软件定义物理层反向散射系统的 OTA 配置方法

朱丰源 狄麒龙 柳卫星 田晓华
（上海交通大学电子信息与电气工程学院 上海 200240）

摘 要 反向散射通信技术是物联网领域近十年来受到持续关注的重要研究方向，为物联网设备提供了低功耗、低成本的上行通信手段。现有的反向散射研究主要集中在实现符合商用协议的反向散射通信。这些系统与早期的射频身份识别（RFID）系统相比，无需专用的 RFID 阅读器，节约了部署成本。尽管这些工作在支持 Wi-Fi、BLE、LoRa 和 ZigBee 等日常物联网协议方面取得了进展，但存在着软硬件固化的缺陷。这导致技术一旦芯片化就无法更改，而芯片化是实现 μW 级功耗所必需的。近期，软件定义物理层的反向散射通信技术被提出，使反向散射标签在异构无线网络中的协议配置更加灵活，从而提升了其在工业现场部署中的适配能力。然而，现有的软件定义物理层反向散射通信缺少无线配置的能力，无法彻底解决异构无线网络部署问题。本文探索了软件定义物理层反向散射的无线配置机制，首次在软件定义物理层反向散射通信中实现了空中编程（OTA），提出了一种支持 OTA 的反向散射软件无线电系统——ULPSDR。该系统主要基于 LoRa 芯片的 OTA 电路和支持软件定义物理层的反向散射通信电路组成，其中 OTA 电路为反向散射通信电路提供下行物理层配置。ULPSDR 的关键设计包含两个部分：低功耗的 OTA 协议设计与 OTA 电路小型化设计，分别解决了 OTA 设计过程面临的多节点共存下如何正确高效配置的挑战，以及 OTA 功能带来的电路尺寸增大的挑战。在协议设计部分，本文主要遵循三项设计原则：（1）每个节点具备唯一 ID；（2）系统应具备确认机制以确保可靠的数据包接收；（3）系统应具备冲突避免机制，以支持大规模部署。在电路小型化方面，本文优化了反向散射通信电路与 OTA 电路之间的射频链路复用，并通过电压域归并，减少了尺寸开销。与现有的软件无线电相比，该系统支持 OTA 配置，且实现了 58 μW 级低功耗、10 秒级的 OTA 配置时间，为物联网设备的大规模部署提供了低功耗通信和低功耗无线配置两大重要能力。

关键词 反向散射通信；空中编程；低功耗；电路小型化
中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2025.01589

The OTA Configuration Method for the Backscatter System Supporting Software-Defined Physical Layer

ZHU Feng-Yuan DI Qi-Long LIU Wei-Xing TIAN Xiao-Hua
（School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240）

Abstract Backscatter communication technology has been a significant and continuously evolving research area in the Internet of Things (IoT) field over the past decade, providing IoT devices with low-power and cost-effective uplink communication. Existing research on backscatter primarily focuses on achieving communication that complies with commercial protocols. Compared to early Radio Frequency Identification (RFID) systems, modern backscatter systems eliminate the need for dedicated RFID readers, reducing deployment costs. Although progress has been made in supporting pervasive IoT protocols such as Wi-Fi, BLE, LoRa, and ZigBee, these protocols suffer from hardware and software rigidity. This rigidity prevents modifications once the technology is

收稿日期：2024-11-13；在线发布日期：2025-03-26。本课题得到国家重点研发计划（2020YFB1708700）、国家自然科学基金青年科学基金项目（B 类）（61922055）、国家自然科学基金面上项目（61872233）资助。**朱丰源**，博士研究生，中国计算机学会（CCF）会员，主要研究方向为反向散射通信、低功耗物联网。E-mail：jsqdzhufengyuan@sjtu.edu.cn。**狄麒龙**，硕士，主要研究方向为空中编程、反向散射通信。**柳卫星**，硕士，主要研究方向为低功耗唤醒接收机、物联网空中编程技术。**田晓华**（通信作者），博士，教授，博士生导师，中国计算机学会（CCF）会员，主要研究领域为智能物联网体系结构、超低功耗超高并发无线通信技术、物联网无线定位技术、智能可穿戴设备。E-mail：xtian@sjtu.edu.cn。

integrated into circuits (ICs), which is crucial for achieving μW-level power consumption. Recently, software-defined physical layer (SD-PHY) backscatter communication has been proposed, enabling more flexible protocol configurations for backscatter tags in heterogeneous wireless networks, thus enhancing adaptability in industrial deployments. However, existing SD-PHY backscatter communication lacks wireless configuration capabilities, failing to fully address the challenges of heterogeneous wireless network deployment. This paper explores a wireless configuration mechanism for SD-PHY backscatter and, for the first time, implements Over-the-Air (OTA) configuration in such systems. We propose ULPSDR, a remotely configurable software-defined backscatter radio system. ULPSDR comprises an OTA circuit based on a LoRa chip and an SD-PHY backscatter communication circuit, where the OTA circuit provides downlink physical layer configuration for the backscatter communication circuit. The key design elements of ULPSDR include: (1) a low-power OTA protocol and (2) a miniaturized OTA circuit. These address two major challenges: ensuring efficient and accurate configuration in multi-node coexistence scenarios and minimizing circuit size while maintaining OTA functionality. For protocol design, this paper adheres to three principles: (1) each node must have a unique identity, (2) the system should implement an acknowledgment mechanism to ensure reliable packet reception, and (3) a collision avoidance method should be in place for network-scale configurations. For circuit miniaturization, we optimize RF chain reuse between backscatter and OTA circuits and integrate power supply circuits. Compared to existing software-defined radios (SDRs), ULPSDR supports OTA configuration while achieving 58 μW-level power consumption and a 10-second OTA configuration time. These features provide two critical capabilities for large-scale IoT deployments: low-power communication and low-power wireless configuration.

Keywords backscatter communication; over-the-air; low-power; circuit miniaturization

1 引 言

反向散射通信因其能够实现微瓦级别的功耗，长期以来备受学术界关注。RFID 技术是其商业化最成功的案例之一，主要在仓储、零售等领域提供快速便捷的清点和定位能力。然而，RFID 依赖专门设计的阅读器，成本较高，读取距离受限于无线电信号的传播衰减，通常在 10 m 以内，应用场景受限。

近年来，物联网领域提出了基于 Wi-Fi、BLE (Bluetooth Low Energy，低功耗蓝牙)等商用无线电设备的反向散射终端读取技术。然而，这些方法只能针对单一协议，而在实际的工业场景中，不同厂家采用的无线电基础设施有所不同，导致这些新技术无法迅速推广应用。为了解决这一问题，Zhu 等人[1]提出了支持物理层软件定义的反向散射通信(SD-PHY)，通过通用射频前端和通用基带，实现了软件可配置的反向散射通信。

然而，现有的软件定义反向散射通信无法实现无线配置，只能通过串口配置，这增加了其在工业场景下大规模部署后的升级维护成本。另一方面，传统支持空中编程(Over-The-Air，OTA)的物联网节点通常通过 Wi-Fi 或蓝牙实现，功耗高、应用局限性大，无法适应工业场景的长期部署。根据目前公开的研究成果，目前尚不存在支持 OTA 且通信功耗在微瓦级别的物联网终端。

针对这一现状，本文在软件定义物理层反向散射通信的基础上提出了一种支持 OTA 配置的反向散射通信终端——超低功耗软件定义无线电(ULPSDR)。其本质上是在 SD-PHY 基础上实现了基于 LoRa 协议的 OTA 模块和功耗管理模块。我们的设计目标是，在增加 OTA 功能的同时保持反向散射终端低功耗和小尺寸的优势。

在上述设计目标下，我们面临的挑战包括：(1) 如何确认反向散射终端成功配置；(2) 如何使得终端保持低功耗和小尺寸。为了解决这些挑战，我们的贡献包括：(1) 提出了一种适用于 SD-PHY 反向散射架构的 OTA 收发机子系统设计，包含配置协议，能够以低功耗提供有效的 OTA 结果反馈；(2) 提出了一种 OTA 电路与反向散射通信电路的联合小型

化设计方法，通过射频链路之间的天线复用降低电路尺寸，归并器件电压域降低电路复杂度；(3) 我们设计了硬件系统验证我们的设计，并在实际场景中实现了 OTA 配置，结果表明其能够实现 58 μW 的功耗和小于 10 s 的 OTA 配置时间，相比当前已有的支持 OTA 的物联网终端，功耗和 OTA 配置时间均显著降低。

2　相关工作

2.1　反向散射技术

自 2013 年华盛顿大学的 Liu 等人[2]首次提出一种利用电视信号进行供能和通信的反向散射通信系统——Ambient Backscatter 以来，反向散射技术已成为物联网领域中的一项重要技术。近年来，反向散射技术不断涌现。

2014 年，Kellogg 等人[3]创新性地提出了 Wi-Fi Backscatter 技术，将射频供电设备与现有商用 Wi-Fi 设备(如 Linksys 路由器和英特尔 Wi-Fi 网卡)相连接，实现了最高 1 kbps 的通信速率和最大 2.1 m 的通信范围。尽管通信速率不高，但这展示了将射频供电设备与现有互联网连接的可能性，这对射频驱动的物联网设备的大规模商用化至关重要。

2015 年，Ensworth 等人[4]实现了 BLE Backscatter，展示了如何调制反向散射信号以生成类似于传统无线设备传输的蓝牙广播信号。实验表明，商用蓝牙设备能够在超过 9.4 m 的范围内正确接收并显示反向散射标签产生的信号。这种反向散射方法不仅显著节省能量，同时保持了与数十亿现有蓝牙智能手机和移动设备的兼容性，为反向散射技术迈向大规模商用奠定了坚实基础。

2017 年，Zhang 等人[5]基于码字转换技术提出了 FreeRider，这是首个能够与多种已商用无线电技术(如 ZigBee、802.11g/n Wi-Fi 和蓝牙)进行反向散射通信的设备。FreeRider 标签在反散射过程中将原激励信号中的码字转换为同一码本中的另一个有效码字，从而使用户能够使用商用无线电设备解码反向散射信号并获取嵌入的信息。不论这些无线电传输的数据是什么，FreeRider 都能进行码字转换，使无线电仍能进行有效的数据通信。同年，华盛顿大学的 Talla 等人[6]提出了兼容商用 LoRa 硬件的超低功耗广域反向散射系统——LoRa Backscatter，可在 475 m 内的任意位置实现反向散射通信。

2022 年，上海交通大学的 Zhu 等人[1]提出了物理层软件定义系统(Software-defined PHY，SD-PHY)，并展示了如何使用 SD-PHY 以在反向散射网络中实现灵活的可重编程性。这将使研究人员不必再面对大量不必要的工程工作量，从而促进该领域的创新。通过 SD-PHY，标签的物理层行为可以通过配置一组参数来实现，这允许通用硬件生成符合各种无线协议的反向散射信号。

其他相关的工作还包括如下：2018 年 Van Huynh 等人[7]对环境反向散射，即利用环境中已有的无线电信号进行反向散射通信的工作进行了总结；2020 年 Yao 等人[8]总结了反向散射技术的发展历程与未来前景；2022 年张晓茜等人[9]对面向零功耗的反向散射通信工作进行了技术方面的综述，并给出了在 6G 中的应用前景；2022 年 Yuan 等人[10]给出了一种面向环境中 Wi-Fi 信号、ZigBee 信号和 BLE 信号等多种不同协议信号的反向散射通信系统，无需显式地切换协议；2023 年 Gong 等人[11]针对环境反向散射通信的工作进行了研究现状的综述；2024 年 Gu 等人[12]给出了反向散射通信技术的发展现状并总结了面临的干扰、信道衰落等瓶颈；2024 年，Peng 等人[13]提出了用射频开关和阻抗网络统一射频架构，通过 OFDM 调制流程实现了 Wi-Fi、BLE 和 LoRa 反向散射信号的灵活生成，但局限于给出射频前端设计。

2.2　空中编程技术

空中编程是一种为电子设备分发新软件和配置的方法。随着移动电子设备的普及，OTA 功能的重要性日益凸显。在现代智能手机等移动设备中，OTA 更新通常指通过 Wi-Fi 或移动宽带分发设备所需的固件或操作系统更新。然而，在物联网应用场景中，常常需要对由数百或数千节点组成的网络进行配置。使用 Wi-Fi 进行配置的覆盖范围有限，难以满足大规模场景的需求；而使用蜂窝网络进行配置则会增加节点的功耗，降低其工作寿命。因此，近年来，基于低功耗协议的 OTA 方法在物联网场景中逐渐增加，如 802.15.4、ZigBee、LoRa 等协议。目前也已经存在软件定义无线电 TinySDR 采用 LoRa 协议作为远程 OTA 的方式[14]。然而，现有的空中编程技术需要完全覆盖式写入新的固件，配置数据量较大，所需的无线传输时间久、效率低。

3　系统设计

ULPSDR 的系统整体工作流程如图 1 所示，

OTA 网关将包含物理层参数的配置信息发送给 ULPSDR 终端，将其物理层进行修改，使得其适配当前部署的网络协议，如 BLE、Wi-Fi，或 LoRa 等；在 ULPSDR 收到 OTA 网关的物理层配置信息后，会将配置参数写入 SD-PHY 软件定义物理层基带，并通过控制通用反向散射通信射频前端，包含射频开关、检波二极管等，与无线网络环境进行交互，实现反向散射通信协议的敏捷适配。其中，SD-PHY 基带中包含了对反向散射通信物理层的抽象化描述和高效的通用化实现，根据寄存器状态改变比特-波形的映射规则。在前期的工作中[1]，已经对 SD-PHY 基带的设计以及与协议的敏捷适配性进行了论述，本文重点介绍 ULPSDR 系统的 OTA 远程无线配置机制的设计。

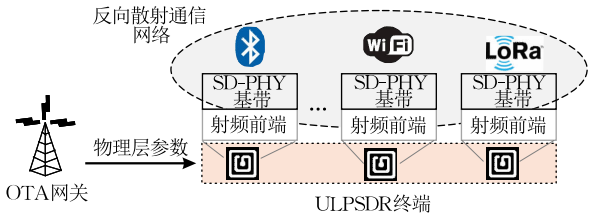


图 1 系统整体工作流程

为了实现基于软件定义物理层反向散射标签的远程配置，我们整体上选用 LoRa 技术作为配置的通信协议。这主要基于两点考量：(1) 首先，我们需要 OTA 的距离足够远，这使得实际部署中我们可以用尽量少的配置网关来实现各节点的 OTA 覆盖，降低复杂度和成本，这与 LoRa 协议的能力相符合；(2) SD-PHY 本身的配置信息数据量仅 2 kB～3 kB，仅需要 kbps 级别的传输速率，这与 LoRa 的数据率较为符合。在选定 LoRa 作为 OTA 的主要技术手段后，我们需要考虑是采用常规的主动式商用 LoRa 芯片还是采用被动的 LoRa 解调作为接收的主要手段。尽管采用后者将可以带来更低的功耗，并且可以与反向散射通信的接收机进行复用，但当前的 LoRa 低功耗接收机设计[15-16]灵敏度较差，难以实现远距离覆盖，且可能导致 OTA 数据的大量误码。基于上述考虑，我们选择将商用的主动式 LoRa 芯片与反向散射节点在软件和硬件两个方面进行整合，构建一个支持远程 OTA 配置的基于 LoRa 通信协议的软件定义物理层反向散射系统——ULPSDR。ULPSDR 系统架构如图 2 所示。

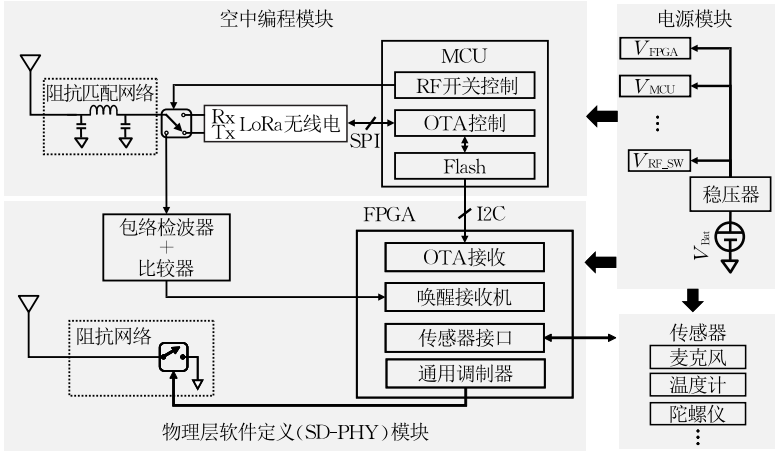


图 2 ULPSDR 系统架构框图

OTA 配置的工作流程如下：LoRa 配置端向周围发送广播信号，反向散射节点接收到广播信号后返回应答信号及其自身地址；LoRa 配置端根据反向散射节点发送的地址信息，有选择地配置特定地址的反向散射节点。每发送一个配置指令，LoRa 配置端在接收到相应终端标签设备的应答信号后决定是否继续发送，如未在规定时间内收到应答信号，则开启重传模式，以确保配置的可靠性。

在实现基于软件定义物理层反向散射标签的远程配置过程中，我们主要面临两个挑战：

第一，如何设计通信协议，以确保配置端能确认反向散射通信节点成功接收配置信号；

第二，如何设计电路，使其符合反向散射节点的小尺寸要求。

针对第一个挑战，我们通过详细设计配置端和反向散射节点的通信协议、通信帧结构和图形化配置方法，来确保反向散射通信节点成功接收到配置信号。针对第二个挑战，我们基于射频开关进行射频链路的天线复用，并设计电压域归并工作电压，从而减少电路尺寸和复杂度。

3.1　OTA 配置收发系统设计

(1) 配置系统通信协议设计

第一，广播与节点选择性。本文所设计的 OTA 配置系统主要应用于大规模反向散射节点的配置。在这种场景下，每个节点可能使用不同的配置协议，如 Wi-Fi、BLE 或 ZigBee 等。因此，配置端需要根据不同节点的需求进行配置，这就引出了节点地址与广播的设计。在广播阶段，待配置的节点会发送其 ID 值，使配置端能够有选择地对节点进行配置。

第二，物联网的无线通信环境较为复杂，通信条件变化迅速，因此需要确保反向散射通信节点能够成功接收到配置信号。为此，本文对系统引入了应答信号 ACK(Acknowledgement)。对于配置端发送的所有指令，包括广播指令、配置指令和休眠指令，待配置端均需进行应答。

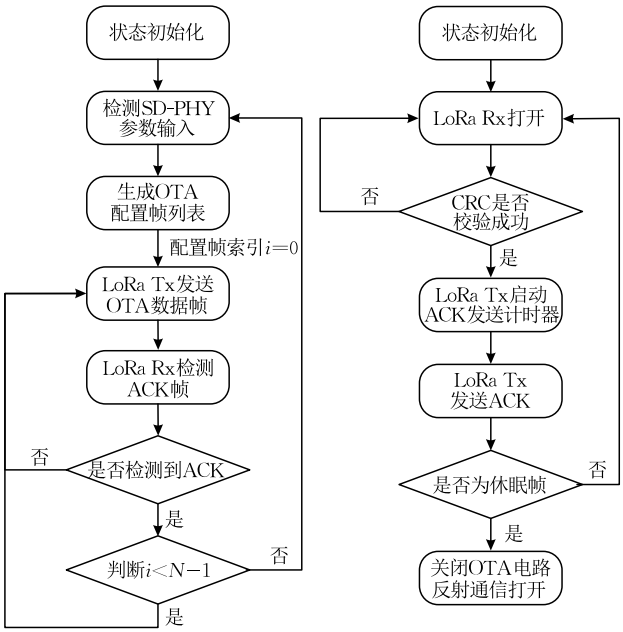
此外，系统采用超时重传机制。由于待配置端多次接收相同配置指令的效果相同，因此配置端在未接收到 ACK 信号时，会进行最多三次的超时重传，以确保配置指令的可靠传输。此外，为进一步确保配置指令的可靠性，系统中还增加了 CRC(Cyclic Redundancy Check)校验机制，配置端与待配置端在发送指令时均加入 CRC 校验。

第三，在大规模反向散射节点的应用场景中，由于所有节点均使用相同的 LoRa 通信链路，ACK 信号容易发生碰撞。为此，ULPSDR 系统采用了随机延时设计。反向散射节点在接收到指令后，会随机等待一段时间再发送 ACK 信号，这段等待时间与节点自身的 ID 相关，其具体计算如式(1)所示。

$$t_{\text{delay}} = Hash(Device_{ID}) + rand() \tag{1}$$

式中，哈希值的计算可以自定义，常见的哈希公式有：简单模运算哈希函数、乘法哈希函数、基于质数的哈希函数等。并且，反向散射节点的 ID 值是可以自定义的，所以可以通过控制节点 ID 值和哈希函数，加上随机函数 $rand()$，将碰撞的概率降到很低的区间。

为了方便理解，我们将 OTA 网关的状态机与 ULPSDR 终端的状态机在图 3 中展示。OTA 网关的工作流程如图 3(a)所示：首先进行初始化，检测用户输入的 SD-PHY 参数输入；将上述参数输入转换成 OTA 配置指令列表后，网关按照配置列表开始从第一帧广播 OTA 数据帧，发送完一帧后检测 ACK；若检测到 ACK，则发送下一帧，否则重传上一帧数据。ULPSDR 终端的工作流程如图 3(b)所示：首先将状态初始化，并打开 LoRa 接收状态，如果检测到配置帧且 CRC 校验通过，则根据式(1)启动计时器倒计时等待发送 ACK，否则继续回到接收状态。若收到的配置帧为休眠帧，则代表配置已经完成，关闭 OTA 电路并将物理层参数交由反向散射通信电路生效。



(a) OTA网关状态机　　(b) ULPSDR状态机

图 3　OTA 网关和 ULPSDR 终端状态机

综上所述，本文对配置系统的通信协议进行了详细设计，其主要特点包括：广播与地址选择性设计、ACK 应答、超时重传与 CRC 校验设计、随机延时防碰撞设计以及休眠帧设计。

(2) 配置系统通信帧结构设计

ULPSDR 采用 LoRa 协议进行 OTA 配置，以配置端为 LoRa 网关，被配置端为反向散射节点。LoRa 物理层帧结构具体如图 4 所示，主要包括以下几个字段：

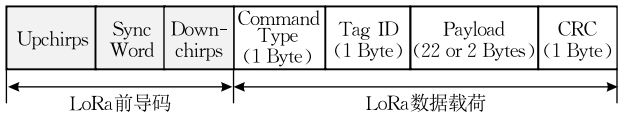


图 4　OTA 系统帧结构

Command Type：表示配置端和被配置端指令帧的类型，包含广播、ACK 和单播。对应的场景分别为：LoRa 网关获取所有反向散射节点的地址、反向散射节点对 LoRa 网关指令进行响应、LoRa 网关对特定 ID 进行配置。

Tag ID：代表反向散射节点的设备 ID，此 ID 类似于设备的 IP 地址，每个反向散射节点的设备 ID

均存储在非易失性内存或 EEPROM 中，并且是可配置的，便于分类管理。

Payload：有效载荷，用户可自定义。在本方案中，有且仅有两种情况：第一种情况：LoRa 网关发射指令对被配置端进行配置，有效载荷固定为 22 个字节，具体内容根据需要配置的信息和具体的配置内容决定；第二种情况：反向散射节点收到数据后，发送给 LoRa 网关的 ACK 帧，有效载荷固定为 2 个字节。第一个字节填充设备号，第二个字节根据接收到的信号类型确定，包括配置帧、广播帧和休眠帧。

CRC：循环冗余校验码。为了进一步提高协议的可靠性，本方案加入了 CRC 校验机制。

3.2 小型化电路设计

(1) 射频电路设计

加入 OTA 设计后，反向散射通信终端对射频链路的需求显著增加。首先，反向散射节点需要具备一个用于接收环境信号和反向散射调制信号的射频接收链路。这是由于反向散射节点需要通过外部发射的单音载波信号来传输本地数据（如传感器信息），传输的信号由其基带运行的通信协议（如 Wi-Fi、蓝牙、ZigBee 等）决定。其次，反向散射节点通常还需要一个唤醒接收机来检测环境信号强度，根据强度情况开启通信流程，降低总体平均功耗。最后，OTA 配置链路包含了用于接收下行配置信息的接收链路，以及反馈信息的上行链路，因此额外还需要至少一个射频链路来时分复用。总的来说，传统设计下，OTA 反向散射通信终端需要三个射频链路才能满足工作要求，而这意味着电路体积的增加，给反向散射节点的设计带来不必要的复杂性。

为了解决这一问题，本文采用射频开关来减少射频链路的数量，从而减少印刷电路的面积。具体而言，本文采用单刀四掷的开关 ADG904 来减少射频链路。该开关的插入损耗在 1 dB 以下，对通信系统性能的影响较小。因此，本文通过 MCU 控制开关的工作模式，以实现射频链路的切换。

(2) 电源管理设计

基于软件定义物理层的反向散射节点包含不同的元器件，比如 MCU、FPGA、主干无线电 LoRa 模块、射频开关以及各种传感器，如加速度计、麦克风、湿度传感器。不同电子元器件的工作电压有所不同，我们将其分类为三个电压域进行电源管理，如表 1 所示。

表 1 ULPSDR 中主要元件的电压域

元件	所需电压范围/V	电压域
MCU(MSP430FR5969)	1.80～3.60	V_1
FPGA(GW1N-LV4QN48C6)	1.20、3.30	V_1、V_3
主干无线电(SX1276)	1.80～3.70	V_1
包络检波器(LT5534)	1.65～2.75	V_2
射频开关(ADG902)	2.70～5.25	V_1
比较器(NCS2200SN1T1G)	0.85～6.00	V_1
晶振(ASTX-H11-20 MHz)	1.60～3.50	V_1
麦克风(MMICT3902-00-012)	1.65～3.63	V_1
湿度传感器(HDC2080DMBR)	1.62～3.60	V_1
加速度仪(ADXL362BCCZ-RL)	2.97～3.63	V_1

本文根据元器件的电压与要求，设定了 1.20 V、1.80 V、3.30 V 三种电压域对元器件进行归并，分别对应为 V_1、V_2、V_3。如果采用传统的两层 PCB 结构，则多种电压域会极大增加电路布局布线的复杂度。因此，本设计采用的归并后的三种电压域，可以通过四层 PCB 结构进行小型电路实现，其中第三层通过分区分布了上述三种主要电压域，通过通孔对电路各元件进行供电，进而降低电路复杂度。

3.3 图形化配置方法

在控制端方面，为了方便用户进行快速上手，本文采用 QT 这一跨平台的 C++图形界面应用程序框架来构建用户界面，通过用户输入生成图 4 中的 OTA 系统通信帧，并通过 UART 总线和 LoRa AP 进行通信发送以控制反射终端的行为。主要工作流程为：用户在图形化界面中点击相应的指令，QT 通过信号与槽函数的机制来激活相应的函数和串口模块。其中相应的函数生成通信帧的内容，而串口模块通过操作系统的服务将信号传输到 USB 接口中，再由硬件电平转换模块将 USB 电平信号转换成 MCU 能够处理的 UART 串口信号。其软件系统整体架构图如图 5 所示。

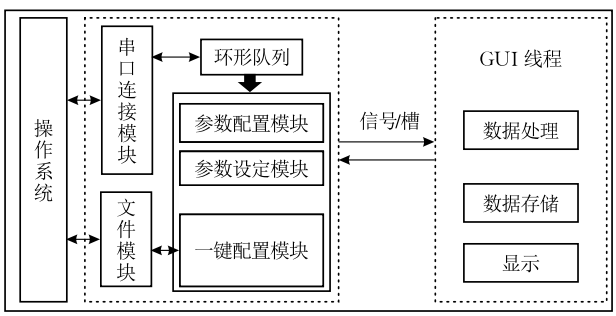


图 5 OTA 图形化配置工具软件架构

经过软件设计后，最终版软件的图形化界面布局如图 6 所示（基于 QT 5.6.0），可见其大致由 8 个部分组成，图中第一部分为串口端口号的选择，对于端口号，本设计在后台开了一个线程定时对端口号

列表进行刷新；第二部分为配置接收端的参数，此配置只为配置终端的设备 ID，单击后在弹出的界面内输入设备 ID 后即可锁定当前要编程的节点。图 6 第四部分为普通的参数构造功能，用户根据需要配置自己想要的参数，可以做到最细粒度的配置，参数帧需要包含 24 个配置指令（被分散在 domain 0～domain 5）分别对应控制软件无线电物理层行为的 24 种不同的参数，另外还具有可配置接收端 ID、休眠状态、是否广播等功能。对于 OTA 通信帧中的配置帧生成，其 Payload 部分的配置指令生成规则如表 2 所示。每一条配置指令均包含指令编号与寄存器数值，一旦被节点成功接收，其数值会修改软件定义物理层的反向散射通信模块中的 FPGA 寄存器数值，从而实现对节点物理层的修改。

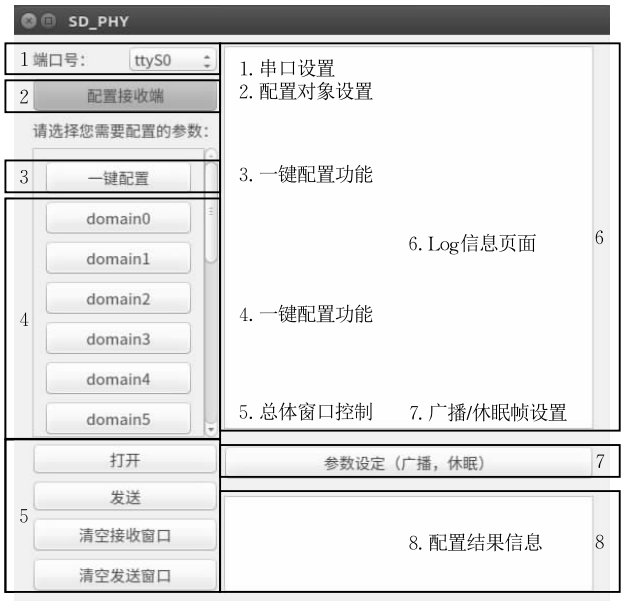


图 6　OTA 图形化配置工具图形界面

表 2　寄存器参数

配置指令编号	寄存器参数	比特数/bit
8'd0	Rate1，Rate0	16，16
8'd1～8'd3	B0～B2	16
8'd4～8'd6	A0～A2	16
8'd7	Mode	1
8'd8	$Bypass_{NCO}$	1
8'd9	Mask，Pattern	16，16
8'd10	$SYNC_{CLK\_RATE}$	10
8'd11	*Uplink_Rate*，*Fs_value*	16，16
8'd12～8'd13	Symbol0，Symbol1	64，64
8'd14	ID	16
8'd15	*SYM_LEN*，*DATE_LEN*	16，10
8'd16～8'd23	数据区	128，8

图 6 中第三部分为一键配置模块，能支持常规通信协议的“一键配置”，极大简化用户的使用和二次开发难度。第五部分则用于串口的开关与接收、发送窗口的控制。第六部分和第八部分分别为接收窗口和发送窗口。第七部分则用于参数设定，可以设置当前发送帧的类型是否为广播帧和休眠帧。

4　实验结果与分析

ULPSDR 将 OTA 配置模块与反向散射节点结合在一起，设计出可支持远程配置的基于软件定义物理层的反向散射节点，实际电路如图 7 所示。主要包含：LoRa 无线电、MCU、FPGA、射频开关、稳压模块、GPIO、唤醒接收模块、传感器模块。

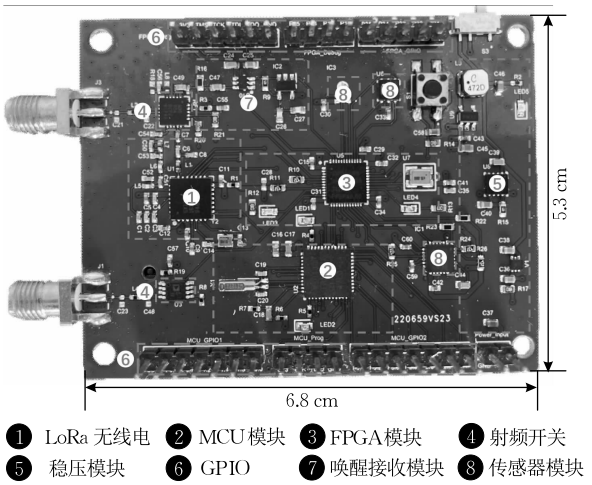


图 7　ULPSDR 原型机

4.1　非直视环境下的 ULPSDR 性能测试

在大多数物联网应用场景中，非直视无线传输（Non-Line-of-Sight，NLoS）是主要的通信方式，其无线电环境比视距无线传输（Line of Sight，LoS）更加复杂。因此，本文主要针对 NLoS 环境下的 ULPSDR 性能进行测试。实验在室内环境中模拟 NLoS 使用场景，LoRa 工作频率为 915 MHz，编码率为 4/6，网关信号发射功率设置为 20 dBm，实际发射功率经过同轴线连接 Keysight N9322C 频谱仪测得为－17.6 dBm，如图 8 所示。可能导致该现象的

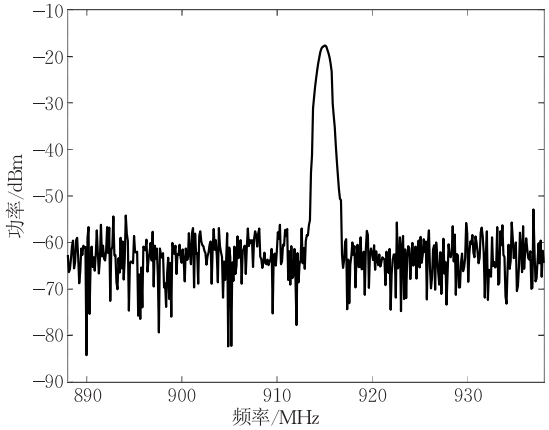


图 8　发射机信号频谱

原因包括:芯片的生产制造误差、射频前端电路的阻抗匹配度不足等。

(1)OTA 信号强度测试

为了实验检测接收端的灵敏度,本文通过访问 SX1276 芯片的 RSSI 寄存器获取信号强度:

实验条件设置如下:发射机放置于四楼的一间房间内,接收机即 ULPSDR 分别部署在同一栋楼的 1～5 层,距离发射机的水平距离约 30 m,均为非视距场景,同楼层有水泥墙壁阻挡。通信带宽为 125 kHz,扩频因子为 12,测试包数量为 100 个。

实测发现,通过 SX1276 计算出的 *RSSI* 值与实际 *RSSI* 值有所偏差,但两者具有正相关关系。经过校准与多次测量取均值后,实测不同楼层的接收端 *RSSI* 值如图 9 所示 。

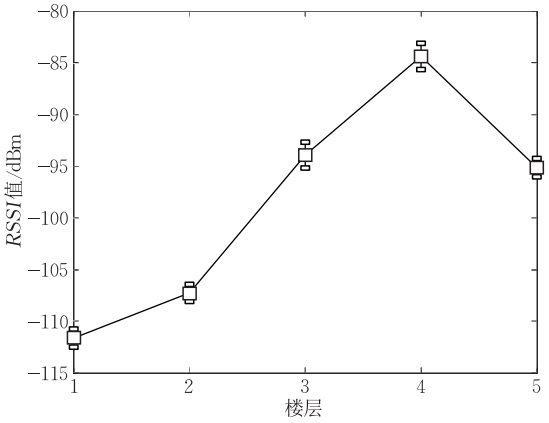


图 9 楼层与接收端 *RSSI* 的关系图

根据图 9 可得同楼层的信号强度最大,信号在不同的楼层之间会有较大程度的衰减,楼层差距越多,*RSSI* 衰减越严重,可见虽然 LoRa 在室内具有较强的穿透性,但随着所穿透距离的增大、障碍物的增多,信号强度衰减越剧烈,进而可能产生信号覆盖不到的盲点。

经过实验测得,100 个发送包下,楼层与接收端丢包率的关系图如图 10 所示。与 *RSSI* 的降低相对

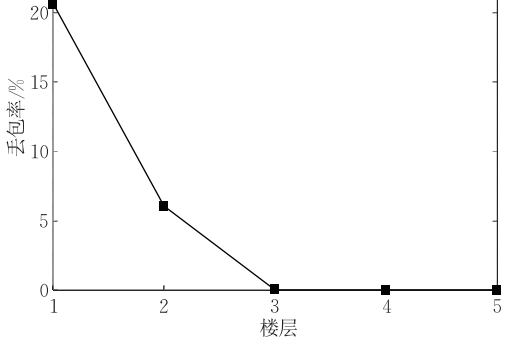


图 10 楼层与接收端丢包率的关系图

应地,在一楼与二楼,接收端产生了丢包的现象,在一楼时丢包率达到 21%。因此,在室内进行 ULPSDR 反向散射节点部署时,需要仔细分析现场环境,合理设置天线,使得整体的丢包率尽可能降低。

(2)OTA 传输时间测试

对于支持 OTA 的系统而言,一个至关重要的性能指标是空中编程所需的时间。OTA 系统总编程时长等于下行链路与上行链路的时长之和。下行链路包含:上位机传输命令至 MCU 的时长、MCU 控制 SX1276 发射时长与空口传输时长,接收端对数据的接收、校验及 MCU 逻辑处理时长。上行链路包含 ACK 帧。

实验条件设置如下:通信带宽为 250 kHz,扩频因子为 8,测试配置协议为 LoRa、BLE,结果如表 3 所示。

表 3 ULPSDR 与 TinySDR 空中编程时间对比

平台	协议	编程文件大小/KB	总用时/s
TinySDR[14]	BLE	40	98.000
ULPSDR	BLE	2	1.695
TinySDR[14]	LoRa	99	189.000
ULPSDR	LoRa	3	3.872

根据表 3 可得,给 ULPSDR 下发 BLE 编程包所需时间为 1.695 s,而同样状态下 TinySDR 的用时是 ULPSDR 的 57 倍多;给 ULPSDR 下发 LoRa 编程包所需时间为 3.872 s,而同样状态下 TinySDR 的用时是 ULPSDR 的 48 倍多。产生这种结果的很大一部分原因是因为本工作所采用的软件定义物理层反向散射系统的特殊的调制器设计,即仅需要提供波形的参数而非完整的数字电路二进制文件。TinySDR 的 BLE 和 LoRa 编程包内容是 FPGA 的完整二进制文件,即使经过了压缩,大小仍然达到了 40 KB 和 99 KB[14];相比之下, ULPSDR 采用的 SD-PHY 架构,无需重新修改 FPGA,而是在对于反射波形的参数进行寄存器级别修改[1],BLE 和 LoRa 编程包大小仅仅为 2 KB 和 3 KB,因此在同样采用 LoRa 协议的情况下大大缩短 OTA 配置时间。

(3)扩频因子对 OTA 性能的影响

在其他条件不变的情况下,扩频因子是影响 LoRa 通信性能的重要因素。扩频因子越大,LoRa 的符号长度越大,通信距离越远。此外,扩频因子还会影响控制信号的传输速度和接收灵敏度。

实验中具体参数设置如下:在室内测试环境下,固定接收机在室内 1 层,通信带宽为 125 kHz,分别设置扩频因子为 7～12,测试 *RSSI* 和丢包率情况。最终结果如图 11 和图 12 所示。

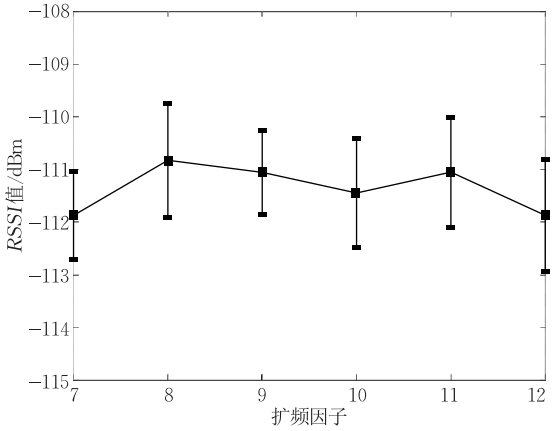


图 11　扩频因子与接收端 *RSSI* 的关系图

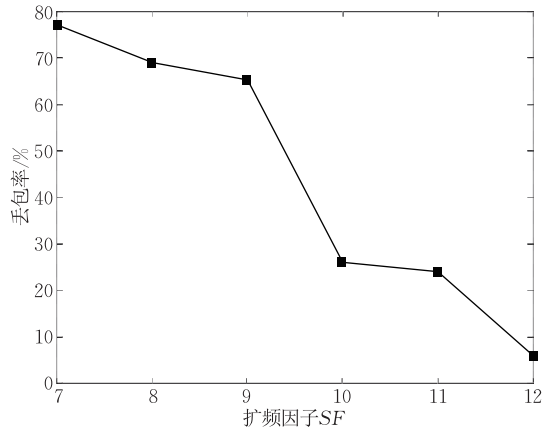


图 12　扩频因子与接收端丢包率的关系图

此外，为探究不同通信带宽与 OTA 编程时间之间的关系，本文在上述相同条件下进行测试，得到通信带宽与 OTA 编程时间的关系如表 4 所示。

表 4　室内不同通信带宽下 OTA 编程时长

通信带宽/kHz	实测端到端编程时长/ms
125	8941
250	5392
500	3700

从表 4 中可见，OTA 通信速率与 LoRa 的通信带宽呈线性正相关，随着通信带宽的增大，OTA 编程的端到端所需的时间逐渐减小。因此，在实际使用过程中需要根据编程时间与通信距离的要求进行通信带宽的权衡。可以发现，即使在最低的 BW 配置下，即 125 kHz 下，端到端编程时长仅为 8.9 s，相比 TinySDR 配置 BLE 和 LoRa 协议下的 OTA 配置时间(98 s 和 189 s，见表 3)至少降低了 1 个数量级。

如图 11 所示，在不同的扩频因子下，信号强度大致维持在 −111.5 dBm 左右，这表明在测试环境中，信号强度保持在一个固定水平。

如图 12 所示，随着扩频因子的增加，系统的丢包率逐渐降低，这意味着较大的扩频因子具有更高的接收灵敏度。此外，随着扩频因子的增加，OTA 的可靠通信范围也会增加。

本文设置了如下实验条件：在固定通信带宽为 250 kHz 时，分别设置扩频因子为 7～12，测试 OTA 编程时间的变化。不同扩频因子与 OTA 编程时间的关系如图 13 所示。

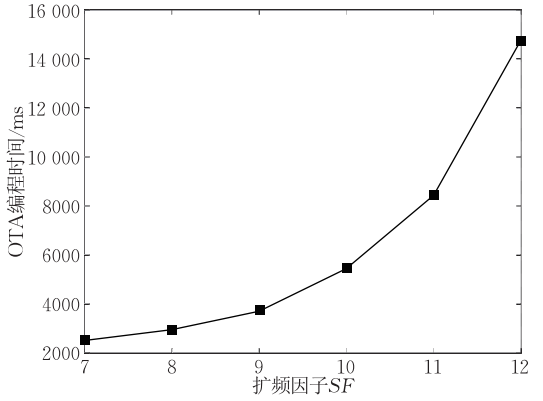


图 13　扩频因子与 OTA 编程时间的关系图

结果显示，随着扩频因子的增加，OTA 编程所需的时间呈指数增长，从 2457 ms 增加至 14791 ms。因此，更大的扩频因子虽然具有更高的接收灵敏度和更远的接收距离，但是 LoRa 信号的码率则相应降低，通信速率大幅度降低。因此，在实际应用中，需要根据应用场景进行权衡。

(4) 通信带宽对 OTA 性能的影响

通信带宽是影响通信系统性能的重要因素。在其他条件不变的情况下，增加通信带宽意味着增加通信速率，但可能会降低系统的接收灵敏度。

实验条件设置如下：发射机固定在四楼房间内，接收机放置在一楼跨楼层测试以得到非零的丢包率测试结果，扩频因子设置为 10，使用 ZigBee 编程文件，分别测试通信带宽为 125 kHz、250 kHz 和 500 kHz 情况下的丢包率。得到通信带宽与丢包率的关系如表 5 所示。

表 5　室内不同通信带宽下丢包率

通信带宽/kHz	发送测试包数	接收测试包数	丢包率/%
125	100	74	26
250	100	46	54
500	100	18	82

通过表 5 可以看出，OTA 使用的通信带宽与接收灵敏度呈负相关，也即通信带宽越大，接收机灵敏度越低，可靠通信范围也越短，丢包率也就相应增加，与 LoRa 调制的特性相符。需要注意的是，为了

探究最极端场景下的丢包率我们将接收机与发射机相隔三个楼层，若接收机放置在其他楼层，则丢包率接近 0。

4.2 直视环境下的 ULPSDR 通信距离测试

为了探究 ULPSDR 的最远工作距离，我们也开展了直视环境下的测试。我们首先尝试在室内走廊内对其进行直视(Line-of-Sight，LoS)条件下的距离测试。我们发现，在走廊两端相距 100 m 的情况下分别部署发射机与接收机，连续接收 1×10^5 比特，通信误码率(Bit Error Rate，BER)在 $SF=8$、$BW=250$ kHz 以及 $SF=10$、$BW=250$ kHz 测试条件下均为 0。

为了进一步探究其通信距离性能极限，我们开展室外直视环境下的通信距离测试，测试地点位于上海交通大学闵行校区的宣怀大道。测试场景如图 14 所示。我们固定发射机的位置，沿着大道移动接收机的位置 100 m 到 400 m，SF 和 BW 的设置同样采用两种：第一种 $SF=8$，$BW=250$ kHz；第二种 $SF=10$，$BW=250$ kHz，结果分别如图 15 与图 16 所示。两种情况下的通信距离分别达到了 350 m 与 400 m。

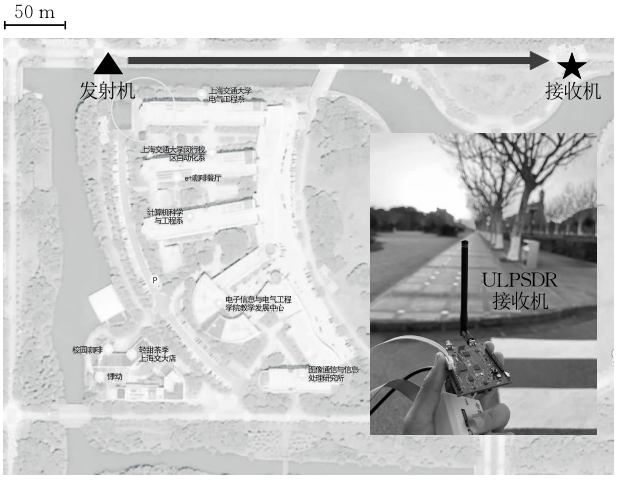


图 14 室外直视条件下通信距离测试场景

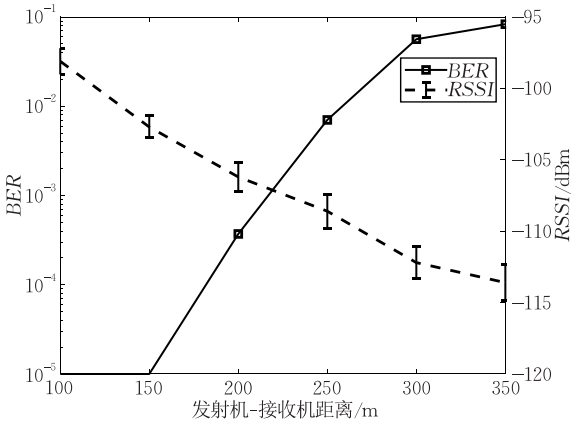


图 15 在 $SF=8$，$BW=250$ kHz 情况下，BER 和 $RSSI$ 随发射机-接收机距离变化

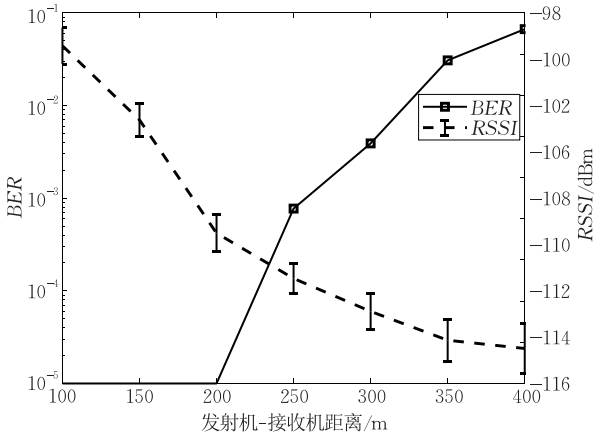


图 16 在 $SF=10$，$BW=250$ kHz 情况下，BER 和 $RSSI$ 随发射机-接收机距离变化

4.3 OTA 配置系统功耗分析

在 3 V 供电的情况下，ULPSDR 原型机经测试表现如下：在 OTA 工作状态下，反向散射节点的平均电流为 16.8 mA，功率为 50.4 mW；而在休眠状态下，反向散射节点的平均电流仅为 19.36 μA，功耗为 58.08 μW。相比之下，TinySDR 的工作功耗为 287 mW[14]，是 ULPSDR 的近 5 倍。ULPSDR 在休眠模式下的功耗也优于其他 SDR 平台，具体数据如表 6 所示。为了验证功耗对配置数据的不敏感特性，我们测量了 ULPSDR 休眠功耗在 OTA 配置物理层参数前后的关系。结果表明，功耗差异在 0.52 μW 以内，其变化主要来源于的硬件随机休眠状态偏差，如电压状态等。

表 6 当前不同 SDR 平台功耗与 OTA 功能比较

平台	休眠功耗	是否支持 OTA
USRP B200mini[17]	不支持	否
USRP E310[18]	2820 mW	否
BladeRF 2.0[19]	717 mW	否
LimeSDR Mini[20]	不支持	否
PlutoSDR[21]	不支持	否
GalioT[19]	350 mW	否
ULPSDR	58.08 μW	是

此外，本设备支持间歇式工作模式，在占空比为 50%的情况下，使用 5000 mAh 的 3 V 锂电池供电，根据理想化的理论推算可以换算为约 595 h 的工作时间，即大约 24 天。而对于目前系统采用的两节 7 号干电池串联供电方案来说，若每节干电池容量为 1300 mAh，可以类似地推测其理想工作时间为 155 h，即大约 6 天半的时间。如果将占空比降低到 10%，则还可以进一步延长至 32 天。需要注意的是，上述数据是基于理想电池的续航时间推测，实际的工作时长还受到组网规划开销、工作环境、电路欠压工作特性等因素的影响。

5 结　论

本文提出了 ULPSDR，一种支持 OTA 配置物理层的反向散射通信终端，结合了 LoRa 协议和功耗管理模块，实现了低功耗、小尺寸的设计目标。通过创新的 OTA 收发机子系统设计和电路小型化方法，ULPSDR 不仅成功解决了反向散射终端的无线配置问题，还显著降低了功耗和配置时间。实验结果表明，ULPSDR 在实际场景中能够实现 58 μW 的功耗和小于 4 s 的 OTA 配置时间，相比现有的支持 OTA 的物联网终端具有明显优势。该系统的开发为低功耗物联网终端的大规模部署提供了一种灵活的无线配置方法。

作者贡献声明　作者一提出了思路和电路设计方案，作者二负责完成电路整合与实验，作者三协助完成电路设计，作者四提出指导意见并修改论文。

参　考　文　献

[1] Zhu Fengyuan, Ouyang Mingwei, Feng Luwei, et al. Enabling software-defined PHY for backscatter networks//Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services. New York, USA, 2022: 330-342

[2] Liu V, Parks A, Talla V, et al. Ambient backscatter: Wireless communication out of thin air. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 39-50

[3] Kellogg B, Parks A, Gollakota S, et al. Wi-Fi backscatter: Internet connectivity for RF-powered devices//Proceedings of the 2014 ACM Conference on SIGCOMM. New York, USA, 2014: 607-618

[4] Ensworth J F, Reynolds M S. Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices//Proceedings of the 2015 IEEE International Conference on RFID (RFID). Piscataway, USA, 2015: 78-85

[5] Zhang Pengyu, Josephson C, Bharadia D, et al. FreeRider: Backscatter communication using commodity radios//Proceedings of the 13th International Conference on Emerging Networking Experiments and Technologies. New York, USA, 2017: 389-401

[6] Talla V, Hessar M, Kellogg B, et al. Lora backscatter: Enabling the vision of ubiquitous connectivity. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017, 1(3): 1-24

[7] Van Huynh N, Hoang D T, Lu X, et al. Ambient backscatter communications: A contemporary survey. IEEE Communications Surveys & Tutorials, 2018, 20(4): 2889-2922

[8] Yao C, Liu Y, Wei X, et al. Backscatter technologies and the future of Internet of Things: Challenges and opportunities. Intelligent and Converged Networks, 2020, 1(2): 170-180

[9] Zhang Xiao-Qian, Xu Yong-Jun. A survey of backscatter communication for zero-power Internet of Things. Journal on Communications, 2022, 43(11): 199-212(in Chinese)
(张晓茜，徐勇军. 面向零功耗物联网的反向散射通信综述. 通信学报，2022, 43(11): 199-212)

[10] Yuan L, Wang Q, Zhao J, et al. Multiprotocol backscatter with commodity radios for personal IoT sensors. IEEE/ACM Transactions on Networking, 2023, 31(3): 1132-1144

[11] Gong W, Huang Y, Zhao J, et al. Understanding state-of-the-art ambient backscatter. Pervasive Ambient Communication for Internet of Things. Cham, Switzerland: Springer, 2023: 11-21

[12] Gu B, Li D, Ding H, et al. Breaking the interference and fading gridlock in backscatter communications: State-of-the-art, design challenges, and future directions. IEEE Communications Surveys & Tutorials, 2024, 26(1): 1-25

[13] Peng Y, He S, Zhang Y, et al. Toward software-defined backscatter modulation via signal emulation. IEEE Transactions on Wireless Communications, 2024, 23(10): 14836-14847

[14] Hessar M, Najafi A, Iyer V, et al. TinySDR: Low-power SDR platform for over-the-air programmable IoT testbeds//Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20). Berkeley, 2020: 1031-1046

[15] Guo X, Shangguan L, He Y, et al. Aloba: Rethinking ON-OFF keying modulation for ambient LoRa backscatter//Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys 20). New York, USA, 2020: 192-204

[16] Guo X, Shangguan L, He Y, et al. Saiyan: Design and implementation of a low-power demodulator for LoRa backscatter systems//Proceedings of the 19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22). Renton, USA, 2022: 437-451

[17] USRP B200mini. https://www.ettus.com/wp-content/uploads/2019/01/USRP_B200mini_Data_Sheet-1.pdf

[18] USRP E310. https://www.ettus.com/wp-content/uploads/2019/01/USRP_E310_Datasheet.pdf

[19] BladeRF 2.0 micro. https://www.nuand.com/bladerf-2-0-micro/

[20] LimeSDR. https://myriadrf.org/projects/component/limesdr/

[21] AD9363 transceiver datasheet. https://www.analog.com/media/en/technical-documentation/data-sheets/AD9363.pdf

[22] Narayanan R, Kumar S. Revisiting software defined radios in the IoT era//Proceedings of the 17th ACM Workshop on Hot Topics in Networks. New York, USA, 2018: 43-49

ZHU Feng-Yuan, Ph. D. candidate. His research interests include backscatter communication and low-power IoT systems.

DI Qi-Long, M. S. His research interest is low-power IoT communication.

LIU Wei-Xing, M. S. His research interests include over-the-air programming system theory and technology, backscatter communication.

TIAN Xiao-Hua, Ph. D., professor, Ph. D. supervisor. His research interests include intelligent IoT architecture, ultra-low power consumption and ultra-high concurrent wireless communication technology, IoT wireless positioning technology, and intelligent wearable devices.

Background

Backscatter communication has long garnered attention in academia for its ability to achieve microwatt-level power consumption. RFID, as an important commercial application of backscatter communication, relies on dedicated readers, which are expensive. Besides, its reading distance is limited, typically within 10 meters, restricting its application scenarios. In recent years, ambient backscatter systems have been proposed, where backscatter terminals can directly communicate with commercial radio devices such as Wi-Fi and BLE (Bluetooth Low Energy). However, these methods are limited to single protocols, and in practical industrial scenarios, different manufacturers adopt diverse radio infrastructures, hindering the rapid adoption of these new technologies. A potential solution to this challenge is the recently proposed Software-defined Physical Layer (SD-PHY) backscatter, which can achieve reconfigurable back-scatter communication through a universal RF front-end and baseband.

However, existing software-defined backscatter communication systems cannot be configured wirelessly and rely on serial ports for configuration, increasing the upgrade and maintenance costs for large-scale deployments in industrial settings. On the other hand, traditional IoT nodes supporting Over-The-Air (OTA) programming typically use Wi-Fi or Bluetooth, which suffer from high power consumption and significant application limitations, making them unsuitable for long-term deployment in industrial scenarios. Based on current public research, there is no IoT terminal that supports OTA while maintaining microwatt-level communication power consumption.

To address this gap, this paper proposes an OTA-configurable backscatter communication terminal—Ultra-Low Power Software-Defined Radio (ULPSDR)—built upon software-defined physical layer backscatter communication. Essentially, it integrates an OTA module and a power management module based on the LoRa protocol into the SD-PHY framework. The main contributions of this paper include: (1) proposing an OTA transceiver subsystem design suitable for the SD-PHY backscatter architecture, including a configuration protocol that provides effective OTA feedback with low power consumption; (2) developing a joint miniaturization design method for the OTA circuit and backscatter communication circuit, reducing circuit size through antenna sharing between RF links and simplifying circuit complexity by consolidating device voltage domains; (3) designing a hardware system that validates our design, which realizes OTA configuration in real-world deployment. The results demonstrate a power consumption of 58 microwatts and an OTA configuration time of less than 10 seconds, significantly reducing both power consumption and OTA configuration time compared to existing OTA-capable IoT terminals.

This work is supported by the National Key Research Program of China (No. 2020YFB1708700), and the National Natural Science Foundation of China (Nos. 61922055 and 61872233).