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

蓝牙5.0与Mesh:物联网新里程碑综述

1023041122孙思源

CONTENTS

蓝牙发展历程

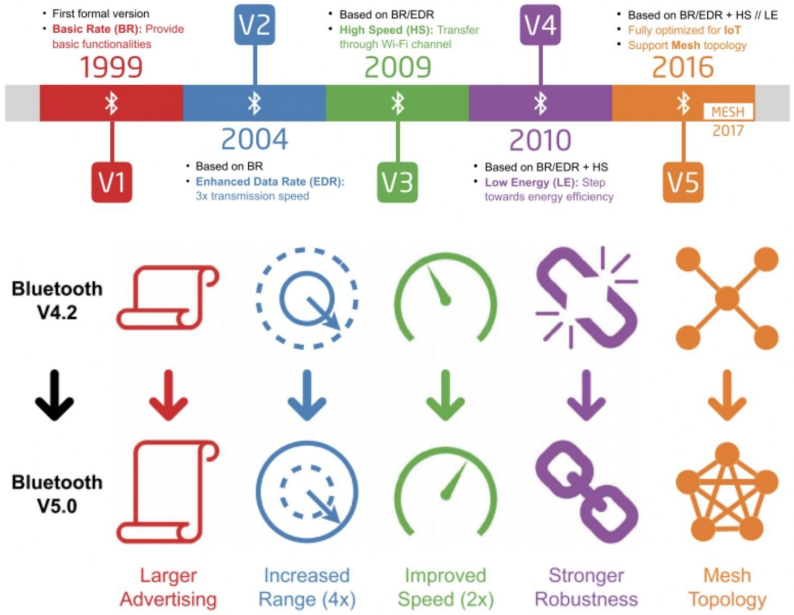
蓝牙1.X——为基本功能提供基本速率

蓝牙2.X——增强数据率（EDR）

蓝牙3.X——高速技术（HS）

蓝牙4.X——低功耗功能（LE）

蓝牙5.0和Mesh网状网络



02 蓝牙5.0的新功能

蓝牙5.0的新功能

蓝牙5.0的大部分创新都是专门针对第四代蓝牙的**低功耗功能**（BLE）提出，而经典的BR/EDR几乎保持不变。其中最重要的三个增强方式分别为：

- 物理层新添加2Msym/s的**调制方案**，允许BLE使用2MHz带宽传输数据，相当于4.2版本传输速度的两倍。
- 通过一种新的编码方案实现的**远程LE**，使传输范围相较4.2版本增加了四倍。
- **LE广播扩展**使用了另外37个在以前的版本中不用于广播的频道，加上其他新功能，使新蓝牙具有是8倍广播容量。

蓝牙5.0的新功能——提高传输速率

速率的提高主要归功于蓝牙5.0新增的2M sym/s PHY的LE特性这一新的物理层调制方案。

在蓝牙5.0中，有三种不同类型的物理定义：**LE 1M无编码**、**LE 1M编码**和**LE 2M无编码**。1M或2M表示符号速率为1Mb/s或2Mb/s。“编码”或“非编码”是指是否使用错误编码方案，这是通信中增加无线信号灵敏度的经典选择，以便信号恢复后在进一步传输时能够达到相同的错误率。

蓝牙5.0的新功能——提高传输速率

工作在BLE模式时，将频带划分为40个子频带，每个子频带占用2MHz带宽。因此，2MHz是BLE的理论最大带宽。

通过选择**2M sym/s PHY**，过去需要2000 ms完成传输的相同数据量现在只需要1000 ms。由于传输速度更快，传输相同大小的文件所需的时间可以减半，蓝牙变得更节能。

在考虑某些广播事件时，另一个新功能，高工作周期非连接广播也有助于提高速度。蓝牙4.x版本将可扫描的无向广播和非连接的无向广播两个广播事件分离，设置最小广播间隔为100ms，而其他设置为20ms。**在蓝牙5.0中，不同广播事件的最小广播间隔都是20ms**。

蓝牙5.0的新功能——扩大覆盖范围

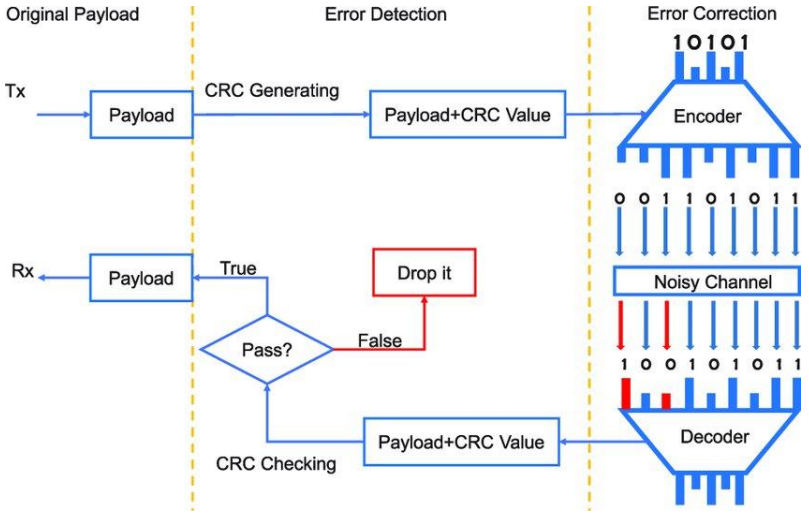
蓝牙5.0最重要的增强可以被认为是扩大了覆盖范围，这种增强功能（远程LE）同样仅适用于BLE，是通过两个更改实现的：

主要的更改是**新引入的编码方案**。此前提到的蓝牙5.0的物理层三种调制方案中，LE 2M无编码方案用于提高传输速率，而LE 1M编码方案用于扩大覆盖范围。蓝牙使用一种编码方案来处理通信过程中发生的错误，以便在较远的距离内正确接收信号。

蓝牙5.0在以往错误检测的基础上增加了**前向纠错功能**。

蓝牙5.0的新功能——扩大覆盖范围

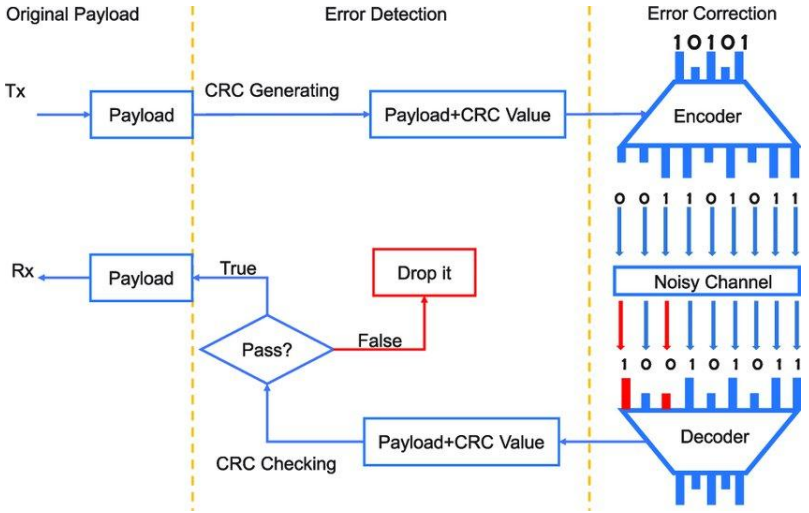
错误检测仍然与早期版本相同，生成一个24位的CRC值用于错误检测。接收端在接收到数据包时，会将接收到的CRC值与重新计算的CRC值进行比较。如果它们相同，接收方将认为没有发生错误；否则，它直接丢弃该数据包。



蓝牙5.0的新功能——扩大覆盖范围

蓝牙5.0采用前向纠错技术（FEC）进行纠错。FEC是通信中用于控制噪声信道中数据传输错误的一种通用方法，以较高的数据敏感度来权衡数据速率。一般来说使用几个符号来表示一个比特，以便在损坏不太严重的情况下可以恢复原始数据。FEC通过冗余增加了实际负载每比特的能量，但并不增加发射功率。

蓝牙5.0中定义了两种编码方案：S = 2和S = 8 (S表示每比特所使用的符号数量)。当符号速率为1Msym/s时，对应于2倍和4倍的范围。



蓝牙5.0的新功能——扩大覆盖范围

次要的更改是**更高的输出功率**。蓝牙5.0规范中定义的最高输出功率从10 dBm提高到20 dBm，这可以直接增加连接范围。此外，对于BLE器件，如果其LE PHY只能支持1M sym/s PHY，则其最高输出功率可以保持在10dBm。在建立连接过程时，最高输出功率电平是不允许使用的。

对于蓝牙5.0，工作范围约为300m，是蓝牙4.2的4倍，这意味着远程模式可以工作。**从不同的物理结构中，我们可以看到蓝牙5.0为用户提供了两种选择，要么用两倍的符号速率更快地传输，要么用更少的数据更远地传输，用户无法同时享受这两种选择。**

蓝牙5.0的新功能——提升广播容量

新版本中另一个重要增强是广播能力的增强，这对BLE最重要也是最成功的应用场景——**信标服务**（beacon-based service）来说意义重大。

一个典型的蓝牙应用场景是，蓝牙设备或仅一个BLE设备以广播方式工作，配备其他蓝牙设备的用户走到它附近，就可以从它那里获取定位或广播信息。

然而由于广播能力的限制，设备一次只能发送很少的信息。同时在广播信息时接收器需要与节点设备建立连接，降低了效率。

蓝牙5.0采用了许多更新来克服这些不便。通过8倍的广播容量，大大提高了BLE的实用性，向无连接广播迈进了一步。

蓝牙5.0的新功能——提升广播容量

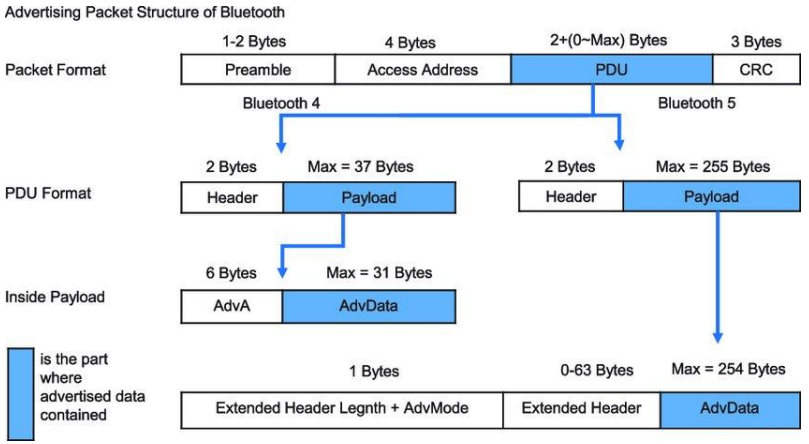
与这种增强相对应的特性是**LE广播扩展**（LE Advertising Extensions）。更详细地说，蓝牙5.0重新设计了一个完整的广播系统，包括扩展新的广播渠道，和相应扩展的新协议数据单元（PDU）。

相比蓝牙4.X版本，广播功能的最显著差异是用于此目的的**渠道数量**。在蓝牙4.X版本中，广播事件仅在40个渠道中的3个上执行，其他37个渠道用于数据传输。在蓝牙5.0中，原有的3个广告渠道作为一级广播渠道，其他37个通道也可以用于广播，被设置为二级广播渠道。

随着新通道的引入，蓝牙5.0增加了几个扩展的**广播协议数据单元**，以提高广播性能。新的pdu允许两个不同步的蓝牙设备在广播时无需配对便可交换数据。从而大大提高了蓝牙信标的接收效率，实现了无连接的广播。

蓝牙5.0的新功能——提升广播容量

除了新的通道和新的PDU，这些新PDU的报文格式也不完全相同。在一个蓝牙数据包中，有一个前导符、一个访问地址、一个PDU和一个CRC。在PDU中，有一个首部和一个实际的负载。蓝牙将可用广告消息的大小从31字节提高到254字节。



蓝牙5.0的新功能——增强健壮性

蓝牙5.0还有两个新特性尚未讨论:插槽可用掩码（SAM）和LE信道选择算法#2。Wi-Fi和蓝牙在许多设备上共存，由于Wi-Fi的一部分共享相同的2.4GHz ISM频段，当两者工作时就会发生相同频段的碰撞，此外有时一方需要等待另一方完成使用微控制器单元。蓝牙有防止与Wi-Fi发生碰撞的方案，但它不会像配对的设备那样工作。**SAM提供了一种在两个蓝牙设备可用时相互通知的方法。**

此外，当一个蓝牙设备与多个蓝牙设备配对时，需要为它们**安排时间槽**，告诉它们何时交换数据。SAM可以帮助蓝牙设备与其他蓝牙设备共存，减少与同一频段内其他技术的碰撞，提高在拥挤的ISM频段内的信号传输效率。

蓝牙5.0的新功能——增强健壮性

信道选择算法#2是信道选择算法#1的增强版本。算法#1只支持连接事件的信道选择，而**算法#2增加了对周期性广播事件的支持**。同时算法#2使用不同的方法来**生成下一个信道索引**，提供了更好的伪随机性，这有助于蓝牙设备与使用相同ISM频段的其他设备更好地共存。

此外，**更高的输出功率**或多或少也有助于更强的健壮性。当发射功率不超过上限时，同一范围内的信噪比也会随之提高。

蓝牙5.0的新功能——总结

通过新引入的功能，蓝牙5.0在速度、覆盖范围、广播能力和健壮性等方面实现了全面的增强。

蓝牙5.0专门优化了其BLE模式，使其已经获得了低功耗的优势，增加了更快的速度和更远的距离的选择。在BLE最成功的应用领域中，蓝牙5.0极大地提高了其易用性，更好地与其他设备共存，提供了更好的用户体验。

除了前面讨论的增强功能，研究人员还表明，蓝牙5.0可以比以前的版本更节能。蓝牙5.0向物联网迈出了具体的一步。

03 蓝牙mesh：一种新范式

蓝牙mesh——现有蓝牙网络的不足

作为一种工作在2.4GHz ISM频段的低功耗无线技术，长期以来，蓝牙网络一直存在可扩展性差、覆盖范围短的问题，其信号在没有中继的情况下传输距离不可能很远，这限制了其在工业和农业等需要广泛覆盖的应用场景中的应用。此外，一个主设备只能有7个从设备的限制也限制了蓝牙在设备密集型应用中的部署。

克服这些缺点的一种方法是添加**网状（mesh）拓扑结构**。mesh拓扑使设备之间能够相互通信，并允许消息转发。使用mesh拓扑可以扩展覆盖范围，建立大量连接。此外，mesh拓扑相对于星型拓扑，其节点失效时受到的破坏更小，增加了网络的可靠性。

蓝牙mesh——基础概念

蓝牙网状网中包含的每个设备称为一个节点，通常对应一个蓝牙芯片模块。然而有可能有多个部件连接到一个芯片模块和控制。因此更小的单位——**元素**，被定义来描述这些部分。

元素是蓝牙网格中最小的物理单元。由于一个元素可以用于不同的目的，因此提出了另外两个术语，**模型**和**状态**，来组织这些功能。一个模型代表一个元素的一种功能，在模型内部会有一个或几个状态来衡量其条件。

正常情况下，同一网络内的蓝牙设备在处理能力、供电条件等诸多方面并不相同。因此需要寻找方法区分不同条件的节点。除了基本的通信功能外，蓝牙mesh还设计了一些额外的功能，以充分利用不同的节点。

因此，构成蓝牙mesh网络的是包含一个或多个元素的异构节点。

蓝牙mesh——基础概念

蓝牙mesh网络中的节点之间通过消息进行通信，消息的内容除包含发送和预期接收节点的地址外，还包括一些采用广播方式的控制字段。根据是否需要响应，消息可以分为已确认消息和未确认消息。

蓝牙Mesh中定义了三种地址:单播地址、组地址和虚拟地址。

任何一个元素添加到网络时都将被分配一个**单播地址**，类似于元素的ID号。

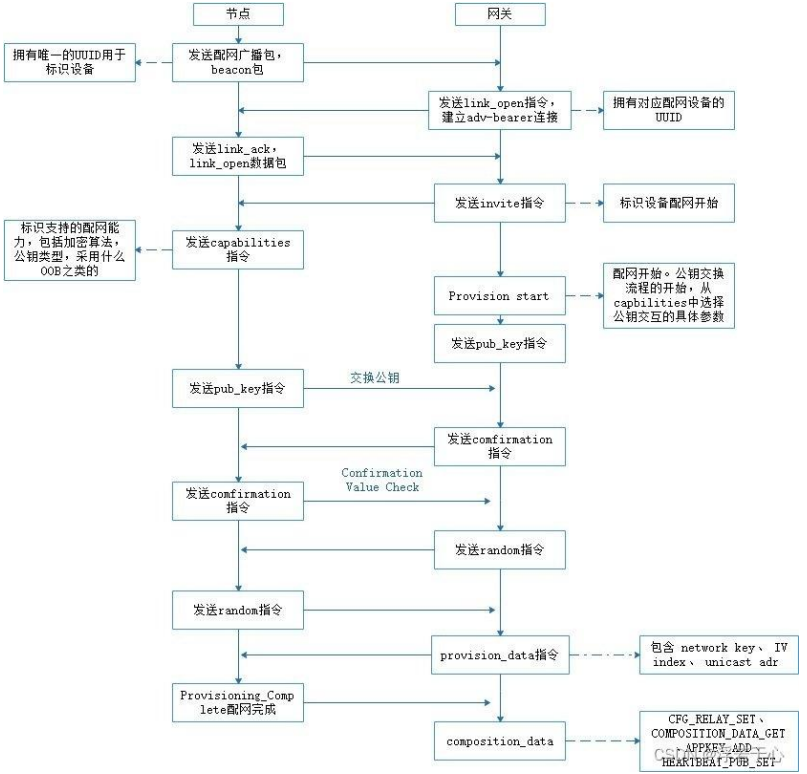
根据用户对元素的组织方式，稍后可以为元素分配**虚拟地址**或**组地址**。

在蓝牙Mesh中，发送或接收消息的活动称为发布或订阅。订阅指的是接收消息并仅处理来自配置地址的消息，而发布指的是发送消息的行为。

蓝牙mesh——基础概念

将一个新的蓝牙设备添加到蓝牙mesh网络的过程称为**配置（provisioning）**。帮助这个新设备成为新节点的节点称为**供应节点**。这个过程分为5个阶段：**信标、邀请、交换公钥、身份验证和分发配置数据。**

随着配置过程的完成，新的蓝牙设备作为一个新的蓝牙mesh网络节点被接受，并可以根据其设置执行通信功能。



蓝牙mesh——特性：有管理的洪泛

网状网的一个主要问题是如何处理中继，通常有基于洪泛的和基于路由的两类。

蓝牙Mesh采用的方法是一种优化的泛洪方法，称为**有管理的泛洪**。泛洪在实践中更简单，延迟更低。但如果没有精心设计，可能会给网络带来沉重的负担。因此，采用了几种方法来进行优化：

- **描述心跳机制**使节点周期性地发布心跳消息，以便其他节点知道它是活动的。此外，根据包含的数据，其他节点可以推断出将消息发送给它需要多少跳。
- 在所有的蓝牙mesh消息中都包含一个被称为**生存时间**（TTL）的特殊值，它告诉接收者一条消息还可以被发布多少次。TTL的存在说明了心跳消息的重要性。
- 在每个节点上设置一个**消息缓存**来存储最近接收到的消息。在基于洪泛的网状网络中，消息可以通过多种不同的方式发送。通过消息缓存进行存储，可以判断消息是否已经接收。接收方可以直接丢弃，避免再处理，提高网络效率。

目前蓝牙网状网没有路由器、路由路径和路由算法，但是将在未来的版本中考虑。

蓝牙mesh——特性：不对称结构

为了提高mesh网络的性能，蓝牙mesh网络中的节点是异构的。为了充分利用不同类型的蓝牙设备，必须考虑设备的供电和处理能力等条件。

根据节点的使用情况和物理限制，节点可以选择不支持或支持中继、代理、朋友和低功耗这4个功能中的几个。

中继功能是蓝牙设计的最基本的附加功能。它允许节点为其他节点转发消息，从而实现mesh网络更大的覆盖率和更高的可靠性。

代理功能使节点可以作为蓝牙mesh网络节点与外部蓝牙设备之间的转换器。目前，大多数蓝牙设备仍然使用蓝牙4.x版本，因此设计了代理功能来将这些设备添加到mesh网络中。具体而言在mesh网络中设计了2个承载器，一种叫做GATT承载，用于mesh网络内部的通信；另一个被称为ADV承载器，连接旧的BLE设备。具有代理特性的节点也必须具有中继特性。

蓝牙mesh——特性：不对称结构

朋友和低功耗是两个成对的功能。有些节点对能量消耗非常敏感，由于泛洪机制的存在，节点需要不断地扫描不同的信道，极大地降低了能量敏感节点的实用性。蓝牙Mesh设计了**低功耗**功能来降低占空比，低特征节点不需要频繁活动，只需要按编程方式，唤醒自身并在工作时间接收消息即可。

然而，当占空比较低时，这种方式有可能丢失重要信息，作为补充，引入了朋友功能。

朋友功能使节点与具有低功耗功能的节点形成一种称为友谊的关系。发送给低功耗节点的消息首先会被存储在对应的朋友节点中。当低功耗节点处于活动状态时，它将接收来自朋友节点的消息。此外，朋友节点需要承担转发其低功耗节点消息的义务，也需要具有中继特性。

蓝牙mesh——特性：网络安全

在蓝牙Mesh中，安全性是强制性的，不能关闭。蓝牙Mesh提供了从新增设备到消息处理的全程安全设计。

• **添加新设备过程的安全性**：为阻止恶意设备进入。配置过程增加了两个安全步骤:交换公钥和身份验证。设备添加前需要通过认证。这增加了恶意设备被错误接受的难度。

• **通信过程的安全性**：由于无线通信通过空气传输信息，因此很容易被覆盖区域内的任何设备捕获。在蓝牙Mesh中，所有消息都使用128位密钥进行AES-CCM加密。为了进一步提高隐私性，消息也被混淆，这样节点就不容易被跟踪。

• **消息的安全性**：为防止消息来自传输过程中的中继节点，mesh网络设计了两个密钥分别用于保护网络中的消息和应用程序中的消息。网络密钥由同一网络中的所有节点获取，保证消息在传输过程中安全；应用密钥用于正确解密其中的信息。

• 蓝牙Mesh还对一些典型的攻击进行了防范：为了抵抗**回收站攻击**，供应者将把删除的节点放入一个黑名单，并更改该节点曾经处理过的密钥。通过匹配序列号和索引号也可以针对**重放攻击**。

04 新蓝牙应用场景

一对一：设备配对

由于电力供应有限，大多数可穿戴设备，都是使用蓝牙与手机或其他设备进行通信。新蓝牙的一个直接好处是为使用蓝牙配对的设备提供了更强大的通信链接，且取决于设备使用哪种模式：BR/EDR还是BLE。

对于**基于BLE的设备**，可以使用蓝牙5.0中引入的所有新功能。

对于**基于BR/EDR的设备**，新蓝牙几乎与之前的蓝牙4.2相同，但可以使用更高的输出功率和SAM。

对于使用蓝牙进行一对一通信的应用，使用蓝牙5.0可以获得比以前更快的速度和更长的通信距离，同时不影响性能质量或获得更稳定的高质量通信服务。

一对多：邻近信标

基于信标的接近是应用程序使用蓝牙形成一对多拓扑的一个经典例子。

设备不断向邻近设备广播其ID和包含的信息，然后根据与这些设备的距离或角度收集多个ID进行定位。还可以进一步提供基于位置的服务，比如基于信标的导航。

更大的广播容量使信标能够在携带ID的同时携带更详细的信息，因此可以提供各种上下文丰富的基于位置的服务。

蓝牙在室内定位应用中应用广泛，基于指纹的室内定位方法是一种主要的定位方法，通过测量并收集多个不同信号源的信号索引，形成一个指纹数据库。

多对多：网格对象

智能家居/办公室和工业控制是物联网时代两大有前景的场景。

• **智能家居/办公室**：由于蓝牙网络容量小，它并不是多传感器应用的首选，ZigBee一直被认为是智能家居和办公应用的理想选择。随着蓝牙mesh技术的发展，一方面，使用ZigBee就需要额外的硬件，而大多数笔记本电脑、平板电脑和智能手机都配备了蓝牙。另一方面，蓝牙比ZigBee提供更高的数据速率，同时使用相同的能量消耗。

• **工业控制**：在工业控制领域，用户交互较少，但需要对更多的设备进行有效连接，对能源效率和可靠性有更严格的要求。通过朋友节点和低功耗节点的设计，使蓝牙mesh的功耗比BLE更低。通过抵抗跳频的干扰和编码方案，蓝牙mesh可以容忍更多的设备协同工作，保证网络可靠性。

蓝牙mesh不需要路由表，理论上只要消息有足够的TTL并且至少有一条物理链路存在，就可以发送消息。**当节点失效时，蓝牙mesh比基于路由的网络更可靠。**

05 蓝牙的未来

蓝牙的未来——更快

较高的数据传输速率仅体现在蓝牙5.0的BLE部分，因此这种增强是否也可以发生在BR/EDR部分，以实现更高的数据率音频传输？此外，在更高的数据速率下，蓝牙是否可以进一步编码以抵抗干扰？

实现这一目标的一种可能方法是**使用其他调制方法**，目前使用的跳频扩频调制方式，虽然抗干扰能力强，但在数据速率方面效率不高，一次只能选择整个频带中的一个进行数据传输。另一种可能的方法是**共轭附近的频带**，在其他条件不变的情况下，数据速率与频带成正比，可以直接将数据速率翻倍。但这两种可能的方法需要对整个系统进行修改，目前不太可能实现。

蓝牙的未来——更节能

在物联网中，更节能的网络总是受欢迎的，BLE和蓝牙mesh都专门针对低功耗应用进行了优化。BLE采用占空比模式，通过缩短工作时间来节省功耗；Bluetooth Mesh提出异构结构来节省低功耗节点的功耗。

解决这个问题的一个可行方法是**研究机制**，以决定如何执行占空比模式以获得更好的能源效率，例如使用不同的数据速率。此外，近年来**后向散射应用**蓬勃发展，显著降低了通信功耗。特别是，研究人员提出了可以通过后向散射蓝牙信号进行通信的原型，可用于设计更节能的蓝牙网络。

蓝牙的未来——更安全

蓝牙瞄准的是工业物联网市场，对利润和员工安全来说，可靠性和安全性问题都是最重要的。

蓝牙网络面临多种威胁，如设备密集型应用中的**干扰攻击**。尽管跳频和安全机制有助于抵御此类威胁，但在调查不同的干扰攻击时，它的效果如何仍有待观察。

在基于泛洪的网络中，所有消息都可以被覆盖范围内的任何节点接收，这可能会导致**隐私泄露**。

蓝牙的未来——更深层

作为一种通信技术，蓝牙提供的物理层信息仅仅是消息的粗糙特征，这为利用蓝牙进行更精确的定位提供了机会。如果更多的蓝牙物理层信息对研究人员开放会怎么样?

例如，Wi-Fi中信道状态信息（CSI）的引入使得基于Wi-Fi的定位精度有了很大提高，因此在静态环境中具有更好的抗噪声和室内常见的频率选择性衰落现象的能力，也可以用于手势识别。

Wi-Fi和蓝牙信号具有不同的波形，蓝牙使用的带宽也比Wi-Fi要小。由于空间分辨率与带宽有关，蓝牙可能无法达到Wi-Fi那样高的精度。

但是，差异并不一定意味着不可能，而是可能带来新的机会，为蓝牙留下了更多的研究可能性。

总结

ZigBee、Z-Wave、Wi-Fi等众多技术提供了异构的服务，以满足不同应用所带来的多样化需求。现在蓝牙在**覆盖范围、速度、广告、健壮性和网络容量**方面都有了全面的改进，不仅巩固了其在商业应用上的优势，而且拓展了其在学术研究上的可能性。尽管未来难以预测，但蓝牙已经成为未来强有力的竞争对手，为满足物联网领域的通信需求提供了完整的解决方案。

THE END

THANKS