使用 LoRa 设计用于安全野外通信的免提短距离互通设备

Ayush Kumar Agrawal计算机科学学院（*SoCS*） *UPES*德拉敦，印度
ayush6295@gmail.com

Soumendu Das电子与通信工程系 贾姆谢德布尔国家理工学院贾姆谢德布尔，印度
2021rsec009@nitjsr.ac.in

Jayendra Kumar电子与通信工程系 贾姆谢德布尔国家理工学院贾姆谢德布尔，印度
jkumar.ece@nitjsr.ac.in

arXiv:2602.23924v1 [eess.SP] 27 Feb 2026

摘要—**在战术、军事和灾害响应场景中，短距离、可靠且安全的通信是一项重要优先事项，因为传统通信基础设施可能处于离线状态或容易遭到拦截。当前，甚高频/特高频无线电和软件定义无线电应用广泛，但设备体积较大且功耗高，因此不适合用作轻量级可穿戴设备，也难以实现无缝免提使用。本文介绍了一种微型、基于 LoRa 的加密互通设备的设计与理论框架，该设备可用于安全野外通信，在 1～1.5 km 的通信范围内，并在视距条件下工作。所提出的系统由语音激活采集模块、数字音频压缩、嵌入式微控制器处理器以及 AES-128 加密模块组成，随后通过 LoRa 协议进行低功耗传输。借助啁啾扩频调制所具备的远距离和低能耗特性，该系统能够在保持低功耗和低电磁辐射特征的同时，确保可靠通信。通过链路预算对所提出通信范围进行理论分析，证明了其在实际传播条件下的通信范围具有可行性。该架构重点关注基础设施无关性、点对点安全性以及可穿戴人体工学。该方案展示了 LoRa技术在传统物联网遥测之外的应用潜力，并可进一步扩展为安全战术语音通信平台。**

索引词—**LoRa、战术通信、高级加密标准加密、可穿戴设备、安全语音通信**

I. 引言

在动态且充满敌意的野外环境中，实现有效通信是执行关键任务的必要条件。军事巡逻、边境监视、灾害响应和紧急救援人员开展行动时，往往身处标准通信基础设施无法使用、负载过重，或容易受到干扰和破坏的区域；这些基础设施包括蜂窝系统或卫星连接。通信系统在这些情况下，必须满足严格的标准，例如低延迟、高可靠性、低可探测性和高密码安全性。

战术通信传统上采用甚高频（VHF）和超高频（UHF）无线电系统。尽管这些系统能够提供中等通信范围和较高的稳健性，但在实际应用中存在诸多局限。其硬件设计通常体积庞大、能耗较高，导致移动能力不足并限制了可穿戴性。此外，许多老旧系统基于按键通话系统和外置天线系统，可能会妨碍在主动执行任务期间顺畅地进行免提通信。在安全性方面，即使是较新的型号也已配备加密模块，但在嵌入式层面，安全密钥交换和端到端机密性的设计并不总是高效。此外，持续的高功率传输会增强电磁可探测性，从而可能暴露行动人员的存在。

近年来，低功耗广域网技术不断发展，尤其是基于啁啾扩频调制的 LoRa技术，为短距离战术通信带来了全新的范式。LoRa据称具有较高的接收灵敏度、较大的链路预算和较低的能耗，因此理论上适用于小型可穿戴系统。然而，与实时加密语音传输不同，LoRa主要用于低数据速率遥测和传感器网络。为弥合这一差距，本文提出一种基于LoRa的可穿戴安全语音互通平台，旨在短距离点对点模式下部署使用 [1]。该系统在LoRa传输之前，结合了语音激活功能、数字音频压缩、集成微控制器处理和基于高级加密标准的加密。所提出的架构将实现基础设施独立性、缩小设备体积

并提升运行安全性，同时支持数据包和语音的安全交换，并确保在1至1.5公里的视距范围内可靠地交换语音。

II. 系统架构

A. 总体通信模型

所提出的架构基于模块化分层架构，旨在现场提供安全、低延迟且节能的语音通信。总体通信拓扑如图1所示。该

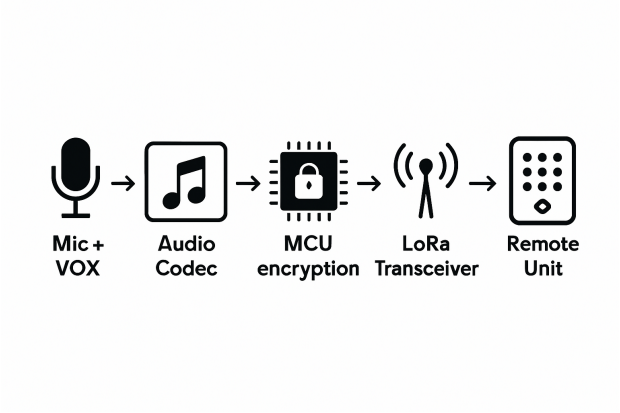


图1. 总体通信流程

通信流水线由一系列信号变换阶段构成：

VOX麦克风 → 音频编解码器 → MCU处理 →AES加密 →LoRa传输 →远程解密与播放

输入阶段由启用声控交换（VOX）的麦克风模块对模拟语音数据进行采样。只有当信号幅度超过一定阈值时，声控交换（VOX）机制才会触发，这有助于降低空闲功耗、抑制意外的射频发射，以及由功耗 [2] 引起的任何意外射频发射。

音频编解码器将模拟信号编码为低比特率的压缩流，并转换为数字形式，使其能够在 LoRa 的带宽限制内进行传输。微控制器单元（MCU）负责缓冲、帧分组、添加循环冗余校验（CRC），以及定时同步[3]。传输前，采用 AES-128 加密，以确保机密性和完整性。随后，编码后的消息通过 LoRa 的啁啾扩频（CSS）方法进行交织，并经 ISM 频段发送。

接收端也会执行相同的工作，包括对音频信号 [4]进行解调、解密、解码和重构。接收端同样会执行这些操作，包括对音频信号进行解调、解密、解码和重构。

B. 点对点子系统架构

如图 2 所示，该子系统架构是镜像子系统架构，展示了两个可穿戴野外设备处于对称的点对点模式。

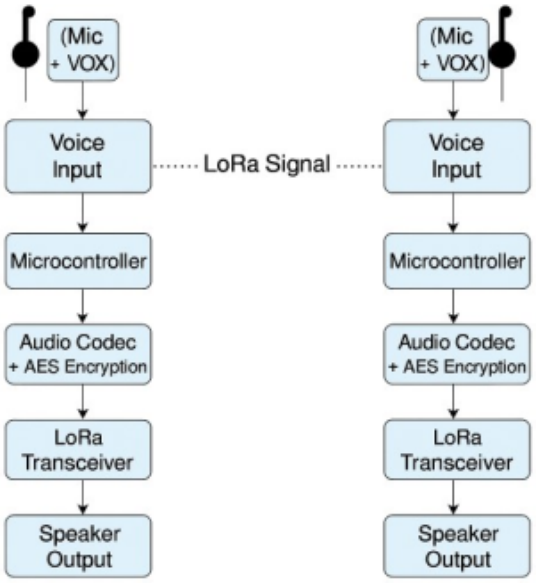


图 2. 双镜像垂直子系统架构

每个子系统的功能层包括以下内容：

1. 语音采集层：启用声控交换（VOX）的麦克风会持续检测环境声音；当系统检测到语音时，便会启动。这可降低占空比并延长电池续航时间。

2. 信号处理层：音频编解码器负责进行模数转换和压缩。由于 LoRa 的数据速率较低，压缩比需要经过调整，以在可懂度与传输效率之间取得平衡。

3. 控制与安全层：任务调度、数据包分段、加密和错误处理均由 ESP32 微控制器完成。采用硬件加速，以确保通过 AES-128 加密减少计算量。

4. 通信层：SX1276 LoRa收发器采用啁啾扩频调制来传输加密数据包。LoRa 具有极高的接收灵敏度（最高可达 -148 dBm），并能以较低的发射功率实现远距离通信。

5. 音频重建层：接收时会对解密后的数字音频进行解码，并通过小型扬声器模块播放。

该架构采用半双工模式，传输与接收过程交替进行 [5]。该架构为半双工模式，也就是说，传输与接收轮流进行。这减少了发生冲突的可能性，便于同步，并降低了平均功耗。

C. 硬件布局与物理设计图3展示了该设备的物理布局。

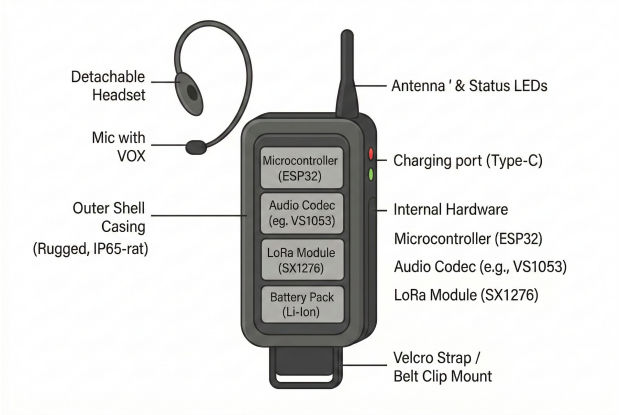


图3. 所提设备的硬件布局

硬件设计更加注重现场适应性、加固和便携性。外壳采用 ABS材料制成，并达到 IP65等级，可防尘防水。系统堆栈包括以下内部硬件：

- ESP32微控制器模块
- VS1053或类似的低功耗音频编解码器
- SX1276收发器LoRa模块
- 37V锂离子可充电电池
- 内置充电和电源调节电路。

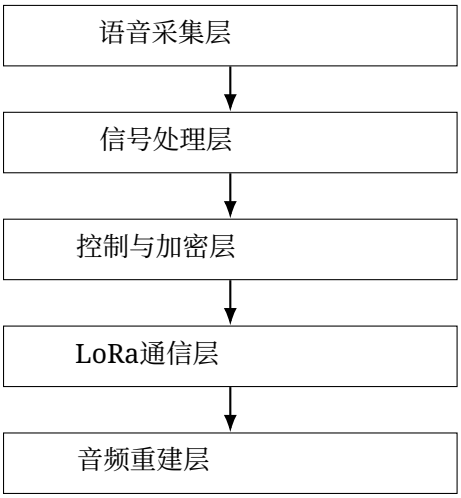


图4. 所提出系统的分层功能架构

可拆卸的轻型耳机让用户在长时间任务中佩戴更加舒适 [6]。这款可拆卸的轻型耳机还可确保用户在整个长时间任务期间经济高效地使用设备。天线接口安装在外部，以实现最高辐射效率。设备重量控制在 200 克以内，使其在部署期间佩戴舒适 [7]。功耗优化策略包括：

- 声控触发激活
- 空闲状态下 MCU 深度睡眠
- 自适应发射功率控制
- 高效数据包调度

在典型野外使用条件下，可确保连续运行 12–16 小时。

III. 技术规格

A. 通信参数

所提出的通信平台在运行时使用工业、科学和医疗频段，包括 433兆赫和 868兆赫 [8]。选择这些频段是因为它们具有良好的传播特性、法规准入条件，并符合 LoRa啁啾扩频调制 [9]。主要工作参数如下：

- **频段：** 433 / 868兆赫（ISM频段）
- **工作范围：** 1–1.5 千米（视距）
- **延迟：** ≤ 300 毫秒端到端
- **加密：** AES-128 对称密钥加密
- **工作模式：** 半双工
- **发射功率：** 14–20dBm
- 接收灵敏度：</style}最高可达 -148dBm（取决于扩频因子）
- **备用电池：** 可连续运行 12–16 小时

LoRa调制采用啁啾扩频（CSS）方法，可使接收器具有较高的灵敏度 [10]。提高扩频因子有助于增强链路鲁棒性，但会降低数据速率，因此可以在通信范围与延迟之间进行可行的权衡[11]。

为降低冲突概率和平均电流消耗，决定采用半双工通信 [12]。AES-128安全性很高，且计算开销很低，因此适用于战术通信环境 [13]。

采用半双工通信以降低碰撞概率并最大限度地减少平均电流消耗 [12]。AES-128 加密在确保计算效率的同时，提供适用于战术通信的强大密码安全性 [13]。端到端时延可以表示为以下各项延迟之和：

$$T_{\text{total}} = T_{\text{encoding}} + T_{\text{encryption}} + T_{\text{packetization}} + T_{\text{airtime}} + T_{\text{decoding}} \quad (1)$$

通过优化压缩并采用适中的扩频因子（例如 SF7–SF9），系统可将延迟保持在 300 毫秒以内，因此适用于对话语音通信。

B. 链路预算分析

通信范围基于理论可行性，并通过常规链路预算公式加以验证。接收到的信号功率由以下公式确定：

$$P_r = P_t + G_t + G_r - L_p - L_s,$$

其中:

- P_t = 发射功率（dBm）
- G_t =发射天线增益 (dBi)
- G_r = 接收天线增益 (dBi)
- L_p = 自由空间路径损耗 (dB)
- L_s = 系统损耗（电缆、阻抗失配、衰落余量）

自由空间路径损耗 (FSPL) 使用广为人知的关系式进行估算

$$L_p = 20\log_{10}(d) + 20\log_{10}(f) + 32.44 \tag{2}$$

其中， d 表示以千米为单位的链路距离， f 表示以 MHz 为单位的载波频率。对于所考虑的通信场景,

$$d = 1.5 \text{ km}, \qquad f = 868 \text{ MHz}. \tag{3}$$

将这些值代入式 (2) 得

$$\begin{aligned} L_p &= 20\log_{10}(1.5) + 20\log_{10}(868) + 32.44 && (4)\\ &= 3.52 + 58.77 + 32.44 && (5)\\ &\approx 94.73 \text{ dB}. && (6) \end{aligned}$$

接收功率由标准链路预算表达式得出

$$P_r = P_t + G_t + G_r - L_p - L_s \tag{7}$$

其中， P_t 为发射功率， G_t 和 G_r 分别表示发射天线和接收天线的增益， L_s 表示各种系统损耗。假设以下数值:

$$P_t = 17 \text{ dBm}, \quad G_t = 2 \text{ dBi}, \quad G_r = 2 \text{ dBi}, \quad L_s = 5 \text{ dB}. \tag{8}$$

根据式 (7)，接收功率为

$$\begin{aligned} P_r &= 17 + 2 + 2 - 94.73 - 5 && (9)\\ &\approx -78.73 \text{ dBm}. && (10) \end{aligned}$$

因此，链路余量可表示为

$$\text{Link Margin} = P_r - P_{\text{sensitivity}}. \tag{11}$$

LoRa 接收器的灵敏度通常约为 -130 dBm 至 -148 dBm，具体取决于扩频因子。即使采用保守假设,

$$P_{\text{sensitivity}} = -120 \text{ dBm}, \tag{12}$$

由此得到的链路余量为

$$\begin{aligned} \text{Link Margin} &= -78.73 - (-120) && (13)\\ &\approx 41 \text{ dB}. && (14) \end{aligned}$$

这一较大的连接余量验证了在视距条件下 1-1.5 km 通信范围内的良好通信性能，并且能够承受中等程度的环境劣化和干扰。

C. 功耗分析

占空比循环和声控交换控制的传输对平均功耗的影响如下:

$$P_{avg} = D \cdot P_{tx} + (1 - D) \cdot P_{sleep},$$

其中， D 为发射占空比。由于语音传输是间歇性的，因此 D 的值相对较小，这有助于大幅延长电池续航时间。通过优化固件调度、固件休眠和自适应发射功率控制，该设备可连续运行 12 至 16 小时，满足长时间语音传输需求 [14]。

IV. 开发方法

在开发所提出的基于 LoRa 的安全互通设备时，采用了结构完善的软硬件协同设计流程。该流程围绕依次推进且反复迭代的阶段精心构建，从而确保了可靠性、可扩展性和现场部署就绪度。整体开发流程如图 5 所示。

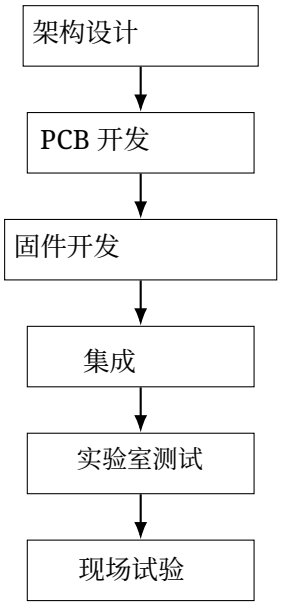


图 5. 开发流程

A. 架构设计

第一步是根据运行要求确定系统级架构，包括通信范围、延迟、加密强度和电池续航时间 [15]。系统采用模块化分层模型，将语音采集、处理、加密和通信分开。

理论可行性研究：开展了一项可行性研究，内容包括：

- 链路预算估算
- 数据速率和延迟分析
- 功耗建模
- 加密开销评估

在选择组件时，综合考虑了计算能力、能效和射频能力，因此选用了 ESP32 和 SX1276 模块。

B. PCB 开发

随后进行了架构验证，并完成了原理图和印刷电路板布局。布局设计特别注重确保射频运行稳定且运行噪声低。关键设计因素包括控制射频走线阻抗、合理分割接地平面以确保噪声抑制、实现模拟/数字隔离，以及优化天线位置以防止耦合效应。

通过信号完整性分析，降低了音频编解码器与射频收发器部分之间的电磁干扰。采用多层 PCB 叠层旨在实现紧凑集成，并最大限度地减少寄生效应和不必要的耦合路径。

C. 固件开发

同时开展软件开发并进行印刷电路板制造，以缩短设计周期。固件架构采用模块化设计，各功能模块均可独立验证和优化。实现的模块包括基于声控交换（VOX）的阈值检测、音频采样与压缩、AES-128 加密集成、LoRa 数据包封装与循环冗余校验验证，以及低功耗休眠调度。

采用实时轻量级任务调度，确保语音传输具有确定性延迟。此外，对加密算法进行了优化，使其易于优化，从而避免耗费过多计算时间，同时满足所需的安全级别。

D. 系统集成

硬件和固件子系统分别经过测试后，逐步加入系统。这种做法有助于分阶段隔离故障，并缩短系统启动过程中调试所花费的时间。集成测试主要围绕音频信号的连续性、加密与解密的一致性，以及数据包丢失和端到端延迟的表现展开。

系统运行时，使用逻辑分析仪和射频频谱分析仪确认了调制精度、定时同步和协议级正确性。

E. 实验室测试

在部署到现场之前，还进行了室内实验，以测试核心系统功能。测试内容包括功能检查、不同占空比下的功耗测试、不同扩频因子下的语音可懂度测试，以及在受控干扰环境下进行的分组错误率测试。

延迟通过比较传输时间戳与接收器处的播放时间戳来测量。

F. 现场试验

室内实验也已开展，以便在其部署到现场之前测试核心系统功能。测试依据功能检查、不同占空比下的功耗测试、不同扩频因子下的语音可懂度测试，以及干扰测试受控环境中的分组错误率测试进行。

延迟通过查看传输时间戳，并将其与接收器处相应的播放时间戳进行比较来测量。

V. 预期成果

预计所提出系统的成功实施将促成一种紧凑型国产安全短程战术通信平台的提供，该平台独立于传统通信基础设施。通过将采用 LoRa 的啁啾扩频调制与嵌入式 AES-128 加密相结合，可为现场部署提供机密的点对点语音通信框架，例如用于国防和灾害响应场景。

从硬件角度来看，与传统的软件定义无线电（SDR）系统和传统甚高频/特高频战术无线电相比，该设备预计可显著减小尺寸并降低功耗。可穿戴设备的轻量化配置提高了行动的机动性，并可在 1–1.5 公里的视距距离内保持通信可靠。语音激活的传输集成还可通过限制不必要的无线电活动，进一步优化能源利用并减少电磁暴露。

在网络层面，该架构提供了一种可扩展的班组级通信模型，只需极少依赖基础设施，即可扩展至多节点配置。加密分组通信机制可确保数据机密性、完整性，并防止未经授权的截获。

总体而言，所提出的框架表明，低功耗广域通信技术的应用可扩展至物联网传统遥测应用之外，并进一步用于安全、可在现场部署的实时战术语音通信系统。

VI. 结论

本文介绍了一种面向短程战术行动的基于LoRa的可穿戴安全互通系统的设计、理论验证和原型实现。通过结合语音激活采集、嵌入式数字信号处理、AES-128 加密与啁啾扩频调制，所提出的架构实现了一种安全且独立于基础设施的点对点语音通信架构。

分析性链路预算分析验证了在1-1.5公里距离范围内实现可靠通信的可能性，且链路余量充足；延迟分析则验证了端到端时延处于可接受的会话限制之内。

采用半双工传输和自适应占空比对能效的影响要大得多，使紧凑型可穿戴设备形态下的运行待命时间可达12–16小时。

与传统的甚高频／特高频和基于 SDR 的战术无线电相比，所开发的系统硬件复杂度更低、功耗更低、便携性更高，并且在设备级嵌入了加密功能。模块化架构还支持扩展至多节点班组通信，并可与网状网络框架集成。

总体而言，这项研究验证了 LoRa 技术在常见遥测应用之外的用途，展现了该技术支持野外安全实时语音通信的能力。所提出的平台为长期现场验证、加固以及后续改进奠定了良好基础，有望构建完全可扩展的战术通信生态系统。

参考文献

[1] A. Augustin、J. Yi、T. Clausen 和 W. M. Townsley，“LoRa 研究：面向物联网的远距离、低功耗网络”，传感器，第 16 卷，第 9 期，第 1466 页，2016 年。[2] U. Raza、P. Kulkarni 和 M. Sooriyabandara，“低功耗广域网：概述”，*IEEE*通信调查与教程，第 19 卷，第 2 期，第 855–873 页，2017 年。[3] F. Adelantado、X. Vilajosana、P. Tuset-Peir´o、B. Martinez、J. Melia-Segui 和 T. Watteyne，“了解 LoRaWAN 的局限性”，*IEEE*通信杂志，第 55 卷，第 9 期，第 34–40 页，2017 年 9 月。[4] M. Centenaro、L. Vangelista、A. Zanella 和 M. Zorzi，“非授权频段中的远距离通信：物联网与智慧城市场景中的新星”，*IEEE Wireless Communications*，第 23 卷，第 5 期，第 60–67 页，2016 年 10 月。[5] M. Bor、J. Vidler 和 U. Roedig，“面向物联网的 LoRa”，载于*Proc. ACM EWSN*，2016 年，第 361–366 页。[6] J. Pet¨aj¨aj¨arvi、K. Mikhaylov、A. Roivainen、T. H¨anninen 和 M. Pettissalo，“低功耗广域网的覆盖范围：LoRa 技术的通信范围评估与信道衰减模型”，载于*Proc. ITST*，2015 年。[7] J. Haxhibeqiri、I. Moerman 和 J. Hoebeke，“通过低开销调度 LoRa 传输提升可扩展性”，*IEEE*物联网期刊，第 6 卷，第 2 期，第 3097–3109 页，2019 年。[8] R. Sanchez-Iborra 和 M. D. Cano，“面向工业物联网服务的低功耗广域网解决方案现状”，传感器，第 16 卷，708，2016 5，第 。[9] C. Goursaud 和 J.-M. Gorce，“面向物联网的专用网络：物理层／媒体访问控制层现状与挑战”，*EAI*认可的物联网汇刊，第 1 卷，第 1 期，2015 年。[10] M. Magno、T. Polonelli、L. Benini 和 E. Popovici，“用于建筑监测的低功耗无线传感器节点架构”，*IEEE Sensors Journal*，第 9 卷，第 11 期，第 1463–1470 页，2009 年。[11] J. Granjal、E. Monteiro 和 J. S´a Silva，“物联网安全：现有协议综述与开放研究议题”，*IEEE*通信调查与教程，第 17 卷，第 3 期，第 1294–1312 页，2015 年。[12] G. Naik、B. Choudhury 和 J. Park，“IEEE 802.11ah：独立的物联网技术”，*IEEE*通信杂志，第 54 卷，第 12 期，第 41–48 页，2016 年 12 月。[13] L. Vangelista，“频移啁啾调制：LoRa 调制”，*IEEE*信号处理快报，第 24 卷，1821，2017 12，1818，第 – 页。[14] B. Reynders、W. Meert 和 S. Pollin，“低功耗广域网中的功率与扩频因子控制”，载于*Proc. IEEE ICC*，2017 年。[15] H. Bogucka 和 A. Conti，“能量感知无线通信的自由度”，*IEEE*通信杂志，第 51 卷，第 7 期，第 56–63 页，2013 年 7 月。