1-2019

A survey on bluetooth 5.0 and mesh: New milestones of IoT

Juenjie YIN

Zheng YANG

Hao CAO

Tongtong LIU

Zimu ZHOU
Singapore Management University, zimuzhou@smu.edu.sg

See next page for additional authors

A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT

JUNJIE YIN and ZHENG YANG, Tsinghua University
HAO CAO, Tianjin University
TONGTONG LIU, Tsinghua University
ZIMU ZHOU, ETH Zurich
CHENSHU WU, University of Maryland, College Park

Ubiquitous connectivity among objects is the future of the coming Internet of Things era. Technologies are competing fiercely to fulfill this goal, but none of them can fit into all application scenarios. However, efforts are still made to expand application ranges of certain technologies. Shortly after the adoption of its newest version, Bluetooth 5.0, the Bluetooth Special Interest Group released another new specification on network topology: Bluetooth Mesh. Combined together, those two bring Bluetooth to a brand new stage. However, current works related to it only focus on part of the new Bluetooth, and discussion over the entire one is lacking. Therefore, in this survey, we conduct an investigation toward the new Bluetooth from a comprehensive perspective. Through this, we show that the new Bluetooth not only consolidates its strengths in original application fields but also brings alterations and opportunities to new ones, making it a strong competitor in the future for providing complete solutions to meet the demands of seamless communications in the Internet of Things area.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Networks** → *Network performance analysis*;

Additional Key Words and Phrases: IoT, Bluetooth, application

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

1 INTRODUCTION

Recent years have seen an explosion of Internet of Things (IoT) applications. From home to office, diversities of IoT devices have been born and are at work around us, such as smart doors, shared bikes, and sweeping robots, which gives us a feeling that IoT technologies are literally connecting everything into networks. And from the numbers, we can see that this feeling is coming true. Gartner estimates that there will be 26 billion units of bases installed with IoT technologies by

This work was supported by the National Key Research Plan under grant 2016YFC0700100, and the NSFC under grants 61832010, 61632008, 61672319, 61572366, and 61872081.
Authors' addresses: J. Yin, Z. Yang (corresponding author), and T. Liu, Tsinghua University; emails: yinjj16@gmail.com, hmilyyz@gmail.com, jshaltt7@163.com; H. Cao, Tianjin University; email: nyz1500@gmail.com; Z. Zhou, ETH Zurich; email: zhouzimu.hk@gmail.com; C. Wu, University of Maryland, College Park; email: wucs32@gmail.com.

1550-4859/2019/05-ART28 $15.00
https://doi.org/10.1145/3317687

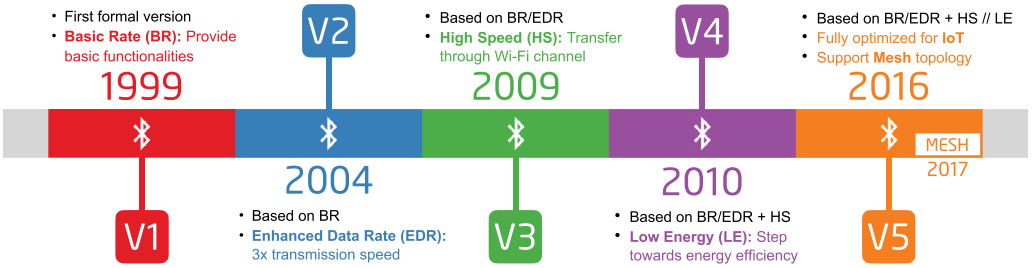

Fig. 1. A brief history of Bluetooth.

2020 [31] and that the market of IoT technologies, products, and services will reach $267 billion by then, according to a BCG's report [12]. It seems that IoT technologies have profoundly changed our daily life and transformed industrial manufacturing, and may even reform the way our society works in the near future.

In the picture of the coming IoT era, one basic and distinctive feature is the pervasive connectivity among people, devices, or even things. To fulfill this goal, varieties of technologies (e.g., RFID, Wi-Fi, Bluetooth, ZigBee, LoRa, NB-IoT) have been developed in the past decades. However, since the concept of IoT covers so many different kinds of application scenarios, none of the existing technologies can serve well or even merely be applicable in all of them. Actually, certain technologies are designed for meeting certain demands, or in other words, certain applications require appropriate IoT technologies [21]. For example, for applications that require a long transmission range but are limited in power supply, such as environmental monitoring, the priority option is to pick one from the category of low-power wide-area networks (LPWANs), such as LoRa and NB-IoT. But for those demanding low latency(e.g., industrial control) or high transmission throughput (e.g., video transmission), LPWANs are completely out of consideration.

Of course, IoT technologies do not remain the same forever. Instead, they continue to evolve and sometimes develop new functions to expand their application fields. Take IEEE 802.11, mostly called *Wi-Fi*, as an example. Most people see this as a house-wide high-throughput wireless transmission technology. And when it comes to its weaknesses, one of the most frequently mentioned features is its high power consumption, which makes it seldom considered in low-power applications. Therefore, to address this problem, the IEEE 802.11 Working Group has published a sub-1GHz low-power version called *802.11 ah* [48], aiming at the markets of LPWANs.

The most recent evolution drawing our attention is the newest generation of Bluetooth. More concretely, the Bluetooth Special Interest Group (SIG) released Bluetooth 5.0 [34], together with its first official specification for mesh topology, Bluetooth Mesh [8]. And why does this new generation of Bluetooth matter?

If we look at the history of Bluetooth, as illustrated in Figure 1, there is a tradition starting from the first generation that provided the Basic Rate (BR) for basic functionalities; each generation of Bluetooth came with a brand new mode that either added new functions or boosted certain performance. In 2.x and 3.x generations, the Bluetooth SIG introduced the Enhanced Data Rate (EDR) and High Speed (HS) to boost throughput with different manners, which composed one basic part of Bluetooth, BR/EDR. In the 4.x generation, another basic part, Low Energy (LE), was introduced to expand application fields of Bluetooth to low-power ones. Hence, as a convention, we expected to see the same happen to the fifth generation. And it did not fail us. The fifth generation is certainly a greatly enhanced new generation. According to the Bluetooth SIG, Bluetooth 5.0 achieves two times the transmission speed, four time times the transmission range, and eight times the broadcasting capacity of Bluetooth 4.2 [37]. Those enhancements can strengthen the competitiveness

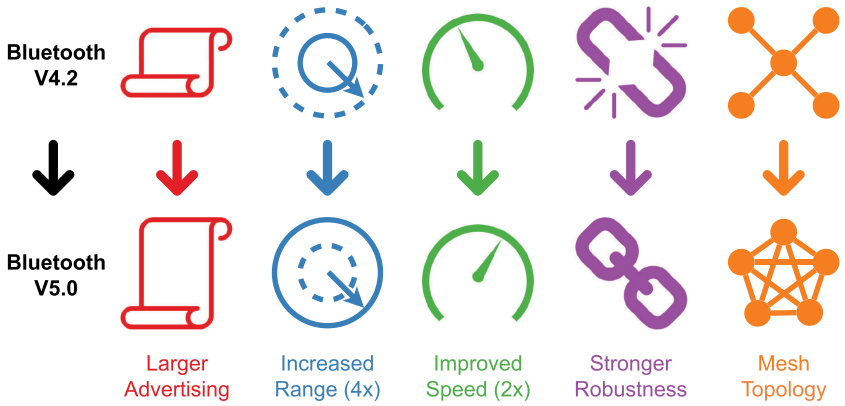

Fig. 2. Improvements of Bluetooth 5.0 & Mesh over Bluetooth 4.2.

of Bluetooth, because with them, devices equipped with Bluetooth 5.0 can now transfer information faster and further and can establish more stable connections with richer content. And in the following Bluetooth Mesh, the official support for mesh finally comes to Bluetooth. Both of the two updates greatly strengthen Bluetooth and enlarge its application fields. Especially, with mesh, Bluetooth now is able to be massively deployed in applications with completely different forms. Therefore, the fifth generation of Bluetooth may possibly be as important as the BLE to both the Bluetooth technology itself and the IoT area, which makes it worthy to be evaluated with both its predecessors and its competitors.

In addition, Bluetooth Mesh is not tied to Bluetooth 5.0. Actually, Bluetooth Mesh can be combined with any version after Bluetooth 4.0 as long as BLE is supported. However, in this work, we take Bluetooth 5.0 and Bluetooth Mesh as a group and see mesh topology as one major enhancement of this fifth generation, as illustrated in Figure 2. The reason behind this point of view is that the majority of enhancements achieved in Bluetooth 5.0 and mesh topology are both for the LE part. It is natural to take a whole picture of the upgraded BLE after combining those two specifications together. And we see enhancements in Bluetooth 5.0 as an upgrade in end-to-end connections between two devices, whereas Bluetooth Mesh is an upgrade in network structure among groups of devices. In other words, those two specifications are different layers of upgrades of Bluetooth and shall be considered together when evaluating the new Bluetooth. With mesh topology, Bluetooth gains access to new applications as well. Evaluations on how joint Bluetooth will influence these new applications are required.

In this survey, we have made efforts to investigate and discuss issues around the new Bluetooth. Specifically, we are going to address the following questions:

(1) Since this new Bluetooth is important, what exactly is it? Especially, what exactly are those desired new capabilities that this new Bluetooth brings, and how they are achieved?
(2) How will the IoT area be influenced by the new Bluetooth? Especially, how can IoT applications, no matter old or new to Bluetooth, benefit from those new features?
(3) How does the joint Bluetooth perform in real scenarios? In addition, compared to its competitors, what are its pros and cons?
(4) Those questions open other issues. How may Bluetooth be further improved to meet the requirements of seamless connections in the coming IoT area? With performance fully improved, what are the possible next directions that Bluetooth can head toward?

Several research works have been conducted to answer some of the preceding questions.

Two works have investigated Bluetooth 5.0 and Bluetooth Mesh. Collatta et al. [3] give a brief introduction on Bluetooth 5.0 over enhancements and benefited applications. In addition, simple experiments comparing Bluetooth 4.2, Bluetooth 5.0, and IEEE 802.15.4 regarding throughput, range, and power consumption are conducted. Baert et al. [1] thoroughly investigate how Bluetooth Mesh operates and introduces related concepts and mechanisms. Performance of Bluetooth Mesh is evaluated in terms of latencies through theoretical analysis, experimental assessments, and graph-based simulation. Both of these two works have introduced and evaluated part of the new Bluetooth but lack evaluations over the entire group due to limits of published time or hardware conditions. Based on them, we go one step further to combine Bluetooth 5.0 and Bluetooth Mesh together and evaluate the performance of the new Bluetooth in a more comprehensive perspective. Huge amounts of comparisons over Bluetooth 5.0 and Bluetooth Mesh against other wireless technologies have been conducted. In the work of Karvonen et al. [16], performance parameters (i.e., throughput and range) are evaluated under both indoor and outdoor conditions for measuring how much Bluetooth 5 gets improved compared to Bluetooth 4. In the work of Silicon Labs [19], thorough tests over Bluetooth Mesh, ZigBee, and Thread in real scenarios are conducted with regard to performance parameters like latency and throughput. In the work of Samie et al. [32], a bunch of communication technologies are compared on their properties and typical application fields, including Bluetooth 5.0. Additionally, things are different now, as Bluetooth has added mesh functionality.

However, current works only focus on part of the new Bluetooth, and discussions over the entire technology is lacking. Therefore, in this survey, we make an effort to present a comprehensive introduction toward the new Bluetooth, regarding issues from new features written in specifications to applications to performances in real scenarios. Based on these, we discuss how the new Bluetooth will influence the IoT area. The main contributions of this survey are the following:

- To the best of our knowledge, this survey is the first research work concerning both Bluetooth 5.0 and Bluetooth Mesh together for discussing how the fifth generation of Bluetooth will influence the IoT area.
- We thoroughly survey research and tests done on different aspects of the new Bluetooth and integrate them in our survey for comprehensively discussing the new Bluetooth.
- Through joint evaluations and discussions, we show that by combining them together, Bluetooth can gain marvelous advantages over ZigBee, which gives it the potential to take over the market of ZigBee in its new applications.

The outline of this article is summarized as follows. Bluetooth 5.0 and Bluetooth Mesh are separately presented in Sections 2 and 3. In Section 2, new features of Bluetooth 5.0 are listed and discussed to figure out how Bluetooth benefits from them. In Section 3, detailed explanations on Bluetooth Mesh are provided, ending with a toy example for demonstrating communicating and controlling processes of it. In Section 4, based on new features introduced in the two specifications, we qualitatively discuss how it may impact applications of the IoT area. In Section 5, we qualitatively evaluate it through theoretical and experimental comparisons. Specifically, we start with an overall comparison between Bluetooth and its competitors in new applications regarding typical properties considered in such applications to see how it will alter the relative strength of Bluetooth and its competitors. After that, experimental comparisons over single-link and networked connections are conducted between the new Bluetooth and ZigBee. In Section 6, we discuss possible research directions and future work with regard to Bluetooth, mainly concerning how Bluetooth can further promote the IoT area. Section 7 summarizes this survey.

Table 1. New Features Introduced in Bluetooth 5.0

New Features [34]	BR/EDR	LE	Explanations
Slot Availability Mask	Yes	Yes	Enabling two Bluetooth devices to indicate to each other the availability of their time slots for transmission and reception.
2Msym/s PHY for LE	No	Yes	One of the three PHYs defined in Bluetooth 5.0 (LE 1M, LE 1M coded, LE 2M). It is a new optional modulation scheme that uses a 2Msym/s symbol rate and does not support a coding scheme.
LE Long Range	No	Yes	A new mode achieved by a new coding scheme using forward error correction.
High Duty Cycle Non-Connectable Advertising	No	Yes	Disabling heterogeneous minimum advertising intervals.
LE Advertising Extensions	No	Yes	An upgraded advertising mode utilizes another 37 channels that are not used for advertising in previous versions. Additionally, some corresponding features are appended.
LE Channel Selection Algorithm #2	No	Yes	A new channel selection algorithm defined in the link layer. Compared to Channel Selection Algorithm #1, which only supports channel selection for connection events, it adds support for channel selection for periodic advertising packets.
Higher Output Power	Yes	Yes	The highest output power raises from 10 to 20 dBm.

2 WHAT'S NEW IN BLUETOOTH 5.0

According to the Bluetooth SIG, compared to its predecessor Bluetooth 4.2, Bluetooth 5.0 achieves doubled speed, four times the transmission range, and eight times the advertising capacity. Apart from those, this new version also shows stronger robustness to interferences compared to Bluetooth 4.2. To make these advertisements come true, plenty of new features are introduced in Bluetooth 5.0. We extract the new features from the specification of Bluetooth 5.0 [34] as listed in Table 1 and provide our concluded explanations and simple judgments on whether they can be used in certain Bluetooth modes.

As shown in Table 1, most of the innovations in this new version are specifically proposed for BLE, and the classic BR/EDR almost remains identical. Three features match the three most significant enhancements of Bluetooth 5.0:

- The newly added modulation scheme in the PHY layer is 2Msym/s. It allows BLE to use 2MHz bandwidth to transmit data, which corresponds to the doubled speed.
- LE Long Range, as the name says, is for the quadrupled transmission range, which is done by a new coding scheme that will be introduced in detail in the following section.
- LE Advertising Extensions is the main contributor to the eight times advertising capacity. It utilizes another 37 channels that are not used for advertising in previous versions.

Together with other new features, they make a more competitive new Bluetooth.

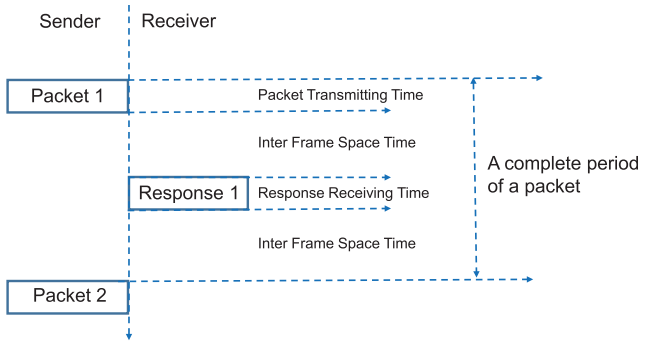

Fig. 3. Parts contained in a complete period of a Bluetooth packet.

In addition, although Bluetooth 5.0 is backward compatible, it cannot be directly applied in old Bluetooth devices because it requires a change in hardware to support its new features. In the following sections, we show how those new features lead to increased speed, enlarged coverage, greater advertising capacity, and stronger robustness.

2.1 Increased Speed

Increased speed is mainly contributed to the new feature, 2 Msym/s PHY for LE, which is a new modulation scheme of the PHY layer added in Bluetooth 5.0.

In Bluetooth 5.0, there are three different kinds of PHYs defined: LE 1M uncoded, LE 1M coded, and LE 2M uncoded. The name contains three parts. "LE" means that it is used for BLE. "1M" or "2M" means that the symbol rate is 1Mb/s or 2Mb/s. "Coded" or "uncoded" means whether it uses an error coding scheme, a classic choice in communication for increasing sensitivity of wireless signals so that after recovery, signals can achieve same error rates while being transmitted further.

But as we know, bandwidth is a limited resource that cannot be expanded as wished, and we expand on why this can happen. Bluetooth uses the 2.4GHz ISM band for communication, specifically 2.400GHz ~ 2.4835GHz in Europe and America. When working in BLE mode, it divides the band into 40 subbands, each of which occupies 2MHz bandwidth. Therefore, 2MHz is the theoretical maximum bandwidth for BLE. Thus, when this resource is fully utilized, the result is the "doubled speed."

By choosing 2Msym/s PHY, the same amount of data that used to need 2,000ms to finish transmission now only needs 1,000ms. And with a faster transmission speed, Bluetooth becomes more energy efficient as the time needed to transfer a same-size file can be halved.

However, as we know, doubled bandwidth, or a doubled symbol rate, does not mean doubled throughput. According to calculations in an official blog on the website of Bluetooth [30], the actual throughput of Bluetooth 5.0 is about 1.4Mbps, which is 1.7 times the actual throughput of Bluetooth 4.2 due to unchanged time intervals between packets and so forth.

Specifically, with regard to Bluetooth, in a complete period of a packet, there are two segments of inter-frame space time: one slot for the received packet from the sender's peer device and one slot for transmitting data, as illustrated in Figure 3. Halved though the packet transmitting time and the response receiving time, the inter-frame space time remains the same as previously. To be specific, the time of the slot for transmitting data is reduced from 2,120μs to 1,060μs, and to 40 μs from 80 μs for receiving confirmation data. But the inter-frame space time remains the same at 150μs.

In addition, due to the packet structure, not all bits are for actual payload inside a packet. Take the advertising packet that we present later in Figure 5 as an example. The useful payload data only occupies a part of the whole packet. Therefore, the real data rate will be less than the symbol rate

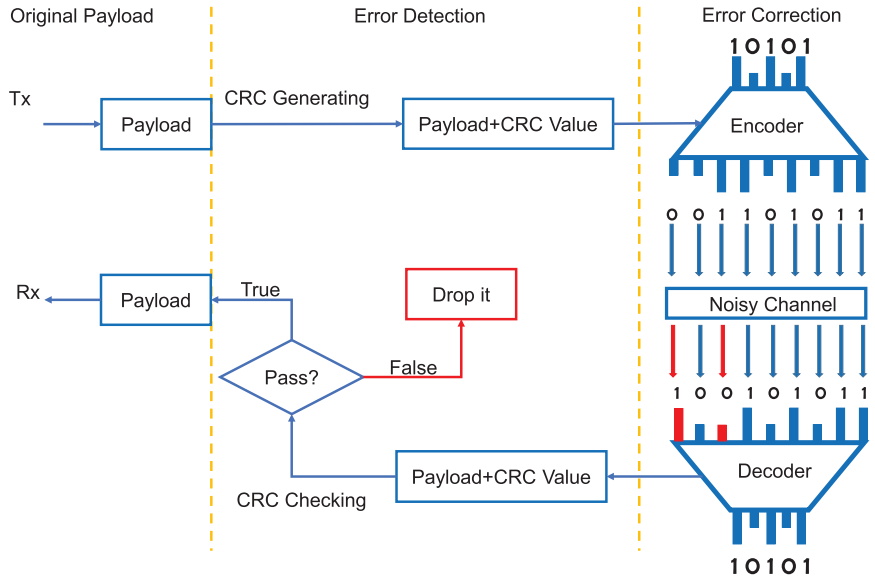

Fig. 4. A simplified example for illustrating error processing of Bluetooth.

given. And with regard to Bluetooth 4.2 and Bluetooth 5.0, maximum throughput can be calculated as up to around 0.8 and 1.4 Mbps, respectively.

Another new feature, high duty cycle non-connectible advertising, also contributes to an increased speed when considering certain advertising events. Several types of advertising events are defined in Bluetooth. However, in Bluetooth 4.x versions, they are treated differently. Bluetooth 4.x versions separate two advertising events, Scannable Undirected and Non-Connected Undirected, with the others through setting their minimum advertising interval at 100ms, whereas the others are set at 20ms. And in Bluetooth 5.0, minimum advertising intervals of different advertising events are uniform at 20ms. Thus, theoretically, the advertising data rates of some advertising events can be four times larger than before.

2.2 Enlarged Coverage

Maybe the most important enhancement of Bluetooth 5.0 is the enlarged coverage. Again, like the increased speed, this enhancement is only for BLE, as pointed out in the name of the corresponding new feature, LE Long Range.

This enhancement is achieved through two changes. The major change is the newly introduced coding scheme. In the previous section, we introduced that there are three modulation schemes in the PHY layer of Bluetooth 5.0. The LE 2M Uncoded scheme is for the increased speed, and the LE 1M Coded scheme is for the enlarged coverage. Bluetooth uses a coding scheme to deal with errors occurring in communication processes so that signals can be correctly received in longer distances.

Compared to the previous way of processing errors, Bluetooth 5.0 adds error correction in addition to error detection [39]. A simplified error processing procedure is illustrated in Figure 4.

Error detection remains the same as in early versions, as shown in the left and middle parts of Figure 4. A 24-bit cyclic redundancy check (CRC) value is generated for error detection. When a packet is received, the receiver will compare the received CRC value to the recalculated CRC value. If they are the same, the receiver will think that no error has occurred. Otherwise, it just drops the packet.

However, in Bluetooth 5.0, forward error correction (FEC) is adopted for error correction. FEC is a general approach used in communication for controlling errors occurring in data transmission over noisy channels, which trades off the data rate for higher data sensitivity. In general, it uses several symbols to represent one bit so that original data can be recovered if the damage is not too severe, as illustrated in the right part of Figure 4, where we show a very simple example of classic Hamming code [10] to do FEC. Equivalently, FEC increases the energy of each bit of the actual payload through redundancy but does not increase transmitting power.

According to the number of symbols used for one bit, there are two coding schemes defined in Bluetooth 5.0: $S = 2$ and $S = 8$ (S represents the number of symbols used per bit). With the symbol rate of 1Msym/s, it is easy to calculate the theoretical maximum bit rate decreases to 500kbps or 125kbps, corresponding to the two and four times range.

The minor one is the higher output power. This is a new feature for both modes of Bluetooth. The highest output power defined in the Bluetooth 5.0 specification is raised from 10 to 20 dBm, which can lead to a straightforward increase in connection range. Additionally, for BLE devices, the highest output power can remain at 10dBm if its LE PHY can only support 1 Msym/s PHY. And for establishing connections, the highest output power level is not allowed to be used.

It is hard to give an accurate number on how far on earth Bluetooth 5.0 can reach. According to tests mentioned in one official blog [39], even Bluetooth 4.2 can achieve up to 350m outdoors, and a Bluetooth module exists whose datasheet claims a possible range of 500m. But in experiments conducted in one survey work [3], the throughput of Bluetooth 4.2 decreases to zero when the distance is 120m. And for Bluetooth 5.0, the throughput is 105kbps, which means that the long range mode works.

From the different PHYs, we can see that Bluetooth 5.0 offers its users two options, either transmitting faster with a doubled symbol rate or transmitting farther while carrying fewer data, and users cannot enjoy both at the same time.

2.3 Greater Advertising Capacity

Another important enhancement in this new version is the greater advertising capacity, which means a lot to the most important and successful application scenario of BLE: beacon-based service.

One classic application scenario of BLE is that a Bluetooth or merely a BLE device works in a broadcasting way, such as iBeacon [18], and users equipped with other Bluetooth devices walk near it and get information such as localization or advertisement from it.

However, due to the limitation of advertising capacity, devices can send very little information at one time. Nevertheless, for broadcasting information, receivers need to establish connections with the beacon device, which slows down efficiency.

Bluetooth 5.0 adopts many updates to overcome these inconveniences. It greatly increases BLE's practicality through the eight times advertising capacity and makes a step forward toward connectionless advertising.

The feature that corresponds to this enhancement is LE Advertising Extensions. In more detail, Bluetooth 5.0 redesigns a whole system for advertising, including extending new advertising channels, accordingly extended new Protocol Data Units (PDUs) [38].

Comparing Bluetooth 5.0 to Bluetooth 4.x versions, we find that the most remarkable difference regarding the functionality of advertising is the number of channels for this purpose.

As mentioned earlier, BLE divides the 2.4GHz ISM band into 40 subbands. In Bluetooth 4.x versions, advertising events are performed on only 3 of 40 channels, and the other 37 channels are reserved for data transmission. However, in Bluetooth 5.0, the other 37 channels can also be used

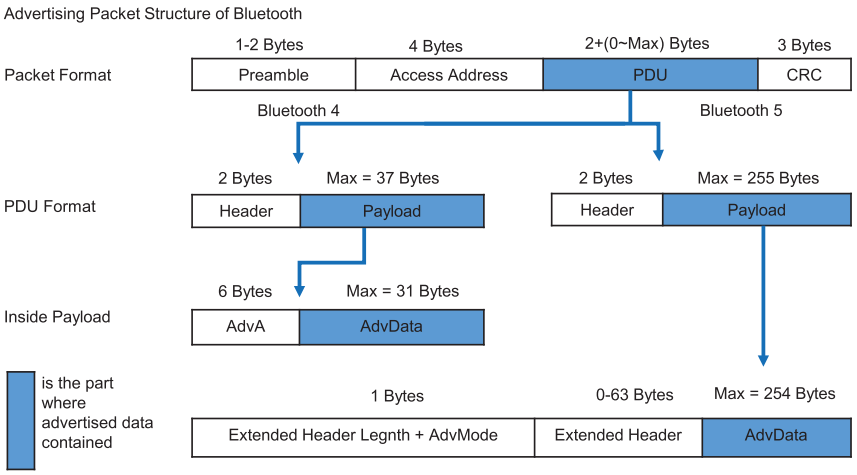

Fig. 5. Formats of advertising packets in Bluetooth 4 and 5 [38].

for advertising. Bluetooth 5.0 treats the original 3 advertising channels as primary channels and further sets the other 37 channels as secondary advertising channels.

With new channels having been brought in, the new PDUs shall be designed to fully use them. In Bluetooth 5.0, several extended advertising PDUs are added, targeting at better performance on broadcasting. Specifically, new PDUs allow two unsynchronized Bluetooth devices to exchange data and eliminate the need for pairing when broadcasting. Thus, the efficiency for receiving Bluetooth beacons is greatly increased, and connectionless advertising can be realized.

Besides new channels and new PDUs, the packet formats of those new PDUs are not identical to others. As shown in Figure 5, in a packet of Bluetooth, there are a preamble, an access address, a PDU, and a CRC. Inside the PDU, there is a header and an actual payload. Bluetooth raises the size of a usable advertising message from 31 to 254 bytes.

2.4 Strengthened Robustness

Although not mentioned in official announcements or promoted as a selling point, robustness is also strengthened in Bluetooth 5.0. There are two new features not yet discussed: Slot Availability Mask (SAM) and LE Channel Selection Algorithm #2.

ASAM is a new scheme for two Bluetooth devices to share their available time slots for transmission and reception. Such functionality is quite useful in practice. For instance, Wi-Fi and Bluetooth coexist on many devices, especially on smartphones. As one part of Wi-Fi shares the same 2.4GHz ISM band, collisions in the same band occur when both of them are working. In addition, sometimes one needs to wait for the other to finish using a Microcontroller Unit (MCU). Bluetooth has schemes to prevent such collisions with its colleague Wi-Fi, but it does not do what its paired device are doing. SAM provides a way for two Bluetooth devices to inform each other when they are available.

dditionally, for a Bluetooth device paired with several other Bluetooth devices, it needs to arrange the time slots for them, telling them when to exchange data. SAM helps a Bluetooth device coexist with the other Bluetooth devices and reduces the chance of collision with other technologies working in the same band, which improves signal transmitting efficiency in the crowded ISM band.

LE Channel Selection Algorithm #2 is an enhanced version of Channel Selection Algorithm #1. Compare d to algorithm #1, which only supports channel selection for connection events,

algorithm #2 adds support for periodic advertising events. And algorithm #2 use a different method (we will not go deeply into the details of the algorithm) to generate the next channel index. Algorithm #2 provides better pseudo-randomness for selecting the next channel, which helps Bluetooth devices coexist better with other devices utilizing the same ISM band.

Additionally, the higher output power can also contribute to stronger robustness, more or less. Raised transmission power leads to raised SNR in the same range when its value does not exceed the upper bound.

2.5 Conclusion

As discussed earlier, through newly introduced features, Bluetooth 5.0 achieves full enhancements over aspects such as speed, coverage, advertising capacity, and robustness.

Bluetooth 5.0 specifically optimizes its BLE mode, which has already gained the advantage of low power consumption, strengthening it with choices on faster speed and longer range. In the most successful application field of BLE, Bluetooth 5.0 greatly improves its usability to guarantee its supremacy. And as usual, efforts for better coexistence with other devices are made, aiming for a better user experience.

Apart from the enhancements discussed previously, researchers also have shown that Bluetooth 5.0 can be more energy efficient than previous versions. It achieves higher speed or extended range while maintaining or even reducing its power consumption [3].

Bluetooth 5.0, as said in the work of Collatta et al. [3], has made a concrete step forward toward the IoT.

3 BLUETOOTH MESH: A NEW PARADIGM

Bluetooth-based networks have long suffered from the lack of extensibility and short coverage. As a low-power wireless technology working in a 2.4GHz ISM band, it is physically impossible for its segnals to go very far away without relaying, which limits its usage in applications requiring wide coverage, such as industrial and agricultural scenarios [27]. Apart from that, a limitation of seven slave devices for one master device also restricts Bluetooth deployment in device-intensive applications.

One way to overcome these weaknesses is by adding mesh topology. Mesh topology enables devices to communicate with each other and allows messages to be relayed. With mesh, coverage can be extended and massive connections can be established. In addition, compared to the star topology, mesh topology can suffer less damage when its nodes fail, increasing the reliability of networks, as shown in Figure 6.

Therefore, plenty of research has been done to realize mesh functionality for Bluetooth [4], and products using BLE-based mesh networks (e.g., Wirepas Pino, CSRmesh, nRF OpenMesh) have appeared in application scenarios like home automation, where massive connections or wide coverage are required. But the absence of official support on mesh topology still was thought to be one major defect of Bluetooth.

Meanwhile, other technologies supporting mesh topology get the chance to step in, such as Z-Wave and IEEE 802.15.4–based technologies like ZigBee and Thread.

Therefore, this official mesh is important to both the IoT area and Bluetooth technology itself. In this section, we start by introducing the basic concepts of Bluetooth Mesh. After becoming familiar with basic terms, unique mechanisms designed in this specification are presented, including its managed flooding mechanism and asymmetrical structure. In addition, as the network security of IoT is getting more and more attention, we provide a brief study on the security mechanism of Bluetooth Mesh. A toy example to show how Bluetooth Mesh works ends this section.

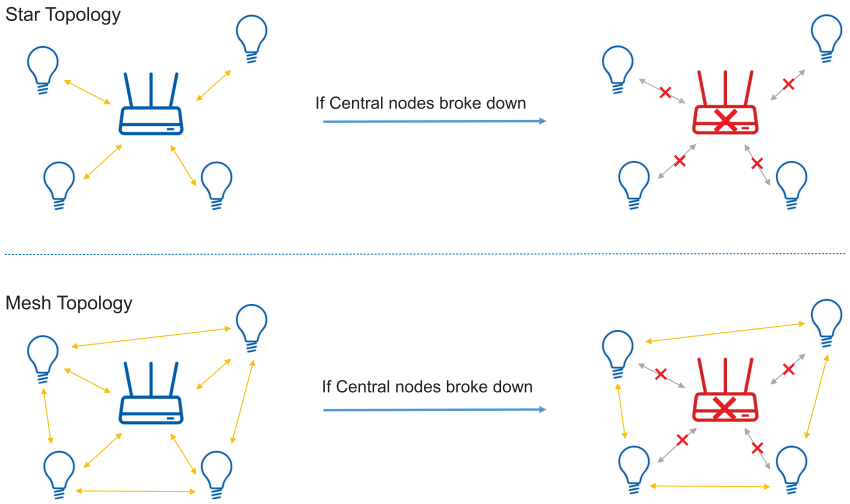

Fig. 6. Star topology vs. mesh topology.

3.1 Basic Concepts

In this section, we introduce the basic concepts of Bluetooth Mesh through three questions:

- What are the basic units of Bluetooth mesh networks?
- How do devices communicate with each other in Bluetooth mesh networks?
- How can a new Bluetooth device be added to a Bluetooth mesh network?

Through these questions, we can see how a normal Bluetooth device gets added to a Bluetooth mesh network, how it does basic works, and the terms used in this procedure.

3.1.1 What Are the Basic Units of Bluetooth Mesh Networks? Generally, mesh networks are made up of devices that are capable of communicating with each other besides their basic functionalities. To properly organize these functionalities, a layered structure is designed for units that form a Bluetooth mesh network, as illustrated in the upper left part of Figure 7.

Each device contained in Bluetooth mesh networks is referred to as a node. Normally, a node corresponds to one Bluetooth chip module. However, it is possible for there to be multiple parts connected to and controlled by one chip module. Thus, there is a smaller unit, an element, defined to describe those parts.

An element is the smallest physical unit in Bluetooth Mesh. And since one element can serve different purposes, another two terms, *model* and *state*, are proposed for organizing those functionalities. One model represents one functionality of an element. And inside a model, there will be one or several states to measure its condition.

Let us take the lamp group drawn in the right part of Figure 7 as an example. The lamp group is abstracted as a node in Bluetooth mesh networks. Three lamps are contained in the group and abstracted as three elements. For each lamp, besides the basic functionality lighting, there may be some other functionalities, such as measuring the light intensity of nearby environments. Thus, several models are designed for elements. For example, a model of measuring light environment, it can contain states such as brightness, which measures how bright the lamp shines.

In addition, it is inefficient to abstract all Bluetooth devices as nodes identical in status. Normally, Bluetooth devices inside the same networks do not have the same processing ability, power

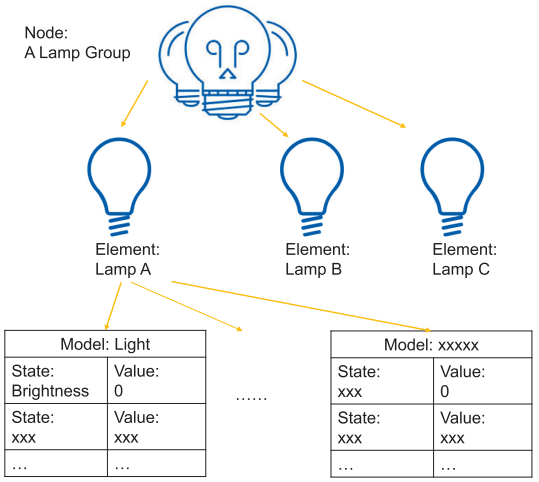

Fig. 7. Structure of the basic unit of Bluetooth Mesh and a naive sample.

supply condition, and many other aspects. Thus, these devices cannot be fully utilized if uniformly abstracted as nodes, and ways need to be found to distinguish nodes with different conditions.

Besides basic communication functionalities, several additional features are designed for fully utilizing different nodes. Currently, there are four additional features (which will be discussed in detail later). Each node can selectively choose to support and enable zero or more of these features.

Thus, it is heterogeneous nodes containing one or more elements that form Bluetooth mesh networks.

3.1.2 How Do Devices Communicate With Each Other in Bluetooth Mesh Networks? Nodes of Bluetooth mesh networks communicate with each other through messages in an advertising manner, which means that besides content, a message contains the address of the sender node and its intended receiver node and some other control fields.

Depending on whether responses are needed, messages can be divided into acknowledged ones and unacknowledged ones. As the name suggests, acknowledged messages need their receivers to send responses back, whereas unacknowledged messages just need to be sent out.

Additionally, addresses need to be included in messages so that devices can know where they are from and where they are going. Three kinds of addresses are defined in Bluetooth Mesh: unicast address, group address, and virtual address.

Any single element will be assigned a unicast address when added to a network. It is like the ID number of an element. Suppose that the user of the lamp mentioned earlier wants to specifically open or close one of the three arrays; he or she can send a message carrying that order to its unicast address.

Depending on how users organize them, elements may be assigned virtual or group addresses later. For instance, lamps in the same room (e.g., a dining room) may be organized as a group and share one group address called *dining room*, as pictured in Figure 8.

In Bluetooth Mesh, the activities of sending or receiving messages are called *publishing* or *subscribing*. Subscribing refers to nodes receiving messages and processing only those from configured addresses, and publishing is the act of sending a message.

Combing these mechanisms, we can picture how users control certain nodes or elements. Imagine that there is a building with multiple meeting rooms. Each of them has several lamps, and all of those lamps are managed by a smart light system based on Bluetooth Mesh. To manage those

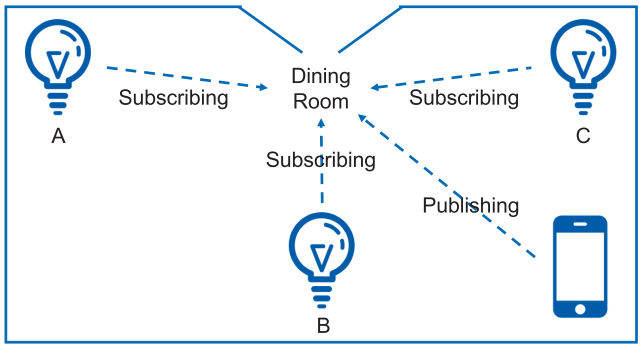

Fig. 8. Example of subscribing and publishing manners.

lamps, the system can be configured as follows. Lamps in the same room share one group address and subscribe to this address. If a manager wants to turn one room's lights off, he or she can use a connected controller to publish an OFF message to the corresponding group address and then all the lamps will be turned off. Specifically, if he or she wants to turn only one lamp on, he or she can use its unicast address.

3.1.3 How Can a New Bluetooth Device Be Added to a Bluetooth Mesh Network? The procedure of adding one new Bluetooth device to a Bluetooth mesh network is called *provisioning*. The node that helps this new device become a new node is called the *provisioner*. There are five stages to finish this procedure: beaconing, invitation, exchanging public keys, authentication, and distribution of the provisioning data.

The first two stages are like a customer coming to a restaurant and asking for service. He or she starts by calling for service, which is *beaconing*. Then an appropriate waiter or waitress comes and asks what the customer wants, and he or she responds with the corresponding information. Exchanging public keys and authentication are the security mechanism performed for adding a new node.

After the preceding stages, the last one, the distribution of the provisioning data, is conducted to finish the provisioning procedure and mark the acceptance of a new node. With the provisioning procedure finished, the new Bluetooth device gets accepted as a new node in the Bluetooth mesh network and can perform communication functionality according to its settings.

3.2 Managed Flooding

One major concern of mesh networks is how relaying is handled. Commonly, there are two categories: flooding based and routing based. Both have been adopted in Bluetooth in non-official versions of BLE-based mesh networks. A comparison over those two categories is performed in the work of Murillo et al. [24], which claims that flooding can get a lower end-to-end delay with a price of higher power consumption.

The scheme that Bluetooth Mesh adopts is an optimized flooding approach called *managed flooding*. Flooding is more simple in practice and has lower latency. But it can generate a heavy burden for the network if not carefully designed [46]. Thus, several approaches are adopted to do optimization.

First, we describe the heartbeat scheme. A node advertises heartbeat messages periodically so that other nodes know it is active. In addition, based on the data contained, other nodes can infer how many hops will need to send messages to it.

Second, a specifically designed value called *Time to Live* (TTL) is contained in all Bluetooth mesh messages to tell receivers that how many times a message can still be published. For example, when a node receives a message with a TTL number of 3, it first minuses it by 1 and gets 2, then the message can be relayed twice again until it is received by the right receiver. Thus, with a TTL number reduced to zero, the travel of the message will be ended right now.

The existence of TTL shows the importance of heartbeat messages. As mentioned, heartbeat messages contain data for nodes to infer how many hops will be needed if they want to communicate with the sender. Therefore, it helps nodes correctly set the TTL number. If the number is too high, it decreases the efficiency of the whole mesh network. And if the number is too low, messages may not be able to get to their destination.

Third, a message cache is set on each node to store recently received messages. As in flooding-based mesh networks, messages can be sent via many different ways. Suppose that the TTL number is high enough, and there is a circle where three nodes, A, B, and C, are located. Every node is within the coverage of the other two nodes. Then if node B publishes a message to node A, node A will receive a message directly from node B and another one relayed by node C. Thus, with a message cache for storing, it can be judged whether a message has been received before. And if so, the receiver can just discard it to avoid reprocessing, improving the network's efficiency.

Currently, there are no routers, routing paths, and routing algorithms employed in Bluetooth mesh networks. But routing functionality, as said in the specification, will be considered in future versions [8].

3.3 Asymmetrical Structure

To improve the performance of mesh networks, nodes are heterogeneous in Bluetooth Mesh. As mentioned earlier, given nodes with different conditions, it is natural to design an asymmetrical structure in Bluetooth mesh networks. To fully utilize different kinds of Bluetooth devices, their conditions, such as the power supply and processing ability, must be considered. For example, users cannot count on a tiny Bluetooth beacon that is powered by a coin cell to serve well as a node that can both advertise location information and relay messages for others.

According to its usage and physical constraints, a node may optionally support none or a few of the four features: relay, proxy, friend, and low power.

The relay feature is the most basic additional feature designed in Bluetooth. It allows nodes to relay messages for others, which achieves the larger coverage and higher reliability of mesh networks. Of course, the TTL number of received messages shall not be larger than zero. But it should be noted that the relay feature is not mandatory for nodes. In Bluetooth Mesh, some nodes are not suitable for relaying messages and serve at the edge of mesh networks.

The proxy feature enables a node to serve as the translator between nodes of Bluetooth mesh networks and Bluetooth devices outside. Currently, the majority of Bluetooth devices are still using Bluetooth 4.x versions and have not upgraded to support Bluetooth Mesh. Thus, the proxy feature is designed for adding these devices into mesh networks. Specifically, two bearers are designed for describing different messages transmitted in mesh networks. One is called the *GATT bearer*, which is for communicating inside mesh networks. And another is called the *ADV bearer*, which is for old BLE devices.

For example, an old sensor that uses Bluetooth 4.0 and does not support Bluetooth Mesh can send its messages to a lamp with the proxy feature. After receiving messages from the sensor, the lamp retransmits these messages by publishing them in formats defined in Bluetooth Mesh. And as we can see, a node with a proxy feature must have the relay feature as well.

Low power and friend are a couple of pairwise features. Some nodes are very sensitive to power consumption, such as beacons that are powered by coin cells. And certainly it is not necessary and

is extremely inappropriate to frequently acquire such kinds of nodes. As a matter of fact, due to the flooding mechanism, nodes need to keep on scanning different channels, which greatly damages the practicability of power-sensitive nodes.

Considering that, Bluetooth Mesh designs the low power feature to reduce the duty cycle and thus realize power reservation. Nodes with a low feature do not need to be active frequently but only need to wake themselves as programmed and receive messages at the working time.

However, such a manner risks missing vital messages. With a lower duty cycle, it will have a higher possibility of losing messages sent to it. As a complement, the corresponding feature, the friend feature, is introduced.

The friend feature enables a node to form a relationship called *friendship* with nodes with a low power feature. Nodes with the friend feature can store messages for related low-power nodes and relay those messages when needed. Thus, a message sent to a low-power node will first be stored in the correspondent friend node. And when the low-power node is active, it will receive the message from its friend node. In addition, a friend node needs to undertake the due obligations for relaying messages from its low-power nodes. Therefore, friend nodes also need to have the relay feature.

3.4 Network Security

With more and more devices coming into and getting closer to our daily life, security issues become a more severe issue in the IoT area [47]. As for Bluetooth, studies on its security issues have been conducted [9, 14] and designs for resisting attacks have been considered [7, 23] since almost as early as the release of its first version.

Considering the application scenarios of Bluetooth Mesh, the issue becomes more vital. It cannot imagine what the consequence will be if a home automation system or an industrial control system is controlled or damaged by hackers. Therefore, in Bluetooth Mesh, the security system ihas a dedicated design.

Unlike being optional in previous specifications, in Bluetooth Mesh, security is mandatory and cannot be switched off. Bluetooth Mesh provides a whole-process security design, from adding a new device to processing messages.

First, we discuss securing the process of adding a new device. It is known to all that the easiest way to capture a fortress is from within. Thus, to protect mesh networks, the first thing is to keep hostile devices out. The provisioning process mentioned earlier adds two steps for security: exchanging public keys and authentication. A device needs to pass authentication before being added. This increases the difficulty of hostile devices being wrongly accepted.

Second, we describe securing the communication process. As messages are transmitted through the air in wireless communication, they can easily be captured by any device in the coverage area. Thus, it is necessary to encode messages. In Bluetooth Mesh, all messages are encrypted with AES-CCM using 128-bit keys. And to further improve privacy, messages are also obfuscated so that nodes cannot be easily tracked.

Third, we discuss securing messages so that they can only be processed by the right receivers. As in mesh networks, a message normally is not directly sent to its destination. Therefore, it will be received by several nodes during its whole journey, which makes it important to prevent messages from relay nodes. Bluetooth Mesh provides a two-layer security mechanism [5], where two keys are designed for protecting messages in networks and applications, respectively. The network key is the key used for securing messages in transmission and is acquired by all nodes inside the same network. Receivers use it to decode received raw messages. But for correctly decrypting the information inside, the application key is necessary. Imagine that there is an attacker who successfully disguises itself as a relay node. Then when it gets added to the network, it suddenly possesses the

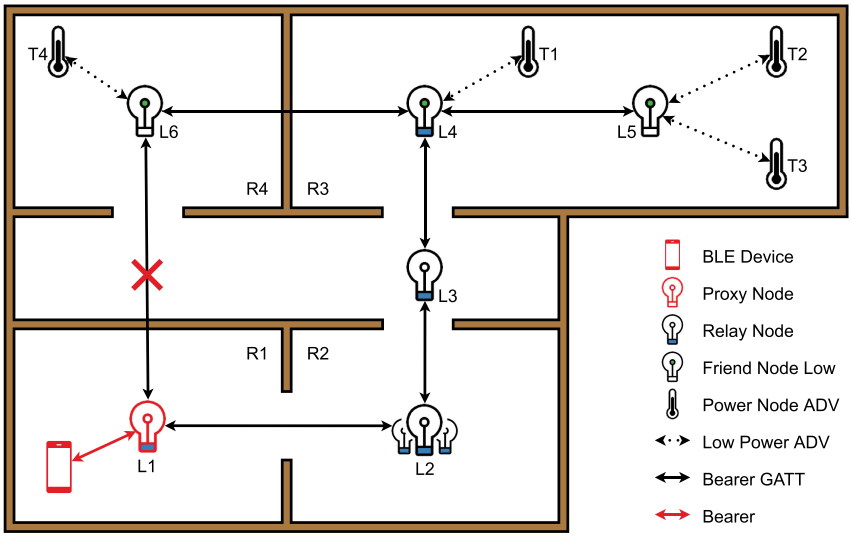

Fig. 9. Example topology of a Bluetooth mesh network [8].

network key. But it needs to find other ways to decode messages for certain applications without correspondent application keys. Actually, there is another key, called the *device key*, which is only possessed by a node and its provisioner.

Meanwhile, besides those mechanisms, Bluetooth Mesh has also prepared for some typical types of attacks. For instance, trash attacks can use information stored in an abandoned node, such as network keys, or reactivate the node as an attacker. To resist trash attacks, if a node is removed, the provisioner will put it into a blacklist and start a key refresh procedure to change the keys that the node has ever processed. It is like when an intelligence agent is relieved of duty, he or she will not be allowed to access confidential information and codes used by him or her are replaced. In addition, replay attacks are also targeted through the sequence number and the index number. Only when those two numbers get matched as calculated can a message be thought as a safe message for further processing. Otherwise, it simply gets dumped.

3.5 A Toy Example

A toy example of a Bluetooth mesh network is illustrated in Figure 9. We show a hypothetical floor plan for one floor of a building, which contains four rooms and a corridor. The lamp is one piece of basic equipment in each room for lighting. Normally, each room has at least one lamp, and in some rooms, there are thermostats for controlling temperatures. All lamps and thermostats on this floor form a mesh network using Bluetooth. This is a typical scenario in a smart home.

The example is illustrated through a process that a user wants to adjust the temperature of room R4 using thermostat T4 and changes the setting of it. To communicate with thermostat T4, the most direct way is to pass through lamp L1 and lamp L6, and arrive at T4. However, somehow, this shortest way may be blocked due to obstruction of walls and distance, or possibly a microwave oven is in the way. Thanks to mesh, the procedure can still choose another longer way. In this situation, relay nodes L2, L3, and L4 can help establish a communication path between the user and thermostat T4.

Starting from room R1, the user uses a smartphone that does not support Bluetooth Mesh but is equipped with Bluetooth 4.1. As a device that does not support Bluetooth Mesh, the smartphone needs to find a proxy node to serve as its translator. Lamp L1 is this proxy node. It receives messages

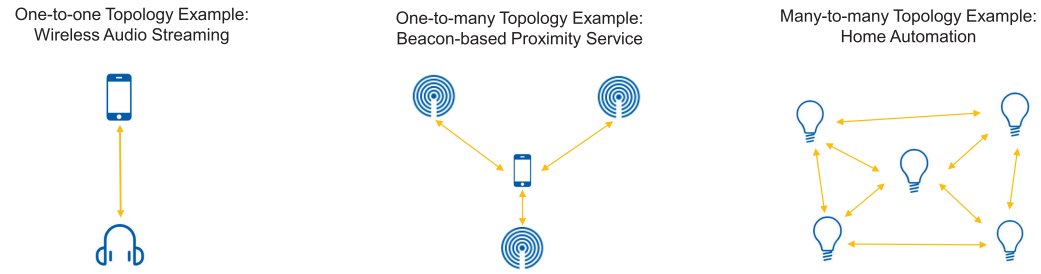

Fig. 10. Three examples of three kinds of topologies of Bluetooth.

from the smartphone through GATT bearers and relays for it using ADV bearers, publishing them to the whole mesh network.

The second station is lamp L2 in room R2. L2 is a lamp with three bulbs, which can be abstracted as a node with three elements. If the user wants to separately control three bulbs, he or she can do so through correspondent addresses.

L3 in the corridor is a pure relay node and contains only one element in this situation. Therefore, it only processes a network key for transmitting messages in this network and a device key of itself.

In the larger room, R3, there are two lamps: L4 and L5. They serve as friend nodes to thermostats T1, T2, and T3, which are abstracted as low-power nodes. L4 and L5 can subscribe messages sent to one group address so that if the user wants to, he or she can control them simultaneously through this group address.

The last room, R4, has one friend node, lamp L6, and the desired low-power node, thermostat T4. That is how this controlling procedure is done.

However, in a simple toy example, it is hard to demonstrate the complete picture of Bluetooth Mesh specification. In this example, it does not consider new features of Bluetooth 5.0, such as a larger transmission range. Considering an application requiring house-level coverage, it may only need star topology with a quadrupled range. And in the future, Bluetooth Mesh, together with Bluetooth 5.0, can provide connection services for applications requiring much larger coverage.

4 APPLICATION SCENARIOS: HOW THEY WILL BE INFLUENCED BY THE NEW BLUETOOTH

We introduced the new Bluetooth in the preceding sections. Now it is time to think about how enhancements to Bluetooth will influence the IoT area. In this section, we will see this question in the perspective of applications.

Bluetooth is one of the most successful wireless technologies existing in IoT markets. However, its application range is limited due to hardly extendable coverage and network capacity. Normally, it is used in direct communication between two devices and broadcasting, which can be summarized as one-to-one topology and one-to-many topology applications, respectively. We draw two examples, as presented in the left and middle of Figure 10 (e.g., wireless audio streaming and beacon-based proximity, which are typical representations of applications using such topologies). And now, with the support for mesh topology, the range of Bluetooth-enabled applications is further extended to many-to-many device communication applications, such as shown in the right example in Figure 10 (e.g., home automation).

In this section, we discuss in detail how the enhanced Bluetooth will affect its application range. Specifically, we categorize those applications based on their topologies, such as one-to-one topology, one-to-many topology, and many-to-many topology. For each, we provide one or two examples to better explain how Bluetooth can promote them.

4.1 One-to-One: Paired Devices

One direct benefit of the new Bluetooth is the more powerful communication link for paired devices using Bluetooth. It is known to all that Bluetooth prevails in short-range, low-data-rate, one-to-one device communication. Due to the limited power supply, most wearable devices, such as smart watches and wireless earphones, are using Bluetooth for communication with cell phones or other devices. This prevalence can be maintained due to the enhanced performance of Bluetooth. However, how much they can benefit from the new Bluetooth depends on which mode they use: BR/EDR or BLE.

For those using BLE, all of the new features introduced in Bluetooth 5.0 can be enjoyed. Consider the smart watch as an example. The doubled data rate almost halves the time required for activities like transferring data or updating the firmware. Therefore, it needs less active time to accomplish the same amounts of work, which leads to increased battery life. And with the quadrupled transmission range, users can have a much wider free space. At least he or she can be totally freed from his or her cell phone in a house that is not very big.

For those based on BR/EDR, the new Bluetooth is almost the same as the previous Bluetooth 4.2. But they can at least enjoy the higher output power and SAM. For example, consider wireless music streaming. We know that most wireless headsets and earphones use Bluetooth for streaming audio. At least higher output power gives a wireless headset another choice when its user is farther from the source (usually a PC or a cell phone) than before, except reminding him or her that he or she is out of range. And SAM can help to deal with situations where plenty of other Bluetooth devices are coexisting together, such as on a train.

In conclusion, for applications using Bluetooth to perform one-to-one communication, with Bluetooth 5.0, they can enjoy faster speed and longer range while keeping performance quality uninfluenced or get a more stable high-quality communication service than before.

4.2 One-to-Many: Proximity Beacons

One practical and classic example of applications forming one-to-many topology using Bluetooth is beacon-based proximity. Representative products include Apple's iBeacon and Google's Eddystone.

Its working mechanism is just as the name *beacon* suggests. For instance, iBeacon devices continuously broadcast their IDs and contained information to neighbor devices. End users then collect multiple IDs for localization based on their distances or angles to these iBeacon devices. And companies can further provide location-based services, such as navigation, on beacon-based proximity.

The larger advertising capacity enables beacons to carry more detailed information along with their IDs. Consequently, beacon devices can now provide various context-rich location-based services. For example, devices deployed in a shopping mall can advertise discounts to customers when they are close to the corresponding shops.

In addition, we know that Bluetooth is widely used in indoor localization applications. One of the major approaches adopted in indoor localization is the fingerprint-based scheme [44], which generally measures and collects signal indexes from several different signal sources (e.g., iBeacons) to form a fingerprint database. Then suppose that if a user comes in, he or she can collect the same signal indexes and match them to the database to get his or her location.

4.3 Many-to-Many: Meshed Objects

The support for mesh topology, an important new feature of Bluetooth 5.0, extends the applications of Bluetooth to many-to-many device communication. Smart homes/offices and industrial controls are two promising scenarios in the era of IoT.

4.3.1 Smart Homes/Offices. Various IoT devices have been designed and deployed in household and office environments in the vision to serve the residents inside those environments seamlessly and intelligently. Examples include robot cleaners, smart lighting, and Amazon's Echo.

Seamless smart home and office services require reliable and energy-efficient connections among heterogeneous IoT devices within and across rooms. The required data rate may vary from several kilobytes per second for periodic temperature/humidity queries to tens of megabytes per second for real-time audio and speech transmissions. User commands and device feedback may need to be delivered inside the entire building despite blockage of furniture, walls, and floors. In addition, many appliances, such as wireless environment monitors, are expected to operate on low power.

However, Bluetooth was not the first choice in sensor-rich applications due to its small network capacity. Consider building automation as an example. It is quite normal to see plenty of sensors and controllers spreading inside whole buildings. However, with a maximum of seven devices in a Bluetooth-enabled star topology network, it may not be able to cover a conference room. Of course, Bluetooth could form a layered tree-like structure using the star topology, but it could greatly add complexity.

Now with Bluetooth Mesh, Bluetooth finally has a good chance of being applied in such applications. And due to some advantages, Bluetooth can even be a later but more competitive player.

ZigBee has long been considered ideal for smart home and office applications, yet Bluetooth Mesh may take over. On the one hand, most laptops, tablets, and smartphones are equipped with Bluetooth. It is convenient for end users to control and manage their smart homes/offices on these smart devices and via Bluetooth. With ZigBee, however, extra hardware is needed. On the other hand, Bluetooth provides higher data rates than ZigBee while using similar energy consumption. Bluetooth holds promise in meeting the increasing popularity of audio-based commands, which requires a data rate prohibitive for ZigBee.

4.3.2 Industrial Control. Industrial control is another promising market of Bluetooth Mesh, where less user interaction is involved but more devices need to be connected effectively. Compared to smart homes/offices, industrial control has stricter demands on energy efficiency and reliability.

Energy efficiency affects the production efficiency in industrial control. The power consumption of Bluetooth Mesh is reduced even more than with BLE, with the design of friend and low-power nodes. Devices in Bluetooth mesh networks can serve different roles depending on how they are powered. Devices with sufficient power supply can serve as friend nodes, whereas battery-powered devices can be set as low-power nodes.

Network reliability is also vital in industrial applications. Bluetooth resists interference with frequency hopping and a coding scheme, which reduces the probability of packet loss or errors and also can tolerant more devices working together.

Compared to other mesh networks using routing algorithms, Bluetooth mesh networks eliminate the need for routing tables. Thus, theoretically, messages can be sent to any corner as long as they have enough TTL and at least one physical link exists. Therefore, Bluetooth Mesh is more reliable than routing-based networks when nodes fail.

5 COMPARISON: BLUETOOTH VS. ITS COMPETITORS

Normally, communication technologies are application oriented, which means that they are proposed for addressing the requirements of certain applications. For example, Bluetooth was first proposed for providing a short range wireless alternative to RS-232 cables, whereas ZigBee was proposed for enabling low-power and networked devices [2]. However, with constant updating,

Table 2. Comparison Among Bluetooth 5.0, Bluetooth 4.2, and Other Typical Wireless Communication Technologies

Technology		Bluetooth		Wi-Fi	ZigBee	Z-Wave
		BLE 4.2	BLE 5.0			
Speed	Maximum Data Rate	1Mbps	2Mbps	600Mbps	250kbps	40kbps
Coverage	Transmission Range (Indoor)	10–20m	40m	<50m	10m	30m
	Mesh Support?	No	Yes	No	Yes	Yes
Energy Efficiency	Battery Life	High	High	Low	High	High
Accessibility	Existence in Cell Phone?	Yes	Yes	Yes	No	No
Cost	Module Price	$1–$5	$5–$10	$5–$10	$1–$5	$1–$5
	Additional Router	No	No	Yes	Yes	Yes
Network Capacity	Maximum Number of Nodes	8	32,767	255	>65,000	232

suitable fields of one communication technology will be expanded. Just as discussed earlier, due to improved performance and new features, there are some new application fields in which the new Bluetooth can be adopted, such as home automation.

However, applications new to Bluetooth are not new to all. For example, Wi-Fi, Z-Wave, and ZigBee are widely used in building and home automation [15]. Therefore, before deploying the new Bluetooth in such applications, how well it actually performs against those competitors has yet to be evaluated.

After the qualitative discussions on how the new Bluetooth will influence Bluetooth-related IoT applications in Section 4, in this section we take a quantitative perspective, comparing it to its predecessor and competitors both theoretically and experimentally.

In the theoretical evaluation, we focus on aspects that are frequently considered in new application fields of Bluetooth, such as home/building automation. Typical wireless communication technologies adopted in applications like Wi-Fi, Z-Wave, and ZigBee are compared to Bluetooth 5.0 and Bluetooth 4.2. Through this, we try to see how enhancements of the fifth generation will alter the relative strength of Bluetooth and its competitors.

After that, the performance of the new Bluetooth in real scenarios is tested with regard to throughput and distance. Apart from that, we have also surveyed experimental tests conducted by previous works for measuring the new Bluetooth.

Results and discussions are presented in following sections.

5.1 Theoretical Evaluation

The results of parameter evaluation on IoT-related aspects are listed in Table 2. Discussions over these aspects are presented as follows.

5.1.1 Speed. Considering the on-air data rate, Wi-Fi ranks at the top and is much higher than the rest. Bluetooth 5.0 doubles its max data rate and widens the gap between it and ZigBee. Z-Wave has the smallest data rate in Table 2.

The data rate is one important parameter when selecting communication technologies. Depending on how services are conducted, different data rates can suit different levels of messages, such as text level, voice level, image level, or video level. A higher data rate means more choices and quicker time for completing tasks. For example, with an upper-bound data rate as low as 40kbps,

Z-Wave can only afford to transfer small packets of data. And Wi-Fi is the priority choice for transferring videos, if needed.

However, it should be noted that the data rate is not equal to throughput, as many factors will lead to a shorter value, such as the time interval between two packets and waiting time for responses. Moreover, even in a 100% duty cycle without ACKs, the on-air data rate is unreachable because the actual payload only consumes part of a packet. Throughput will be evaluated in the experimental evaluation.

Of course, for building and home automation, a very high data rate is usually not required. And a higher data rate normally represents larger bandwidth and a more complex modulation scheme, which leads to higher energy consumption and more expensive hardware. Therefore, developers will make choices depending on demand.

5.1.2 Coverage. The transmission range influences the important coverage problem when deploying IoT devices. Especially for those using the star topology, the transmission range simply decides the coverage of one wireless network. Of course, for mesh-based technologies, it can acquire larger coverage through relaying. But relay will introduce an increase in time latency and cost. Placing one device every 1m and placing one device every 10m to fully cover the same building are fundamentally different in practicability in most applications.

Considering one-link transmission, Wi-Fi outperforms others and Bluetooth achieves an increase through new coding schemes. Z-Wave and ZigBee have a short transmission range, but they can achieve large coverage using mesh topology. Therefore, for home automation, Bluetooth was unsuitable previously because it not only could only transmit a short range but also lacked mesh functionality. The transmission range of Bluetooth will be evaluated in the experimental tests.

Mesh topology enables wireless signals to be relayed. In wireless communication, the transmission range of a single link is highly restricted. Signal strength simply decreases with distance, not to mention obstacles. Therefore, to cover a very large area, support for mesh topology is required for technologies without base stations. In Table 2, only Wi-Fi does not support mesh. But thanks to its relatively long transmission range, it remains suitable in houses that are not very large.

5.1.3 Energy Efficiency. Energy efficiency means a lot to the user experience. We use battery life to measure it, as battery life represents how long a certain IoT device can keep working with one or two standard batteries directly influences the feeling of its users on its energy efficiency. Especially for battery-powered devices, battery life influences the frequency of recharging or replacing batteries. And no one wants to change batteries every few hours.

Wi-Fi is much more power consuming than others, as sending an OFDM-modulated large-bandwidth signal consumes much more power than a simple FSK-modulated small-bandwidth one. BLE, ZigBee, and Z-wave claim to be low-power communication technologies with battery life levels of months to years. They are designed for devices that work in a low duty cycle and generate very small amounts of datasuch as sensors for monitoring various environmental indices.

5.1.4 Accessibility. Existence in cell phone can improve competitiveness of one certain communication technology regarding convenience. One simple fact is that most people today have at least one cell phone. And because almost all cell phones are equipped with Bluetooth and Wi-Fi, there is no need to purchase and take an extra controller for users of IoT systems that use Bluetooth or Wi-Fi to control and communicate.

Apart from that, existence in cell phone also makes it much more convenient to collect Bluetooth and Wi-Fi signals than ZigBee and Z-wave, which makes them better choices in serving data-driven applications and applications requiring massive deployment. For example, as the cell phone

gradually becomes a necessity in modern life, it is rather convenient to collect Wi-Fi and Bluetooth signals to serve as signal maps for localization and navigation [40, 41].

5.1.5 Cost. Cost is also considered in IoT applications, especially when there are plenty of IoT devices. Two factors mainly influence the cost in the users' perspective.

One factor is the unit price of each module. Imagine a skyscraper where tens of thousands of sensors are spreading, and thus the unit price of each sensor matters in terms of budget. We choose the price of one module for comparison. As looked up at Alibaba.com, Wi-Fi and Bluetooth 5.0 modules are slightly more expensive than others. Due to more complex circuits, the cost of producing one Wi-Fi module exceeds others. As for Bluetooth 5.0, it is new and therefore is a bit more expensive than an old one.

Another factor is whether an extra router is required. A "yes" answer means that an extra fee will be paid for constructing a wireless network.

5.1.6 Network Capacity. Network capacity is decided by the maximum number of devices that can be contained in a network. Although Bluetooth can extend its network size through scatternet (a topology formed by layers of star networks), it is hardly considered for connecting a large number of devices. And now with mesh, its theoretical network capacity is greatly enlarged to tens of thousands of devices. Wi-Fi and Z-Wave can support networks containing more than 200 devices, which is shorter than Bluetooth 5.0 and ZigBee but adequate in many home/building-scale IoT applications.

5.1.7 Conclusion. From the preceding discussion, we can see that the most comparable competitor of Bluetooth is ZigBee, as both are low power, low cost, and able to form mesh topology. Due to updates in this fifth generation, Bluetooth now gains mesh functionality, making up for its shortcomings in coverage and network capacity. Furthermore, from a numerical point of view, Bluetooth completely exceeds ZigBee, as it is superior in the data rate, single-link transmission range, and accessibility while being similar in energy efficiency and cost. Therefore, can we just draw the conclusion that Bluetooth will take over ZigBee in overlapped applications? Well, not yet. Simple comparison over claimed parameters is totally not enough. Performance in real scenarios remains to be evaluated.

5.2 Experimental Evaluation

In this section, we evaluate the performance of the new Bluetooth considering two different kinds of connections: single-link connection and networked connection. Due to the limit of experimental conditions, we only conducted part of the experiments and evaluate the new Bluetooth based on results generated by previous works.

To eliminate the influence brought by different hardware conditions, the test board we choose in our tests is the Nordic nRF52840 development board [33] from Nordic Semiconductor, which integrates both Bluetooth 5.0 and ZigBee. During the whole process of testing, the transmission power is set to 0dBm.

5.2.1 Single-Link Evaluation. Several works have been conducted to evaluate the single-link performance of Bluetooth. In the work of Collatta et al. [3], Bluetooth 4.2, Bluetooth 5.0, and IEEE 802.15.4 are measured and compared with regard to power consumption, throughput, and transmission range of each under both LoS and non-LoS conditions. Karvonen et al. [16] focus on enhancements achieved, comparing the performance of Bluetooth 5.0 and Bluetooth 4.2 to figure out the extent of enhancements. Both Baert et al. [1] and Silicon Labs [19] measure the one-hop latency of Bluetooth.

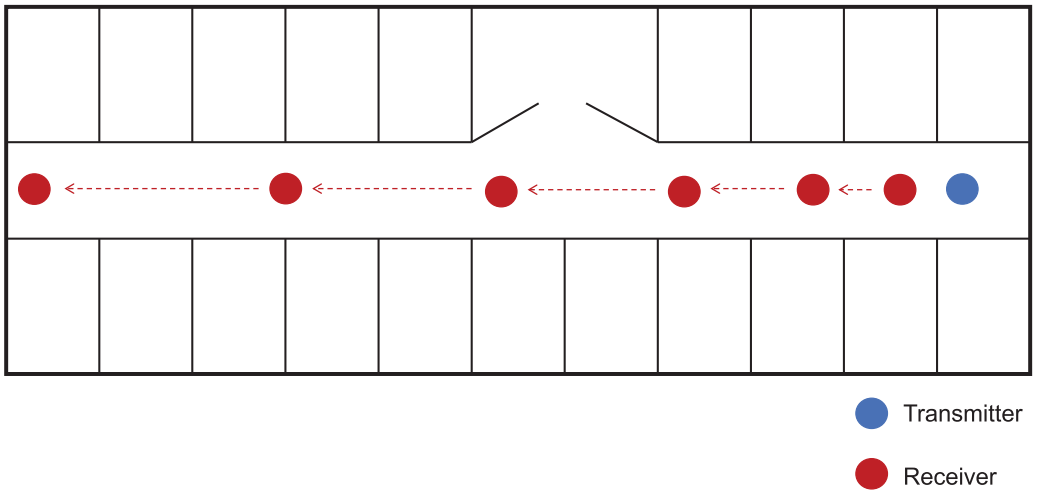

Fig. 11. An abstract sketch of the experimental scenario of single-link evaluation.

Here we measure the single-link performance of Bluetooth and ZigBee in a perspective of related IoT applications, in which the throughput and transmission range are more frequently considered than latency. Considering that we cannot have both a longer range and higher data rate at the same time, different modes of Bluetooth are compared separately. All of the three different PHYs—LE 1M Uncoded, LE 2M Uncoded, and LE 1M Coded ($S = 8$)—are measured together with ZigBee. The firmware is developed based on examples provided in nRF SDK v15.2.0 and nRF SDK for Thread and ZigBee v2.0.0.

Tests are conducted in a corridor of a dormitory, as showed in Figure 11, which is a norm application scenario for a house and building. The payload inside each packet contains 23 bytes, which is an adequate value for common applications. One board is set as a transmitter and marked as the blue point in Figure 11. The transmitter sends one same packet periodically. Another board is set as the receiver and calculates the throughput. The receiver is marked as a red point. We gradually increase the distance between the two boards. Specifically, we measure the throughput when the two boards are 1, 2, 3, 4, 5, 10, 15, 20, 25, and 30 m away.

The result is pictured in Figure 12. Under our experimental configuration, the maximum throughput and maximum distance are concluded in Table 3. For some long-distance situations, the connection between two boards is broken and the corresponding throughput is set to zero. Therefore, we take the distance value where throughput of5 kbps can be achieved. And because of the complex indoor environment, irregular conditions occurred occasionally that when distance gets further, the throughput measured get increased.

As we can see, the results show that different PHYs of Bluetooth perform quite differently over distance and throughput. LE 1M Coded PHY has a rather small throughput but can be received even as far as 50m indoors. Although LE 2M Uncoded PHY starts with a relatively high throughput, it quickly decreases with increasing distance. Therefore, the two modes are proposed for different purposes. As for ZigBee, it is the choice of balance. One interesting thing is that considering ZigBee and LE 1M Uncoded PHY, which represents the old version of Bluetooth, we find that each wins in one aspect. However, with different modes, it seems that Bluetooth gains superiority over ZigBee in the single-link connection.

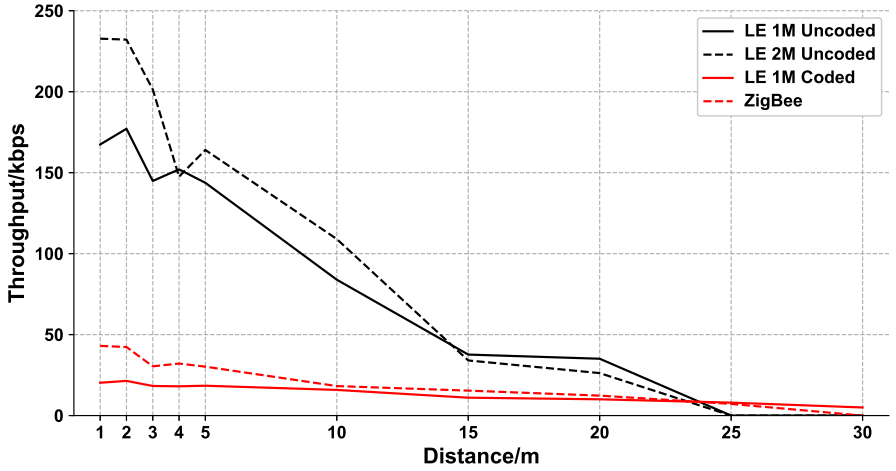

Fig. 12. Throughput measured in different distances.

Table 3. Maximum Throughput and Range Tested in Our Single-Link Tests

Measured PHYs	LE 1M Uncoded	LE 2M Uncoded	LE 1M Coded ($S = 8$)	ZigBee
Maximum Throughput (kbps)	177.10	232.73	21.42	43.28
Maximum Distance (m)	24.2	24.7	>30	28.1

5.2.2 Networked Connection. Next we discuss the performance of networked connections formed by Bluetooth and ZigBee. Due to the limit of experimental conditions, we do not conduct network-level experiments. Therefore, discussions are conducted based on the results generated in other works.

For measuring mesh network performance, some other aspects will be considered. The first aspect is latency. Mesh topology extends coverage through relaying. However, relaying adds latency. With the number of relay increases, the time consumed for transmitting a message from the source to the end might be intolerant for some applications. The second aspect is reliability. With plenty of devices connected together, reliability becomes a more vital problem than how it is in single-link connections due to the increased probability of collision. The third aspect is scalability. How the network performs when its size grows will influence the scale of its suitable applications. For example, for a home-level application, normally a small network containing several devices is enough. But for connecting hundreds and thousands of IoT devices spreading in a skyscraper, only a technology that performs well in large-scale networks can meet the demands.

A thorough comparison over mesh network performance of Bluetooth Mesh and ZigBee has been conducted by Silicon Labs [19]. During the test, they measure throughput, latency, and percentage of the received packet of mesh networks in their lab environment. The scale of networks covers a small one with 24 nodes, a medium one with 96 nodes, and a large one with 192 nodes.

The results show that Bluetooth is slightly better than ZigBee in small-scale networks with small payloads regarding latency. However, when required payloads and the scale of the network grow, the performance of Bluetooth degrades faster than ZigBee.

Such a difference results from the different routing algorithm. ZigBee uses source routing, whereas Bluetooth Mesh chooses flooding. Compared to source routing, managed flooding gains advantages over simplicity and flexibility but tends to suffer more from collisions. In small-scale networks, the problem caused by flooding is not obvious. But in large-scale networks, it is

necessary to conduct relay optimization, disabling the relay functionality of some nodes to improve the performance of the whole network. Apart from that, currently Bluetooth Mesh can only utilize the three advertising channels for communicating, which limits the size of payloads inside one packet. Therefore, transmitting a large payload requires several packets, which also decreases its performance.

5.2.3 Conclusion. Through theoretical and experimental evaluations conducted previously, we can see that the new Bluetooth outperforms ZigBee in single-link connections. And due to the simplicity resulting from managed flooding, Bluetooth can also serve better in small-scale networks, although the difference is not obvious.

However, for large-scale networks, the new Bluetooth still needs further improvement to overcome problems such as collision issues brought by flooding. Apart from that, it has not fully utilized benefits brought by Bluetooth 5.0 like the enlarged secondary advertising channels.

6 FUTURE: WHAT MORE CAN BLUETOOTH ACHIEVE?

Shortcomings of one technology may damage its popularity in markets, but they can also generate research issues worthy of study. For example, lacking mesh functionality was thought to be one major shortcoming of Bluetooth and limited its application fields. To address this problem, looking back to the time when Bluetooth did not support mesh topology, we can find that plenty of works were proposed to realize it. As surveyed by Darroudi and Gomez [4], non-official versions of Bluetooth-based mesh solutions were proposed by both academia [17, 26, 29] and the industry [28]. Based on these efforts, Bluetooth now owns mesh functionality.

Therefore, it is worthy to discuss what the new Bluetooth lacks and question whether it can be better to meet higher demands. In this section, we discuss possible directions the new Bluetooth may need to consider in future versions.

6.1 Can Bluetooth Get Faster?

There is always a question if wireless technologies can be faster. For Bluetooth, this question does own its practical meaning. For example, Bluetooth now is sufficient for streaming lossy compressed MP3 and AAC files. However, we can imagine that in the near future, customers will request more high-resolution audio. However, the higher data rate only happens to the BLE part in Bluetooth 5.0. Thus, we wonder if this enhancement also can happen to the BR/EDR part for achieving higher data rate audio transmittion. In addition, with higher data rates, Bluetooth can further code its audio file to resist interference while keeping high audio quality. Nevertheless, a higher data rate may even allow Bluetooth to gain access to video streaming.

One possible way to achieve this is by using other modulation methods. The currently used modulation method, frequency-hopping spread spectrum, though practices greatly in resisting interferences, is not highly efficient regarding data rate as it only selects one piece of the whole frequency band at a time for transmitting data. Another possible way is to conjugate nearby frequency bands. As the data rate is proportional to the frequency band when other conditions remain, it can directly double the data rate. However, the two possible ways require modifications on the whole system, from hardware to network protocols and sound impossible to achieve at the present time. However, it is still worthy to believe whether there are possible ways to further improve the data rate of Bluetooth.

6.2 Can Bluetooth Be More Energy Efficient?

Power consumption is always a concern in the IoT area. As we know, Wi-Fi is not considered in many battery-powered applications due to its high power consumption. Imagine when a user

deploys thousands of sensors in a forest to monitor its condition. He or she will be desperate if those sensors are Wi-Fi enabled and thus would have to be recharged every several hours or days. In the IoT, a more energy-efficient network is always welcomed.

Both BLE and Bluetooth Mesh have been specifically optimized for low-power applications. BLE uses a duty-cycled mode and cuts down its operating time to save power, and Bluetooth Mesh proposes its heterogeneous structure for saving power of low-power nodes. Therefore, it is low-power nodes with the short operating time that reduce overall power consumption.

One feasible way to address this issue is to study mechanisms to decide how this duty-cycled mode is performed for better energy efficiency, such as using different data rates [36]. In addition, recent years have seen the boom of backscatter applications, which significantly reduce the power consumption of communication. Especially, researchers have proposed prototypes that can communicate by backscattering Bluetooth signals and have a 100x higher energy efficiency for transmitting per bit than conventional BLE transmitters, [6], which may be utilized for designing more energy-efficient Bluetooth networks.

6.3 Can Bluetooth Be More Secure?

Network security, such as the botnet, has become one major concern when referring to IoT applications. Although Bluetooth Mesh has been specifically optimized for resisting attacks, hackers never stop and security will be an eternal issue. As stated by the Bluetooth SIG, Bluetooth is aiming at the market of industrial IoT, where reliability and security issues matter most for both profit and safety of employees.

Many kinds of threats can be faced by Bluetooth-based networks, such as jamming attacks in device-intensive applications. With so many low-power devices working together in the same network, low-power WSNs are vulnerable to jamming attacks, which has been surveyed by Mpitziopoulos et al. [22]. Considering Bluetooth-based networks, although frequency-hopping and security mechanisms help resist such threats, it still remains to be seen how well this works when surveying different jamming attacks.

In addition, privacy is another concerning issue receiving more attention today. In a flooding-based network, all messages can be received by any nodes in coverage. This causes a possibility of leakage of privacy.

For instance, an attacker can collect all messages as long as he or she can receive them if he or she acquires the network key. Thus, even if the attacker without an application key is not able to decode information inside messages, he or she is able to know some other information, such as the received signal strength, and relate it to certain network addresses. Thus, naturally, it is like doing crowdsensing without permission. And he or she might be able to infer the location of a certain device, which causes a possibility of leakage of location [20].

6.4 Can Bluetooth Open Up Deeper Information?

As a technology for communication, the only PHY layer information Bluetooth has provided is merely coarse features of messages, such as RSSI and link quality [11], which have already opened up chances for utilizing Bluetooth for more accurate localization [13, 25]. Thus, it makes us wonder, what if more PHY-layer information of Bluetooth were open to researchers?

For example, the introduction of Channel State Information (CSI) in Wi-Fi makes the accuracy of Wi-Fi–based localization improve greatly compared to RSSI-based methods [45]. As the CSI can be seen as amplitude and phase response values to a group of frequency points, it is much better in resisting noises in static environments and the common frequency-selective fading phenomena indoors. Therefore, CSI is more steady than RSSI, which makes it a practical value in applications. For instance, in detecting invasions, it can achieve a much lower false alarm rate than RSSI [42]. In

addition, as a more fine-grain feature, CSI is better at characterizing physical environments, which enables Wi-Fi to be utilized in gesture recognition [35].

Therefore, as we can see, the advantages of utilizing deeper information buried in the PHY layer are nonpredictable. Of course, it shall be considered that Bluetooth is different from Wi-Fi. For example, whereas Wi-Fi uses OFDM modulation, signals of Bluetooth use FHSS. Since they have different waveforms, it may be harder to get values in a group of different frequency points. Apart from that, Bluetooth uses a smaller bandwidth than Wi-Fi. As the spatial resolution is related to the bandwidth [43], Bluetooth might not be able to achieve precision as high as Wi-Fi.

However, differences do not necessarily mean impossibility but may lead to new opportunity. We believe that they leave more research possibilities for Bluetooth.

7 SUMMARY

For connecting massive devices, wireless technologies in the IoT area can be divided into two broad categories: long-range and short-range technologies based on coverage.

In the long-range category, the area has been dominated by LPWANs like NB-IoT and LoRa, as they fulfill the demands of large spatial scale (city wide), massive connections (tens of thousands of devices per base station), and extremely low power (several years of battery life). Powerful as it seems, LPWANs are not omnipotent. Their shortages on speed, throughput, and being difficult in deployment leave a blank space for short-range technologies.

However, competitions in short-range applications are way more severe. ZigBee, Z-Wave, Wi-Fi, and many other technologies have provided heterogeneous services for meeting the diverse requirements brought up by different applications. And now Bluetooth officially comes into this battle with its two specifications, carrying with full improvements on coverage, speed, advertising, robustness, and network capacity.

In this survey, through comparisons and analyses of those updates, it can be concluded that the new Bluetooth not only consolidates its superiority in commercial applications but also expands possibilities for academia. In summary, although the future is hard to predict, we believe that Bluetooth has made itself a strong competitor in the future of providing complete solutions for meeting the demands of communication in the IoT area.

REFERENCES

[1] Mathias Baert, Jen Rossey, Adnan Shahid, and Jeroen Hoebeke. 2018. The Bluetooth mesh standard: An overview and experimental evaluation. *Sensors (Basel, Switzerland)* 18, 8 (July 2018), 2409. DOI: https://doi.org/10.3390/s18082409

[2] Nick Baker. 2005. ZigBee and Bluetooth strengths and weaknesses for industrial applications. *Computing & Control Engineering Journal* 16, 2 (2005), 20–25.

[3] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz. 2018. Bluetooth 5: A concrete step forward toward the IoT. *IEEE Communications Magazine* 56, 7 (July 2018), 125–131. DOI: https://doi.org/10.1109/MCOM.2018.1700053

[4] Seyed Mahdi Darroudi and Carles Gomez. 2017. Bluetooth low energy mesh networks: A survey. *Sensors* 17, 7 (2017), 1467.

[5] Piergiusepps Di Macro, Per Skillermark, Anna Larmo, and Pontus Arvidson. 2017. Bluetooth Mesh Networking. Retrieved July 22, 2017 from https://www.ericsson.com/en/publications/white-papers/bluetooth-mesh-networking.

[6] Joshua F. Ensworth and Matthew S. Reynolds. 2017. BLE-backscatter: Ultralow-power IoT nodes compatible with Bluetooth 4.0 low energy (BLE) smartphones and tablets. *IEEE Transactions on Microwave Theory and Techniques* 65, 9 (2017), 3360–3368.

[7] Christian Gehrmann. 2002. *Bluetooth Security White Paper*. Bluetooth SIG Security Expert Group.

[8] Bluetooth Mesh Working Group. 2017. Mesh Profile v1.0. Retrieved April 12, 2019 from https://www.bluetooth.com/specifications/mesh-specifications.

[9] C. T. Hager and S. F. Midkiff. 2003. An analysis of Bluetooth security vulnerabilities. In *Proceedings of the 2003 IEEE Wireless Communications and Networking Conference (WCNC'03)*. Vol. 3. 1825–1831. DOI: https://doi.org/10.1109/WCNC.2003.1200664

[10] Richard W. Hamming. 1950. Error detecting and error correcting codes. *Bell System Technical Journal* 29, 2 (1950), 147–160.

[11] A. K. M. M. Hossain and W. Soh. 2007. A comprehensive study of Bluetooth signal parameters for localization. In *Proceedings of the 2007 IEEE 18th International Symposium on Personal, Indoor, and Mobile Radio Communications*. 1–5. DOI: https://doi.org/10.1109/PIMRC.2007.4394215

[12] N. Hunke, Z. Yusef, M. Ruessmann, F. Schmieg, A. Bhatia, and N. Kalra. 2017. Winning in IoT: It's all about the business processes. *BCG Perspectives*. Available at https://www.bcg.com.

[13] H. J. Pérez Iglesias, V. Barral, and C. J. Escudero. 2012. Indoor person localization system through RSSI Bluetooth fingerprinting. In *Proceedings of the 2012 19th International Conference on Systems, Signals, and Image Processing (IWSSIP'12)*. 40–43.

[14] Markus Jakobsson and Susanne Wetzel. 2001. Security weaknesses in Bluetooth. In *Topics in Cryptology—CT-RSA 2001*, D. Naccache (Ed.). Springer, Berlin, Germany, 176–191.

[15] Aravind Kailas, Valentina Cecchi, and Arindam Mukherjee. 2012. A survey of communications and networking technologies for energy management in buildings and home automation. *Journal of Computer Networks and Communications* 2012 (2012), Article 932181, 12 pages.

[16] Heikki Karvonen, Konstantin Mikhaylov, Matti Hämäläinen, Jari Iinatti, and Carlos Pomalaza-Ráez. 2017. Experimental performance evaluation of BLE 4 vs BLE 5 in indoors and outdoors scenarios. In *Advances in Body Area Networks*. Springer, 235–251.

[17] H. Kim, J. Lee, and J. W. Jang. 2015. BLEmesh: A wireless mesh network protocol for Bluetooth low energy devices. In *Proceedings of the 2015 3rd International Conference on Future Internet of Things and Cloud*. 558–563. DOI: https://doi.org/10.1109/FiCloud.2015.21

[18] M. Kouhne and J. Sieck. 2014. Location-based services with iBeacon technology. In *Proceedings of the 2014 2nd International Conference on Artificial Intelligence, Modelling, and Simulation*. 315–321. DOI: https://doi.org/10.1109/AIMS.2014.58

[19] Silicon Labs. 2018. Benchmarking Bluetooth Mesh, Thread, and Zigbee Network Performance. Retrieved January 15, 2019 from https://www.silabs.com/products/wireless/learning-center/mesh-performance.

[20] Qiang Ma, Shanfeng Zhang, Tong Zhu, Kebin Liu, Lan Zhang, Wenbo He, and Yunhao Liu. 2017. PLP: Protecting location privacy against correlation analyze attack in crowdsensing. *IEEE Transactions on Mobile Computing* 16, 9 (2017), 2588–2598.

[21] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497–1516.

[22] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. 2009. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys Tutorials* 11, 4 (2009), 42–56. DOI: https://doi.org/10.1109/SURV.2009.090404

[23] Thomas Muller. 1999. *Bluetooth Security Architecture*. White Paper Version 1.0.

[24] Yuri Murillo, Brecht Reynders, Alessandro Chiumento, Salman Malik, Pieter Crombez, and Sofie Pollin. 2017. Bluetooth now or low energy: Should BLE mesh become a flooding or connection oriented network? In *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'17)*. IEEE, Los Alamitos, CA, 1–6.

[25] I. Oksar. 2014. A Bluetooth signal strength based indoor localization method. In *Proceedings of the 21st International Conference on Systems, Signals, and Image Processing (IWSSIP'14)*. 251–254.

[26] Gaetano Patti, Luca Leonardi, and Lucia Lo Bello. 2016. A Bluetooth low energy real-time protocol for industrial wireless mesh networks. In *Proceedings of the 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON'16)*. IEEE, Los Alamitos, CA, 4627–4632.

[27] Zhongmin Pei, Zhidong Deng, Bo Yang, and Xiaoliang Cheng. 2008. Application-oriented wireless sensor network communication protocols and hardware platforms: A survey. In *Proceedings of the 2008 IEEE International Conference on Industrial Technology (ICIT'08)*. IEEE, Los Alamitos, CA, 1–6.

[28] Qualcomm. 2017. CSRmesh Development Kit. Retrieved May 5, 2018 from https://www.qualcomm.com/products/csrmesh-development-kit.

[29] Yaswanth Kumar Reddy, Praneeth Juturu, Hari Prabhat Gupta, Pramod Reddy Serikar, Shruti Sirur, Sulekha Barak, and Bonggon Kim. 2015. A connection oriented mesh network for mobile devices using Bluetooth low energy. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. ACM, New York, NY, 453–454.

[30] Kai Ren. 2017. Exploring Bluetooth 5—How Fast Can It Be? Retrieved February 20, 2017 from https://blog.bluetooth.com/exploring-bluetooth-5-how-fast-can-it-be.

[31] Janessa Rivera and Rob van der Meulen. 2013. Gartner says the Internet of Things installed base will grow to 26 billion units by 2020. Stamford, CT, December 12.

[32] F. Samie, L. Bauer, and J. Henkel. 2016. IoT technologies for embedded computing: A survey. In *Proceedings of the 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'16)*. 1–10.
[33] Nordic Semiconductor. 2016. Nordic nRF52840. Retrieved April 12, 2019 from https://www.nordicsemi.com/eng/Products/nRF52840.
[34] Bluetooth SIG. 2016. Bluetooth 5.0 Core Specification. Retrieved April 12, 2019 from https://www.bluetooth.com/specifications/bluetooth-core-specification.
[35] Sheng Tan and Jie Yang. 2016. WiFinger: Leveraging commodity WiFi for fine-grained finger gesture recognition. In *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, New York, NY, 201–210.
[36] Jiliang Wang, Zhichao Cao, Xufei Mao, Xiang-Yang Li, and Yunhao Liu. 2016. Towards energy efficient duty-cycled networks: Aanalysis, implications and improvement. *IEEE Transactions on Computers* 1 (2016), 1–1.
[37] Wendy Warne. 2016. Bluetooth 5 Is Here. Retrieved December 14, 2016 from https://blog.bluetooth.com/bluetooth-5-is-here.
[38] Wendy Warne. 2017. Exploring Bluetooth 5—What's New in Advertising? Retrieved February 27, 2017 from https://blog.bluetooth.com/exploring-bluetooth5-whats-new-in-advertising.
[39] Martin Woolley. 2017. Exploring Bluetooth 5—Going the Distance. Retrieved February 13, 2017 from https://blog.bluetooth.com/exploring-bluetooth-5-going-the-distance.
[40] C. Wu, Z. Yang, and Y. Liu. 2015. Smartphones based crowdsourcing for indoor localization. *IEEE Transactions on Mobile Computing* 14, 2 (Feb. 2015), 444–457. DOI: https://doi.org/10.1109/TMC.2014.2320254
[41] C. Wu, Z. Yang, and C. Xiao. 2018. Automatic radio map adaptation for indoor localization using smartphones. *IEEE Transactions on Mobile Computing* 17, 3 (March 2018), 517–528. DOI: https://doi.org/10.1109/TMC.2017.2737004
[42] Chenshu Wu, Zheng Yang, Zimu Zhou, Xuefeng Liu, Yunhao Liu, and Jiannong Cao. 2015. Non-invasive detection of moving and stationary human with wifi. *IEEE Journal on Selected Areas in Communications* 33, 11 (2015), 2329–2342.
[43] Yaxiong Xie, Zhenjiang Li, and Mo Li. 2018. Precise power delay profiling with commodity Wi-Fi. *IEEE Transactions on Mobile Computing* (2018), 1–1. DOI: 10.1109/TMC.2018.2860991
[44] Zheng Yang, Chenshu Wu, and Yunhao Liu. 2012. Locating in fingerprint space: Wireless indoor localization with little human intervention. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking (MobiCom'12)*. ACM, New York, NY, 269–280. DOI: https://doi.org/10.1145/2348543.2348578
[45] Zheng Yang, Zimu Zhou, and Yunhao Liu. 2013. From RSSI to CSI: Indoor localization via channel response. *ACM Computing Surveys* 46, 2 (2013), 25.
[46] Thomas Zahn, Greg O'Shea, and Antony Rowstron. 2009. An empirical study of flooding in mesh networks. *SIGMETRICS Performance Evaluation Review* 37, 2 (Oct. 2009), 57–58. DOI: https://doi.org/10.1145/1639562.1639584
[47] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. 2014. IoT security: Ongoing challenges and research opportunities. In *Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA'14)*. IEEE, Los Alamitos, CA, 230–234.
[48] Y. Zhou, H. Wang, S. Zheng, and Z. Z. Lei. 2013. Advances in IEEE 802.11ah standardization for machine-type communications in sub-1GHz WLAN. In *Proceedings of the 2013 IEEE International Conference on Communications Workshops (ICC'13)*. 1269–1273. DOI: https://doi.org/10.1109/ICCW.2013.6649432

Received August 2018; revised January 2019; accepted February 2019