp. 216–221.

[15] M. Meli, O. Rion, Streaming speech and music using bluetooth low energy, in: Embedded World Conference, Nuremberg, February, WEKA Fachmedien, 2015, pp. 24–26.

[16] C. Shao, S. Nirjon, J.-M. Frahm, Years-long binary image broadcast using bluetooth low energy beacons, in: Distributed Computing in Sensor Systems (DCOSS), 2016 International Conference on, IEEE, 2016, pp. 225–232.

[17] M. Todasco, Systems and methods for completion of item delivery and transactions using a mobile beacon, uS Patent App. 14/154,414 (Apr. 30 2015).

[18] D. Baldie, System and method for providing a bluetooth low energy mobile payment system, uS Patent App. 14/469,230 (Mar. 3 2016).

[19] B. SIG, Bluetooth core specification version 4.0, Specification of the Bluetooth System.

[20] B. SIG, Bluetooth core specification version 4.1, Specification of the Bluetooth System.

[21] B. SIG, Bluetooth core specification version 4.2, Specification of the Bluetooth System.

[22] B. SIG, Bluetooth core specification version 5.0, Specification of the Bluetooth System.

[23] B. SIG, Bluetooth core specification version 5.1, Specification of the Bluetooth System.

[24] M. Galeev, Bluetooth 4.0: an introduction to bluetooth low energy-part ii, EE Times, Design.

[25] C. Gomez, J. Oller, J. Paradells, Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology, Sensors 12 (9) (2012) 11734–11753.

[26] S. Bluetooth, Mesh networking specifications (2017).

[27] J. Yim, S. Kim, N.-K. Kim, Y.-B. Ko, Ipv6 based realtime acoustic data streaming service over bluetooth low energy, in: Communications, Computers and Signal Processing (PACRIM), 2015 IEEE Pacific Rim Conference on, IEEE, 2015, pp. 269–273.

[28] J. Decuir, Introducing bluetooth smart: Part ii: Applications and updates., IEEE Consumer Electronics Magazine 3 (2) (2014) 25–29.

[29] D. Čabarkapa, I. Grujić, P. Pavlović, Comparative analysis of the bluetooth low-energy indoor positioning systems, in: Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2015 12th International Conference on, IEEE, 2015, pp. 76–79.

[30] M. Altini, D. Brunelli, E. Farella, L. Benini, Bluetooth indoor localization with multiple neural networks, in: Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on, IEEE, 2010, pp. 295–300.

[31] F. Palumbo, P. Barsocchi, S. Chessa, J. C. Augusto, A stigmergic approach to indoor localization using bluetooth low energy beacons, in: Advanced Video and Signal Based Surveillance (AVSS), 2015 12th IEEE International Conference on, IEEE, 2015, pp. 1–6.

[32] P. Kriz, F. Maly, T. Kozel, Improving indoor localization using bluetooth low energy beacons, Mobile Information Systems 2016.

[33] M. Ali, L. Albasha, H. Al-Nashash, A bluetooth low energy implantable glucose monitoring system, in: Microwave Conference (EuMC), 2011 41st European, IEEE, 2011, pp. 1265–1268.

[34] L. Guo-Cheng, Y. Hong-Yang, Design and implementation of a bluetooth 4.0-based heart rate monitor system on ios platform, in: Communications, Circuits and Systems (ICCCAS), 2013 International Conference on, Vol. 2, IEEE, 2013, pp. 112–115.

[35] Z.-M. Lin, C.-H. Chang, N.-K. Chou, Y.-H. Lin, Bluetooth low energy (ble) based blood pressure monitoring system, in: Intelligent Green Building and Smart Grid (IGBSG), 2014 International Conference on, IEEE, 2014, pp. 1–4.

[36] B. Zhou, X. Chen, X. Hu, R. Ren, X. Tan, Z. Fang, S. Xia, A bluetooth low energy approach for monitoring electrocardiography and respiration, in: e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on, IEEE, 2013, pp. 130–134.

[37] M. Khan, S. Din, S. Jabbar, M. Gohar, H. Ghayvat, S. Mukhopadhyay, Context-aware low power intelligent smarthome based on the internet of things, Computers & Electrical Engineering 52 (2016) 208–222.

[38] M. Collotta, G. Pau, A novel energy management approach for smart homes using bluetooth low energy, IEEE Journal on Selected Areas in Communications 33 (12) (2015) 2988–2996.

[39] O. Galinina, K. Mikhaylov, S. Andreev, A. Turlikov, Y. Koucheryavy, Smart home gateway system over bluetooth low energy with wireless energy transfer capability, EURASIP Journal on Wireless Communications and Networking 2015 (1) (2015) 1–18.

[40] L. Mainetti, L. Patrono, I. Sergi, A survey on indoor positioning systems, in: Software, Telecommunications and Computer Networks (SoftCOM), 2014 22nd International Conference on, IEEE, 2014, pp. 111–120.

[41] N. Cinefra, An adaptive indoor positioning system based on bluetooth low energy rssi, Master's thesis, Politecnico di Milano, Milano, Italy (2014).

[42] A. H. Omre, S. Keeping, Bluetooth low energy: wireless connectivity for medical monitoring, Journal of diabetes science and technology 4 (2) (2010) 457–463.

[43] N. Abou-Rahme, Six ways to innovation with smart infrastructure (2018).
URL https://www.mottmac.com/views/six-ways-to-innovation-with-smart-infrastructure

[44] S. Kulkarni, S. Piper, S. Lipták, D. Divan, Implementing pay-as-you-go functionality in microgrids using mobile ad-hoc networks, in: 2019 IEEE Decentralized Energy Access Solutions Workshop (DEAS), IEEE, 2019, pp. 207–212.

[45] M. Boukhechba, A. Bouzouane, S. Gaboury, C. Gouin-Vallerand, S. Giroux, B. Bouchard, A novel bluetooth low energy based system for spatial exploration in smart cities, Expert Systems with Applications.

[46] S. Doar, J. Merkin, Bringing neighbors back to neighborhoods (2018).
URL http://www.sidewalklabs.com/blog/bringing-neighbors-back-to-neighborhoods/

[47] R. Frank, W. Bronzi, G. Castignani, T. Engel, Bluetooth low energy: An alternative technology for vanet applications, in: Wireless On-demand Network Systems and Services (WONS), 2014 11th Annual Conference on, IEEE, 2014, pp. 104–107.

[48] J. Yang, C. Poellabauer, P. Mitra, J. Rao, C. Neubecker, Bluenet: Ble-based ad-hoc communications without predefined roles, in: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2017, pp. 1–8.

[49] M. Wu, B. Ma, Z. Liu, L. Xiu, L. Zhang, Ble-horn: A smartphone-based bluetooth low energy vehicle-to-pedestrian safety system, in: Wireless Communications and Signal Processing (WCSP), 2017 9th International Conference on, IEEE, 2017, pp. 1–6.

[50] H. Park, S. Lee, E. Moon, S. H. Ahmed, D. Kim, Performance analysis of bicycle-to-pedestrian safety application using bluetooth low energy, in: Proceedings of the International Conference on Research in Adaptive and Convergent Systems, ACM, 2017, pp. 160–165.

[51] M. Komarov, D. Moltchanov, System design and analysis of uav-assisted ble wireless sensor systems, in: International Conference on Wired/Wireless Internet Communication, Springer, 2016, pp. 284–296.

[52] M. Lodeiro-Santiago, I. Santos-González, P. Caballero-Gil, C. Caballero-Gil, Secure system based on uav and ble for improving sar missions, Journal of Ambient Intelligence and Humanized Computing (2017) 1–12.

[53] M. M. Scheunemann, K. Dautenhahn, Bluetooth low energy for autonomous human-robot interaction, in: Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, ACM, 2017, pp. 52–52.

[54] J. Klinglmayr, B. Bergmair, M. A. Klaffenböck, L. Hörmann, E. Pournaras, Sustainable consumerism via context-aware shopping, International Journal of Distributed Systems and Technologies (IJDST) 8 (4) (2017) 54–72.

[55] M. R. Tinskey, M. Seneski, B. Walter, R. P. Eaton, Wireless payment transactions in a vehicle environment, uS Patent App. 15/092,031 (Oct. 12 2017).

[56] K. Cho, G. Park, W. Cho, J. Seo, K. Han, Performance analysis of device discovery of bluetooth low energy (ble) networks, Computer Communications 81 (2016) 72–85.

[57] J. Liu, C. Chen, Y. Ma, Y. Xu, Adaptive device discovery in bluetooth low energy networks, in: Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th, IEEE, 2013, pp. 1–5.

[58] G. Park, W. Park, M. Hong, K. Cho, W. Cho, J. Seo, K. Han, An adaptive parameter setting algorithm to enhance performance in self-organizing bluetooth low energy networks, Wireless Personal Communications 87 (3) (2016) 953–969.

[59] J. Seo, K. Cho, W. Cho, G. Park, K. Han, A discovery scheme based on carrier sensing in self-organizing bluetooth low energy networks, Journal of Network and Computer Applications 65 (2016) 72–83.

[60] J. Kim, K. Han, Backoff scheme for crowded bluetooth low energy networks, IET Communications 11 (4) (2017) 548–557.

[61] J. Kim, S.-k. Kang, J. Park, Bluetooth-based tree topology network for wireless industrial applications, in: Control, Automation and Systems (ICCAS), 2015 15th International Conference on, IEEE, 2015, pp. 1305–1308.

[62] S. M. Darroudi, C. Gomez, Bluetooth low energy mesh networks: A survey, Sensors 17 (7) (2017) 1467.

[63] O. Turkes, H. Scholten, P. J. Havinga, Blessed with opportunistic beacons: A lightweight data dissemination model for smart mobile ad-hoc networks, in: Proceedings of the 10th ACM MobiCom Workshop on Challenged Networks, ACM, 2015, pp. 25–30.

[64] H.-S. Kim, J. Lee, J. W. Jang, Blemesh: A wireless mesh network protocol for bluetooth low energy devices, in: Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, IEEE, 2015, pp. 558–563.

[65] K. Mikhaylov, J. Tervonen, Multihop data transfer service for bluetooth low energy, in: ITS Telecommunications (ITST), 2013 13th International Conference on, IEEE, 2013, pp. 319–324.

[66] S. Sirur, P. Juturu, H. P. Gupta, P. R. Serikar, Y. K. Reddy, S. Barak, B. Kim, A mesh network for mobile devices using bluetooth low energy, in: SENSORS, 2015 IEEE, IEEE, 2015, pp. 1–4.

[67] A. Balogh, S. Imre, K. Lendvai, S. Szabó, Service mediation in multihop bluetooth low energy networks based on ndn approach, in: Software, Telecommunications and Computer Networks (SoftCOM), 2015 23rd International Conference on, IEEE, 2015, pp. 285–289.

[68] Z. Guo, I. G. Harris, L.-f. Tsaur, X. Chen, An on-demand scatternet formation and multi-hop routing protocol for ble-based wireless sensor networks, in: Wireless Communications and Networking Conference (WCNC), 2015 IEEE, IEEE, 2015, pp. 1590–1595.

[69] C. Jung, K. Kim, J. Seo, B. N. Silva, K. Han, Topology configuration and multihop routing protocol for bluetooth low energy networks, IEEE Access 5 (2017) 9587–9598.

[70] G. Patti, L. Leonardi, L. L. Bello, A bluetooth low energy real-time protocol for industrial wireless mesh networks, in: Industrial Electronics Society, IECON 2016-42nd Annual Conference of the IEEE, IEEE, 2016, pp. 4627–4632.

[71] L. Leonardi, G. Patti, L. L. Bello, Multi-hop real-time communications over bluetooth low energy industrial wireless mesh networks, IEEE Access.

[72] C.-M. Yu, E.-L. Lin, Reliable formation protocol for

bluetooth hybrid single-hop and multi-hop networks, IEEE Network 32 (2) (2018) 120–125.

[73] S. Silva, S. Soares, T. Fernandes, A. Valente, A. Moreira, Coexistence and interference tests on a bluetooth low energy front-end, in: Science and Information Conference (SAI), 2014, IEEE, 2014, pp. 1014–1018.

[74] M. O. Al Kalaa, W. Balid, N. Bitar, H. H. Refai, Evaluating bluetooth low energy in realistic wireless environments, in: Wireless Communications and Networking Conference (WCNC), 2016 IEEE, IEEE, 2016, pp. 1–6.

[75] H. Joh, I. Ryoo, A hybrid wi-fi p2p with bluetooth low energy for optimizing smart devices communication property, Peer-to-Peer Networking and Applications 8 (4) (2015) 567–577.

[76] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, C. Gomez, Ipv6 over bluetooth (r) low energy, Tech. rep., Internet Engineering Task Force (IETF) (2015).

[77] H. Wang, M. Xi, J. Liu, C. Chen, Transmitting ipv6 packets over bluetooth low energy based on bluez, in: Advanced Communication Technology (ICACT), 2013 15th International Conference on, IEEE, 2013, pp. 72–77.

[78] M. Ryan, et al., Bluetooth: With low energy comes low security., WOOT 13 (2013) 4–4.

[79] A. K. Das, P. H. Pathak, C.-N. Chuah, P. Mohapatra, Uncovering privacy leakage in ble network traffic of wearable fitness trackers, in: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, ACM, 2016, pp. 99–104.

[80] A. Ray, V. Raj, M. Oriol, A. Monot, S. Obermeier, Bluetooth low energy devices security testing framework, in: Software Testing, Verification and Validation (ICST), 2018 IEEE 11th International Conference on, IEEE, 2018, pp. 384–393.

[81] T. Willingham, C. Henderson, B. Kiel, M. S. Haque, T. Atkison, Testing vulnerabilities in bluetooth low energy, in: Proceedings of the ACMSE 2018 Conference, ACM, 2018, p. 6.

[82] H. Perrey, O. Ugus, D. Westhoff, Wisec'2011 poster: security enhancement for bluetooth low energy with merkle's puzzle, ACM SIGMOBILE Mobile Computing and Communications Review 15 (3) (2011) 45–46.

[83] S. Chakrabarty, D. W. Engels, Black networks for bluetooth low energy, in: Consumer Electronics (ICCE), 2016 IEEE International Conference on, IEEE, 2016, pp. 11–14.

[84] Y.-C. Pu, P.-C. You, Indoor positioning system based on ble location fingerprinting with classification approach, Applied Mathematical Modelling 62 (2018) 654–663.

[85] C. H. Lam, P. C. Ng, J. She, Improved distance estimation with ble beacon using kalman filter and svm, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–6.

[86] K.-H. Chang, Bluetooth: a viable solution for iot?[industry perspectives], IEEE Wireless Communications 21 (6) (2014) 6–7.