Bluetooth®

解析蓝牙 mesh 网络

开发者入门

mesh 是蓝牙低功耗（Bluetooth® LE）的一种全新网络拓扑结构选择，于 2017 年夏季推出。它代表蓝牙技术的一项重要进 展，将蓝牙定位为包括智能楼宇和工业物联网在内的各大新 领域和新用例的主流低功耗无线通信技术。

目录

致谢：

Bluetooth®

Martin Woolley
作者

Sarah Schmidt
美术设计

1.0 引言

1.0 介绍

自 2000 年初的第一次发布起，蓝牙积极开发的脚步 就从未停歇。初期，蓝牙的主要是用作替代缆线技 术，但很快便拓展到了主流无线音频产品和计算机外设，如无线鼠标和键盘。

2010 年，蓝牙低功耗的推出成为了蓝牙技术向前发展的重要一步。其影响重大，受到广泛关注，尤其是在智能手机和平板电脑、以及健康与健身、智能家居和可穿戴产品领域。

事实证明，基于 mesh 网络拓扑的无线通信系统提供 了一种行之有效的方法，可实现大面积的覆盖范围、扩展传输范围、并提供恢复能力。然而到目前为止，它们都是基于利基技术，与消费者拥有的、或企业中使用的大多数计算机、智能手机和辅助设备并不兼容。

有多达 120 家蓝牙技术联盟成员公司参与到了为蓝牙提供 mesh 网络支持所需的工作之中，这也是史无前例， 也体现了业界对蓝牙 mesh 网络功能达成全球行业标准的需求。

添加 mesh 网络支持体现了一类变化，变化如此之大， 被认为是蓝牙技术的范式转变。

2.0
掌握控制权

2.0 掌握控制权

让智能楼宇真正变智能

想象一下，当你在寒冬天还未亮时就早早驱车到达办公室，安全系统能够为您放行，并自动分配停车位。停车位上的区域号码灯亮起，让您能够轻松驶入。停车位分配系统会相应地更新，让后来者知晓该空间已被占用。

进入楼内，占位传感器会注意到您的到来，并通过穿戴式技术对您进行个体识别。您乘坐电梯到二楼，走向出口。像往常一样第一个到达。当电梯门打开时，从电梯到您办公室和厨房的灯光亮起。其他地区仍保持关灯状态，以节省电力。

您走进办公室，关上身后的门。 LED 射灯和您的台灯已 经开启，并且完全符合您喜欢的亮度水平。您注意到温 度比办公室主区域会暖一些，这也符合您的个人偏好。当您走近您的计算机时，计算机便会自动登录。

您的一天顺利开始，楼宇会根据您的需求作出回应、同时考虑到您的偏好。很显然，系统的利用相当有效。那么，是什么使这成为可能呢？

几个月前，您的公司安装了蓝牙 mesh 网络。最初从 mesh 照明系统开始，后来还添加至占位传感器、环境传感器、无线温控系统和基于 mesh 的停车场管理系统。公司在用电、取暖等方面能够节约成本，工作环境也变得个性化，提高了个人生产力。

维护成本正在下降，因为添加如附加照明开关等物件不再需要昂贵且具有破坏性的物理接线。数据让楼宇的管理团队能够了解建筑物、其所提供的服务、以及人们在其中的行为，并使用这些数据进行优化。

蓝牙 mesh 网络能够更简单、以更低的成本来进行楼宇服务的控制、与其进行无线交互、并实现自动化的操 作。您会不禁感叹在没有如此先进的楼宇技术的过去， 您是如何生活的！

图 1 - A 蓝牙 mesh 网络的覆盖范围可跨越办公室和停车场

3.0 蓝牙 mesh 基础知识

3.0 蓝牙 mesh 基础知识

概念和术语

读者朋友们，您若想了解蓝牙 mesh 网络拓扑结构，就先要了解蓝牙世界中所没有的一系列新的技术术语 和概念。在本章节中，我们将探讨一些最基本的术语 和概念。

mesh vs. 点对点

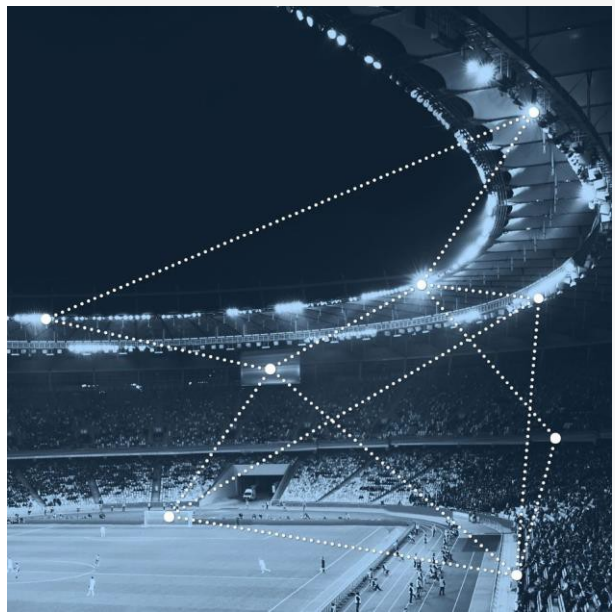
大多数蓝牙低功耗设备使用一对一设备通信的简单点对点网络拓扑结构来进行相互间的通信。在蓝牙核心规格中，这称为“微微网”。

想象一下，智能手机已经建立了与心率监测仪的点对点连接，并可借此传输数据。蓝牙的优点之一就是让设备能够建立多个连接。同样的智能手机也可以建立与活动跟踪设备的点对点连接。在这种情况下，智能手机可以直接与其他每台设备进行通信，但其他设备彼此之间无法直接通信。

相比之下，mesh 网络具有多对多拓扑结构，每台设备都能够与 mesh 网络中的任何其他设备进行通信（稍后我们将在题为“蓝牙 mesh 在行动”的部分中进行更详细的阐述）。通信是基于消息的使用，且设备能够将消息中继至其他设备，使端到端通信范围得以扩展，远远超出每个单独节点的无线电范围。

设备和节点

mesh 网络中的设备称为节点，非 mesh 网络中的设备 称为“未经启动配置的设备”。



将未经启动配置的设备转换为节点的过程称为“启动配置”。您可以考虑购买一款支持 mesh 的新蓝牙 照明灯，将其带回家并进行启动设置。为了使其成为 mesh 网络的一部分，以通过现有的蓝牙照明开关 和调光器进行控制，您需要进行启动配置。

启动配置是一个安全的过程，原本未经启动配置的设备经过启动配置后会拥有一系列加密密钥，并被启动配置的设备（通常是平板电脑或智能手机）识别。其中一个密钥称为网络密钥或简称为 NetKey。 您可以在下面的“安全性”部分阅读到有关 mesh 安 全的更多信息。

mesh 网络中的所有节点都具有至少一个 NetKey，设备必须拥有该密钥才能成为加入相应的网络，并成为节点。在节点投入使用之前，还有其他一些要求，但通过启动配置过程安全地获取 NetKey 是基本 的第一步。我们将在本文的后续部分中详细介绍启动配置过程。

元素

一些节点具有多个组成部分，每个都能独立进行控 制。在蓝牙 mesh 术语中，这些部分被称为“元素”。

图 3 显示了一种 LED 照明产品，如果将其添加到蓝牙 mesh 网络中，则将形成具有三个元素的一个节点，每一个 LED 灯为一个元素。

图 3 – 由三个元素构成的照明节点

消息

当某一节点需要查询其他节点状态，或需要以某种方式控制其他节点时，会发送合适类型的消息。如节点需要向其他节点报告自身状态，则会发送消息。

mesh 网络中的所有通信均“以消息为中心”，且定义了多种消息类型，每种均有自己独特的操作码。

消息分为两类：有应答、或无须应答的消息。

有应答的消息需要收到节点的响应。该响应有两个目的：确认与其相关的消息已被接收，并将与消息接收方有关的数据返回给消息发送方。

如果有应答的消息的发送方没有收到预期响应，则有应答的消息的发送方可以重新发送消息，因此有应答的消息必须是幂等的。这意味着给定的有应答的消息多次到达某个节点的结果将与其仅被接收一次相同。

无须应答的消息则无需响应。

地址

消息必须从一个地址发送到另一地址。蓝牙 mesh 定义了三种类型的地址。

单播地址仅可识别单一元素。在配置过程中，单播地 址被分配给设备。

群组地址是表示一个或多个元素的多播地址。群组地址由蓝牙技术联盟定义，称为蓝牙技术联盟固定群组地址（SIG Fixed Group Addresses），也可以动态分配。 目前已经定义了 4 组蓝牙技术联盟固定群组地址，分别为 All-proxy、All-friends、All-relay 和 All- nodes。本文稍后将介绍代理、好友和中继这几个用
语。

我们期望动态群组地址将由用户通过配置应用程序建立，且它们将能够反映楼宇的物理配置，例如定义与楼宇中的每个房间对应的群组地址。

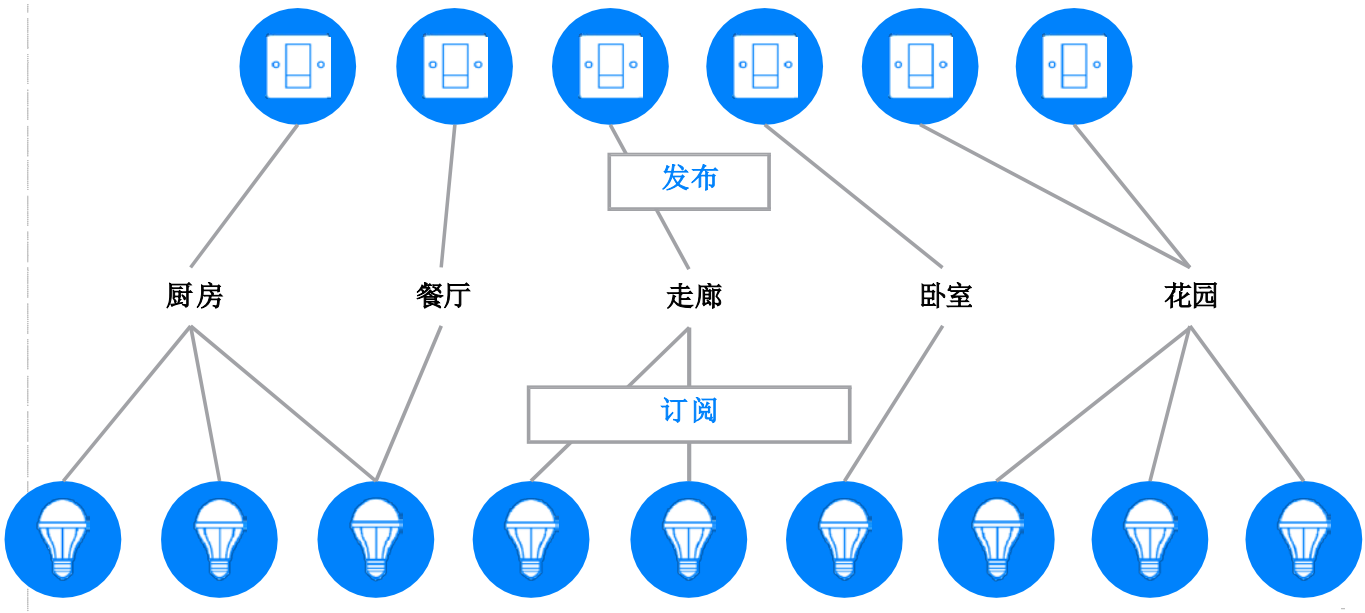


图 4 – 发布/订阅

虚拟地址是可以分配给跨越一个或多个节点的一个或多个元素的地址。它采用 128 位 UUID 值的形式，任何元素都可以与之相关联，基本上相当于一个标签。

虚拟地址可在制造过程中进行预先配置，用于类似轻松定位出自该制造商的所有会议室投影机等场景。

发布/订阅

发送消息的行为称为发布。节点被配置为可选择发送到特定地址进行处理的消息，这被称为订阅。

通常，消息被发送到群组或虚拟地址。群组和虚拟地址名称已广为最终用户所知，易于使用。

在上面的图 4 中，我们可以看到节点“1 号开关”发布 至群组地址“厨房”节点 ，1 号电灯、2 号电灯和 3 号电灯均订阅了厨房的地址，因此可接收并处理发布到 该地址的消息。换句话说，可以使用 1 号开关开启或关闭 1 号电灯、2 号电灯和 3 号电灯。

2 号开关发布到群组地址“餐厅”。只有 3 号电灯订阅了这一地址， 因此是 2 号开关控制的唯一一盏电灯。请 注意，这一例子也说明了节点可以订阅一个以上不同地址的消息——既强大又灵活。

同样地，注意节点 5 号开关和 6 号开关两者是如何发布至同一个“花园”地址的。

使用发布/订阅通信模型的群组和虚拟地址具有额外的实质性好处，因为无需重新配置其他节点就能在网络中删除、替换节点，或添加新节点。您可以思考一下在餐厅安装额外的照明灯将涉及哪些问题。新设备将使用预设流程添加到网络，并配置为订阅餐厅地址。其他节点均不会受到网络中这一改变的影响。2 号开关将一如既往地将消息发布到餐厅，但现在 3 号电灯和新 添加的电灯都会对其作出响应。

状态和属性

元素可以处于不同条件中，这在蓝牙 mesh 中以状态值这一概念来体现。

状态是某个类型的值，包含在一个元素内（在服务器模型中，见下文）。与值相同，状态也有相关行为，不得在其他情况下重复使用。

举个例子，设想一下可以开启或关闭的简易照明灯。蓝牙 mesh 定义了一个名为 Generic OnOff 的状态。电灯将具有该状态项，并且 On 的值对应于并引发亮灯，而 Off 将反映并导致电灯关闭。

术语“泛型”的意义将在后文中讨论。

属性类似于状态，因为它们包含与元素相关的值。但 在其他方面，它们与状态的差异较大。

熟悉蓝牙低功耗的读者会了解特性，并回想起这种数 据类型并没有相关的定义行为，使得它们能够在不同 的情境中重复使用。属性提供了能够解释特性的情境。

为了解属性相关情境的意义和使用，例如，想一下特 性“Temperature 8”——8 位的温度状态类型，其具有多个相关属性，包括“当前室内环境温度”和“当前室外环境温度”。这两个属性让传感器能够发布传 感器读数，让接收的客户端能够确定温度值中包含的情境，更好地理解其真实含义。

属性分为两类：制造商和管理员。制造商为只读类别，管理员则允许读写访问。

消息、状态和属性

消息是调用 mesh 中操作的机制。形式上，给定的消息类型表示针对某一状态或多个状态值集合的操作。所有消息都有三种广义上的类型，反映了蓝牙 mesh 支持的操作类型。三种类型的缩写为 GET、SET 和 STATUS。

GET 消息需要来自一个或多个节点的给定状态值。STATUS 消息的发送是对 GET 的响应，且其中包含相关的状态值。

SET 消息会更改给定状态的值。经确认的 SET 消息将导致 STATUS 消息被退回，以作为对 SET 消息的响应；而未经确认的 SET 消息则无需响应。

STATUS 消息的发送是对 GET 消息、经确认的 SET 消息、或其他独立的消息的响应，可由发送消息的元素上运行的定时器驱动。

通过消息操作码可推断消息引用的具体状态。另一方面，在使用 16 位属性 ID 的通用属性相关消息中，属性也被明确引用。

状态转换

从一个状态到另一个状态的改变称为状态转换。转换可能是瞬时的，或在一段时间内则被称为过渡时期。状态转换可能会对节点的应用层行为产生影响。

绑定状态

状态之间可能存在关系，一种状态的变化会触发另一种状态发生变化。这种关系被称为状态绑定。一种状态可能与其他多种状态绑定。

例如，思考一下由调光开关控制的照明。照明的状态 有二：Generic OnOff 和 Generic Level，两者相互 绑定。调暗照明亮度，直到 Generic Level 值为零（完全变暗），就会导致 Generic OnOff 从 On 变为 Off。

模型

模型将上述概念聚合在了一起，并定义了 mesh 网络相关元素的某些或全部功能。三类模型已得到认可。

服务器模型定义状态、状态转换、状态绑定、和包含这一模型的元素可能发送或接收的消息集合。它还定义了与消息、状态和状态转换有关的行为。

客户端模型不定义任何状态。相反，它定义了自身可以发送或接收的消息，以便获取（GET）、设定（SET）或询问相应服务器模型中定义的状态（STATUS）。

控制模型包含一个服务器模型和一个客户端模型。服务器模型可与其他客户端模型进行通信，客户端模型可与服务器模型进行通信。

模型可以通过扩展其他模型来创建。不可扩展的模型称为根模型。

模型是不可变的，这意味着它们可能不会因添加或删除行为而改变。为落实新模型要求，正确且唯一可行的方法就是扩展现有模型。

通用定义

我们已经认识到许多不同类型的设备通常具有语义上等价的状态，例如 ON 与 OFF 这样简单的意思。想一下 电灯、风扇和电源插座，所有这些都可以被开启或关闭。

因此，蓝牙 mesh 模型规格定义了一系列可重复利用的 通用状态，如 Generic OnOff 和 Generic Level。

与之类似，还定义了一系列基于通用状态的通用消息。 如 Generic OnOff Get 和 Generic Level Set。

通用状态和通用消息用于广义模型，包括通用服务器模型，如 Generic OnOff 服务器，以及通用客户端模 型，如 Generic Level 客户端。

泛型让广泛的设备类型能够支持蓝牙 mesh，而无需创建新的模型。记住，模型可以通过扩展其他模型来 创建。因此，通用模型可能会为快速创建新型设备的 模型打下基础。

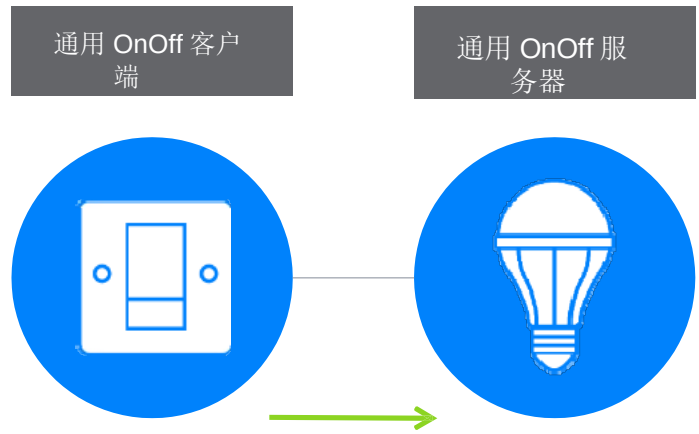


图 5–通用模型

场景

场景是存储的状态集合，可以通过接收特定类型的消息、或在指定时间被调用，使其成为当前状态。场景通过 16 位场景编号来识别，该场景编号在 mesh 网络中是唯一 的。

场景允许在一个协调的动作中，将一系列节点设置为一组先前存储的互补状态。

想象一下，傍晚时分，您喜欢将家中主要空间的温度设置为 20 摄氏度，6 个 LED 射灯将处于一定的亮度水平，并且房间角落桌子上的灯光也设置为恰到好处的黄色调。在本示例场景中，手动将各种节点设置为以上状态，您就能够使用配置应用程序将其存储为场景，并可随时通过发送适当的、与场景相关的 mesh 消息，或者在计划的时间自动启动场景设置。

启动配置

启动配置是设备加入 mesh 网络并成为节点的过程。它涉及几个阶段，会生成各种安全密钥，并且本身是一个安全的过程。

可使用平板电脑等设备上的应用进行预置。在这种情 况下，用于驱动预置过程的设备称为启动配置设备（Provisioner）。

预置过程通过五个步骤进行，这些步骤将在下面进行 描述。

第 1 步. Beacon 广播

为支持各种不同的蓝牙 mesh 功能（包括但不限于预 置），已经引入了全新的 GAP 广播类型（参考：蓝 牙核心规格附录），包括<<mesh Beacon>> 广播类型。

未经预置的设备会通过使用广告封包中的<<mesh Beacon>> 广播类型来指示其可用性。用户可能需要以这种方式启动新的设备广播，例如按下按钮组合、 或按住某个按钮一段时间。

第 2 步. 邀请

在此步骤中，启动配置设备将以启动配置邀请 PDU（Provisioning Invite PDU）的形式向要进行启动配置设备发送邀请。

Beacon 设备会作出响应，即在 Provisioning Capabilities PDU 中回复关于自身的信息。

第 3 步. 交换公共密钥

启动配置设备和要进行预置的设备可以直接或者通过带外（OOB）方式交换他们的公共密钥，这些密钥可以是静态或暂时的。

第 4 步. 认证在认证步骤期间，要进行启动配置的设备会通过一种适合其功能的动作，以某种形式向用户输出一个随机
的单位或多位数字。例如，它可能会闪烁 LED 灯数次。用户将新设备输出的数字输入到启动配置设备中，两台设备之间进行这一随机数的加密交换，以完成两个设备彼此之间的认证。

第 5 步. 启动配置数据的分配认证成功完成后，会通过两台设备的私有密钥和交换 的对等公共密钥生成会话密钥。会话密钥随后用于保 护完成预置过程所需数据的后续分发，包括称为网络 密钥（NetKey）的安全密钥。

预置完成后，经预置的设备会具备网络的 NetKey，这是一项 mesh 安全性参数，也称为 IV 索引和单播地 址，由启动配置设备进行分配。现在被称为节点。

特性

所有节点均可发送和接收 mesh 消息，但节点可能拥有许多可选特性，为其提供额外的特殊功能。有四种可选特性：中继、代理、好友和低功耗特性。节点可以支持这些可选特征中的零到多个，并且任何支持的特征均可在某一时间点被启用或禁用。

中继节点

支持中继功能的节点称为中继节点，能够重新传送接收到的消息。中继是消息可遍历整个 mesh 网络的机制，通过中继在设备之间进行多次“跳跃”。

mesh 网络 PDU 包括一个称为 TTL（生存期）的字段。它需要一个整数值，可限制消息将在网络中跳跃的次数。例如，将 TTL 设置为 3，则消息可被中继，从始发节点开始最多跳三次。将其设置为 0，则无法进行中继，且仅能实现单次跳跃。掌握了 mesh 网络拓扑结构和成员资格的一些基本知识，节点就能够使用 TTL 字段来更有效地使用 mesh 网络。

低功耗节点和好友节点

某些类型的节点供电方式受限，且需要尽可能地节省能耗。

此外，这类设备的工作可能主要涉及消息的发送，但仍然需要偶尔接收消息。

想想一个由小型纽扣电池供电的温度传感器。每当温度高于或低于配置的上限和下限阈值时，它每分钟会发送一次温度读数。如果温度维持在上下阈值内，则不发送消息。这些行为很容易实现，不存在造成功耗上升相关的特定问题。

此外，用户还能向传感器发送消息，其改变温度阈值状态值。这是一类相对罕见的事件，但传感器必须对此提供支持。接收消息的需求对占空比和功耗都有影响。100％的占空比将确保传感器不会错过任何温度阈值配置消息，但功率也会达到最高。低占空比将节省能耗，但传感器就可能存在遗漏配置消息的风险。

这个大难题的答案就是“好友节点”和友谊的概念。

类似于示例中的温度传感器节点可被指定为低功耗节点（LPN），且传感器配置数据中的特性标志也会将节点 指定如此。

LPN 与另一节点（其不受电源约束的节点，例如具有永久 AC 电源）协同工作。该设备称为“好友”节点。

“好友”能够存储发送到 LPN 的消息，并且每当 LPN 探询“好友”节点以求“等待处理的消息”时，就会将其发送到 LPN。 LPN 可能相对没那么频繁地探询“好友”，以便平衡其节省电力、以及及时接收和处理配置消息的需求。当它进行探询时，“好友”存储的所有消息将被一个接一个地转发到 LPN，并且具有被称为 MD（更多数据）的标志，向 LPN 指示“好友”节点处否还会发来更多消息。

LPN 和好友节点之间的关系称为“友谊”。需要接收消息、但功率受限的节点能够在蓝牙 mesh 网络中运行，同时持续以功率有效的方式运，关键就是靠“友谊”。

代理节点

世界上有大量的设备支持蓝牙低功耗，大多数智能手机和平板电脑都在其中。蓝牙 mesh 面世之时，市场上 的蓝牙设备并不具备蓝牙 mesh 网络对战。他们确实有 一个蓝牙低功耗堆栈，因此能够连接到其他设备，并与 GATT 通用属性配置文件进行交互。

代理节点暴露了一个 GATT 接口，蓝牙低功耗设备可使用该接口与 mesh 网络进行交互。定义了代理协议（意 在用作面向连接的承载，例如 GATT）之后，GATT 设 备在 Proxy 节点实施的 GATT 特征范围内读写代理协议 PDU。代理节点将这些 PDU 转换为 mesh PDU。

总而言之，代理节点让不具有蓝牙 mesh 堆栈的蓝牙低 功耗设备能够与 mesh 网络中的节点进行交互。

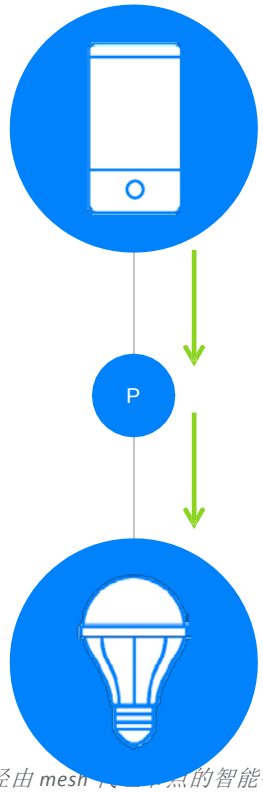


Figure 6–经由 mesh 代理节点的智能手机通信
P = 代理功能开启

节点配置

每个节点都支持在标准配置服务器模型中实施的一组标准配置状态，并使用配置客户端模型进行访问。配置状态数据涉及节点在 mesh 内的能力和行为，与任何特定应用或设备类型行为无关。

例如，节点支持的功能，无论是代理节点、中继节点等，都通过配置服务器状态进行指示。节点已订阅的地址存储在订阅列表中。指示节点所属网络的网络和子网密钥、以及该模式的应用密钥，均被列于配置块中。

一系列配置消息让配置客户端模型和配置服务器模型能够在配置服务器模型状态上支持 GET、SET 和 STATUS 操作。

4.0
mesh 系统架构

4.0 mesh 系统架构

总览

在本节中，我们将详细介绍蓝牙 mesh 架构、其中各 层次、以及各自的职责。我们还会将 mesh 架构定位 为类似于蓝牙低功耗核心架构。

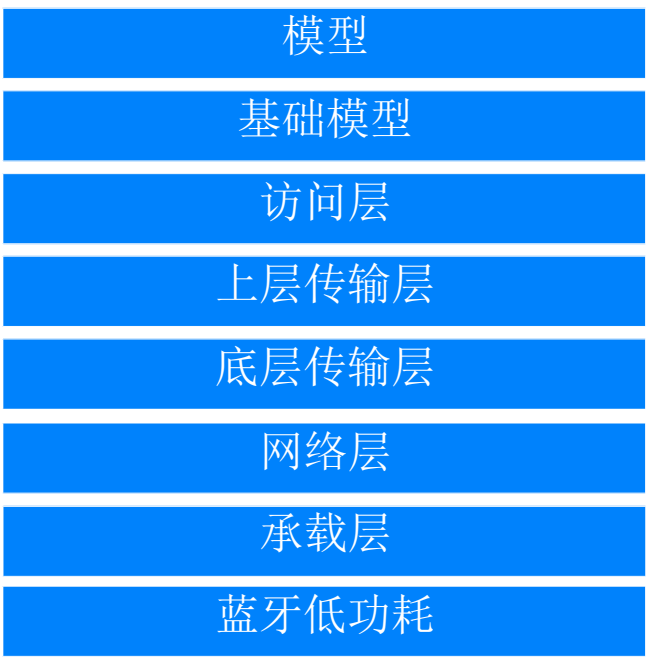


图 7–蓝牙 mesh 架构

在 mesh 架构堆栈底部，有一层名为“蓝牙低功耗”。实际上，这并非仅是 mesh 架构的其中一层，而是完整的蓝牙低功耗堆栈，是提供基础无线通信功能所必需的，这些功能可为位于其上的 mesh 架构所用。应该清楚的是，mesh 系统有赖于蓝牙低功耗堆栈的可用性。

现在就让我们回顾一下 mesh 架构的每个层次，从底层开始。

承载层

mesh 消息需要基础的通信系统来进行传输和接收。承载层定义了网络 PDU 如何由给定的通信系统进行处理。这时定义了两个承载层，即广播承载层和 GATT 承载层。

广播承载层利用蓝牙低功耗的 GAP 广播和扫描功能来传送和接收 mesh PDU。

GATT 承载层允许不支持广播承载层的设备间接地与 mesh 网络中的节点进行通信，mesh 网络使用的协议为“代理协议”，封装在涉及特定 GATT 特性的 GATT 操 作中。mesh 代理节点可实现这些 GATT 特性，并支持 GATT 承载层和广播承载层，以便在两种类型的承载层之间转换和中继消息。

网络层

网络层定义各种消息地址类型，以及允许承载层传 送传输层 PDU 的 mesh 消息格式。

它可以支持多个承载层，每个承载层可具有多个网络接口，包括用作同一节点部分元素之间通信的本地接口。

网络层决定了通过哪个网络接口输出消息。将输入滤波器应用于来自承载层的消息，以明确其是否应被递送至网络层以进行进一步处理。输出消息需要输出过滤器来控制是否将其丢弃或传送到承载层。

中继和代理功能可以由网络层来实施。

底层传输层

底层传输层从上层传输层接收 PDU，并将其发送到对 等设备的底层传输层。它会在所需之处执行 PDU 的分 段和重组。对于较长的数据包，无法通过单一的传输 PDU 进行传输，底层传输层将执行分段，将 PDU 分成 多个传输 PDU。在另一台设备上负责接收的底层传输 层，再将这些分段重新组合到上层传输层 PDU 中，并 将其传递到堆栈。

上层传输层

上层传输层负责对传入和传出接入层的应用数据进行加密、解密和认证。它还负责传输控制消息，这些消息生成于内部、并发送于不同对等节点的上层传输层之间，包括与“友谊”和“心跳”相关的消息。

访问层

访问层负责定义应用如何利用上层传输层，包括：

- 定义应用数据的格式。
- 定义并控制在上层传输层执行的加密和解密过程。
- 在将数据上传到堆栈之前，对来自上层传输层的数据进行验证，判断其是否适用于该网络和应用。

基础模型层

基础模型层负责 mesh 网络的配置和管理相关模型的 实施。

模型层

模型层涉及模型的实施，因此涉及一个或多个模型规格中定义的行为、消息、状态、状态绑定等的实现。

5.0
安全性

5.0 安全性

mesh 安全性为强制性

蓝牙低功耗让配置文件设计人员能够利用一系列不同的安全机制，从各种可能的配对方法、到与个人特性相关的个人安全性要求。事实上，安全性是完全可选的，也允许设备完全开放，没有安全保护或限制。设备设计者或制造商负责分析威胁，并明确其产品的安全要求和解决方案。

相比之下，在蓝牙 mesh 中，安全性则为强制性的。网络、个人应用和设备都必须是安全的，不能以任何方式关闭或降低安全性。

图 8 – 安全性是蓝牙 mesh 网络的中心

mesh 安全性之基础

以下基本安全声明适用于所有蓝牙 mesh 网络：

1. 所有 mesh 消息都经过加密和认证。
2. 网络安全性、应用安全性和设备安全性彼此独立。 请参阅下面的“问题分离”。
3. 通过密钥刷新过程，可以在 mesh 网络的整个生命周期内更改安全密钥。
4. 消息模糊化使得对外界难以跟踪网络内所发送消息，提供了一种隐私保护机制，让外界难以节点。
5. mesh 安全性可保护网络免受中继攻击。
6. 设备添加到 mesh 网络以成为节点的过程本身就是一个安全的过程。
7. 节点可从网络中安全地移除，此方式也能防止垃圾 邮件攻击。

问题分离和 mesh 安全密钥

蓝牙网络安全的核心是三种安全密钥。在它们之间，这些密钥为 mesh 的不同方面提供了安全性，并实现了 mesh 安全性中的关键性能，即“问题分离”。

要理解这一点并认识到其重要意义，请思考一下可用于中继的 mesh 照明。当它发挥中继功能时，可能会去处理与楼宇蓝牙网门窗安全系统有关的消息。照明无需访问和处理这些消息的细节，但是需要将它们中继到其他节点。

为处理这种潜在的利益冲突，mesh 使用不同于用来保护 照明、物理安全、温控等特定应用相关数据的安全密钥， 来保护网络层的消息。

mesh 网络中的所有节点都拥有**网络密钥（NetKey）**。实际上，正是拥有这一共享密钥，才使得节点成为网络的成员。网络加密密钥和隐私密钥直接从 NetKey 导出。

拥有 NetKey 让节点能够对网络层进行解密和验证，以便执行诸如中继等网络功能。但应用程序数据不可被解密。

网络可以被细分为子网，每个子网都有自己的 NetKey， 且只有那些作为该子网成员的节点才拥有 NetKey。例如， 它可以用来隔离特定的物理区域，例如酒店的各个房间。

特定应用的应用数据只能由具有正确**应用密钥（AppKey）**的节点解密。在 mesh 网络的节点中，可能有许多不同的 AppKey，但通常情况下，每个 AppKey 只能为一小部分节点所拥有，即可以参与到给定应用之中。例如，照明和照明开关将具有照明应用的 AppKey，而不具有用于温控系统的 AppKey，后者只有恒温器、散热器阀等才拥有。

上层传输层使用 AppKeys，在将消息传递到访问层之前，对消息进行解密和验证。

AppKeys 只与一个 NetKey 关联。这种关联被称为“密钥绑定”，并且意味着由所拥有的给定 AppKey 定义的特定应用仅能在一个特定网络上工作，而网络可以托管多个独立、安全的应用。

最后一种密钥类型是**设备密钥（DevKey）**。这是一种特殊类型的应用密钥。每个节点都有一个唯一的 DevKey，仅为 Provisioner 知晓。在预置过程中，可使用 DevKey 来确保 Provisioner 和节点之间的通信。

节点移除、密钥刷新和垃圾邮件攻击

如上所述，节点包含各种 mesh 安全密钥。如果节点出现 故障，则需要处理，或者如果所有者决定将节点出售给另 一位所有者，则重要的是，该设备及其所包含密钥不能被 用来针对节点原来所在网络发动攻击。

我们对从网络中删除节点的过程进行了定义。启动配置设备（Provisioner）应用可用于将节点添加到黑名单，然后启动密钥刷新流程。

密钥刷新流程会作用于网络中的所有节点——除了黑名单中的成员，它们无法被授予新的网络密钥、应用密钥和所有相关的派生数据。换句话说，构成网络和应用安全性基础的整套安全密钥被替换。

因此，已从网络中删除、并包含原有 NetKey 和 AppKeys 组的节点就不再是网络的成员，也不再构成威胁。

隐私保护

从 NetKey 导出的隐私密钥用于对网络 PDU 的报头值进行模 糊化，例如源地址。模糊化可以确保无法通过随机的被动窃听来跟踪设备及其使用者。它也使得基于流量分析的攻 击变得难以实施。

这种技术提供的安全性可满足其目的。

中继攻击

在网络安全方面，中继攻击是窃听者拦截并捕获一个或多个消息、稍后重新进行传输的一种技术，目的是欺骗接收者，执行未经被攻击设备授权的任务。常见一个例子是汽车的无钥匙进入系统被攻击者击破，攻击者就能拦截汽车车主和汽车之间的认证序列，然后对这些消息进行中继，以进入汽车并将其偷走。

蓝牙 mesh 可保护网络免受中继攻击。这种保护的基础是分别使用称为序列号（SEQ）和 IV 索引的两个网络PDU 字段。每次发布消息时，元素会增加 SEQ 值。节点 从元素接收消息，如果元素包含的 SEQ 值小于或等于最 后有效消息中的 SEQ 值，则节点会将消息丢弃，因其可 能与中继攻击有关。IV 索引是一个单独的字段，需与SEQ 一同纳入考量。来自给定元素的消息中的 IV 索引值 必须始终等于或大于该元素的最后一个有效消息。

6.0 蓝牙 mesh 实际运作

6.0 蓝牙 mesh 实际运作

消息发布和传输

使用 Wi-Fi 的网络会围绕着一个中央网络节点，即路由 器，所有网络流量都经过此。如果路由器不可用，则会导致整个网络亦不可用。

相比之下，蓝牙 mesh 使用一种称为“管理型网络犯洪机制”的技术来传递消息。消息在由节点发布时被广播，而非直接路由到一个或多个特定节点。所有节点 均可接收来自直接处于无线电范围的节点的所有消息，并且如果配置为如此，则将对所接收的消息进行中继。中继涉及再次广播所接收到的消息，让与始发节点相距较远的其他节点也能接收到消息广播。

多路传输

蓝牙技术使用“管理型网络犯洪机制”的一个重要结果就是消息在网络中经由多条路径到达目的地。这就打造了一个高度可靠的网络，也是选择使用“网络洪泛”方式、而非在蓝牙 mesh 网络设计中采用路由的主要原因。

管理型网络泛洪

蓝牙 mesh 网络利用网络泛洪方法的优势，优化其操作，结果既可靠又高效。在蓝牙 mesh 网络中优化讯息洪泛工 作方式的措施出现于 “管理型网络泛洪”一词被业界所用之后。这些措施如下：

心跳

心跳信息周期性地由节点发送。心跳消息向网络中的其 他节点指示发送心跳的节点仍然有效。

另外，心跳消息包含的数据让接收节点能够根据达到它所需的跳数，来确定发送方的距离远近。这亦知识可在 TTL 字段中得以应用。

TTL

TTL（生存期）是所有蓝牙 mesh PDU 所包含的字段。它能够控制消息中继的最大跳数。TTL 的设置让节点能 够通过中继进行控制，并确保消息不会被中继至所需范围之外，以节约能耗。

心跳消息让节点能够确定所发布的每个消息的最佳 TTL 值应为多少。

消息缓存必须在所有节点实施消息缓存。缓存包含所有近期消 息，并且如果发现消息处于缓存中，即指示该节点之
前已经看到并处理了该消息，则消息立即会被丢弃。

友谊

蓝牙 mesh 网络中最有意义的优化机制可能是由好友节点和低功耗节点的组合所提供的。

如之前所描述的，好友节点可向与其相关联的低功耗节点提供消息存储和转发服务，让低功耗节点能够以高能效的方式运行。

消息的内部传递

接收消息的节点将堆栈从底层蓝牙低功耗堆栈，通过承载层，传递到网络层。

网络层应用各种检查方式，以决定是将消息传递到堆栈上方，还是将其丢弃。

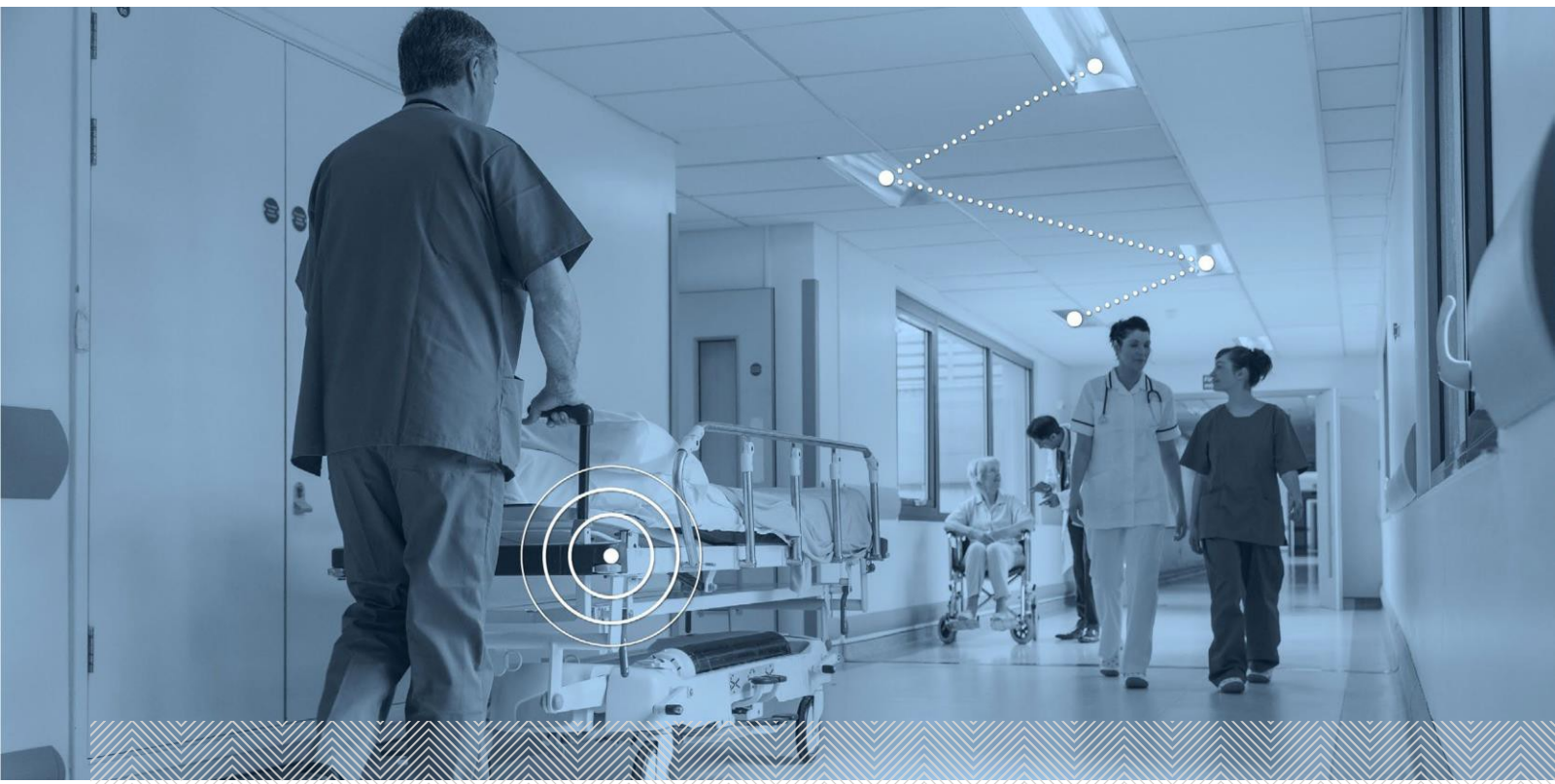
此外，PDU 具有网络 ID 字段，其提供了能够快速明确消 息采用哪种 NetKey 进行加密。如果接收节点上的网络层无法识别 NetKey，则表示它不具有相应的 NetKey， 不是该子网的成员，因此 PDU 会被丢弃。还有一个网络 消息完整性检查（MIC）字段。如果 MIC 检查失败，则 使用对应于 PDU 网络 ID 的 NetKey，则该消息被丢弃。

发送消息的节点所覆盖的传输范围内的所有节点均可接收该消息，但是因为节点所属的网络或子网，消息显然与该节点不相关时，许多消息将迅速被丢弃。

这一原理同样适用于较高的上层传输层中的堆栈。此处， 检查是针对消息相关的 AppKey，并由 PDU 中的应用标识符（AID）字段进行标识。如果该节点无法识别 AID， PDU 将被上层传输层丢弃。如果传输消息完整性检查（TransMIC）失败，则该消息被丢弃。

7.0 蓝牙 mesh 的全新领域

7.0 蓝牙 mesh 的全新领域



本文旨在为读者提供蓝牙 mesh 的基础介绍，包括关 键功能、概念和术语。mesh 是蓝牙，但不同于我们 以往所知。这是一种蓝牙技术，支持设备使用新的 拓扑结构，通过全新的方式进行通信。

最重要的是，蓝牙技术是应用最为普遍的低功耗无线技术，非常适合全新的用例和行业领域。

参考资料

[1] 蓝牙技术联盟，蓝牙 mesh 规格
详见: www.bluetooth.com/specifications/adopted-specifications

[2] 蓝牙技术联盟，蓝牙 mesh 模型规格
详见: www.bluetooth.com/specifications/adopted-specifications

[3] 蓝牙技术联盟，蓝牙 5 核心规格
详见: www.bluetooth.com/specifications/adopted-specifications

[4] 蓝牙技术联盟，蓝牙核心规格附录
详见: www.bluetooth.com/specifications/adopted-specifications