中国科学: 信息科学 2021 年 第 51 卷 第 10 期: 1738–1754
SCIENTIA SINICA Informationis
论文

异构物联网直联通信关键技术

曹东江[1], 王帅[1*], 熊润群[1], 刘云淮[2], 罗军舟[1], 何田[1*]

1. 东南大学计算机科学与工程学院, 南京 211189
2. 北京大学大数据科学研究中心, 北京 100871
* 通信作者. E-mail: shuaiwang@seu.edu.cn, tianhe@seu.edu.cn

收稿日期: 2020–10–12; 修回日期: 2020–12–05; 接受日期: 2020–12–22; 网络出版日期: 2021–10–13

国家重点研发计划 (批准号: 2018YFB2100300)、国家自然科学基金 (批准号: 61902066, 61602112, 61632008) 和江苏省自然科学基金 (批准号: BK20190336) 资助项目

摘要 随着物联网技术的快速发展, 不同应用在通信范围、能耗、时延等方面的需求推动各种无线通信技术的产生. 由于无线通信技术的多样性, 异构设备间存在通信壁垒不能进行直接通信. 由于信息交互能力的缺失, 广泛部署的异构物联网设备相互竞争频谱资源并导致通信干扰日益严重. 此外, 异构设备间的通信障碍限制了信息共享和资源整合. 传统的利用网关实现异构设备间的通信需要额外的开销. 研究人员提出了不需要网关设备进行协议间转换的异构物联网直联通信技术, 使得异构设备能够进行直接通信. 本文首先分析和总结异构物联网直联通信技术的研究现状; 在此基础上, 提出了实现异构物联网直联通信的关键技术: 数据包级、信号级和符号级的异构物联网直联通信技术; 之后, 介绍了所提相关技术在异构物联网设备共存场景下的抗干扰协调应用; 最后, 总结全文并展望了异构物联网直联通信技术的未来发展方向.

关键词 物联网, 无线网络, 异构物联网直联通信, 无线通信协议, 数字调制

1 引言

近年来, 物联网技术不断成熟, 其应用已经渗透到生活的方方面面, 在智能家居、智慧交通、环境监测、智能制造等方面发挥着重要作用. 物联网的蓬勃发展离不开包括 LTE、Wi-Fi、ZigBee、蓝牙等众多异构通信技术的支撑 [1]. 在物联网构架中, 提出众多异构技术, 是为了适应动态复杂的环境以及满足不同场景在通信范围、吞吐量、可靠性、时延和能耗等方面的应用需求 [2]. 这些异构物联网通信技术在各自的应用领域获得了巨大的成功.

然而, 随着物联网的快速发展和广泛应用, 越来越多的异构设备共存于同一场景, 共享同一频段. 统计机构 Gartner 发布的数据显示, 截止 2020 年年底全球将有约 200 亿的物联网设备[1)], 其中大量的

1) Inc Gartner. 2016. Gartner Report. https://www.gartner.com/en/documents/2625419.

引用格式: 曹东江, 王帅, 熊润群, 等. 异构物联网直联通信关键技术. 中国科学: 信息科学, 2021, 51: 1738–1754, doi: 10.1360/SSI-2020-0320
Cao D J, Wang S, Xiong R Q, et al. The key technologies of cross-technology communication (in Chinese). Sci Sin Inform, 2021, 51: 1738–1754, doi: 10.1360/SSI-2020-0320

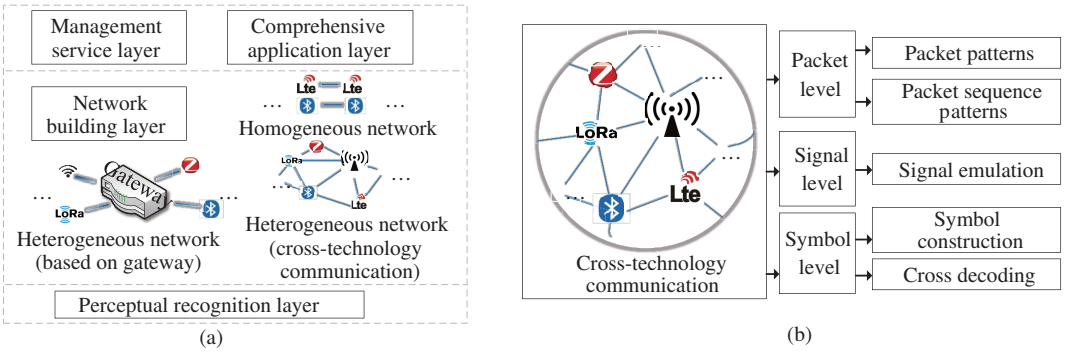

图 1 (网络版彩图) 物联网和异构物联网直联通信体系架构

Figure 1 (Color online) The system of the Internet of Things and cross-technology communication. (a) The system of the Internet of Things; (b) the framework of cross-technology communication

物联网设备共享 ISM (industrial scientific medical) 频段, 使得频谱资源愈发紧张. 由于异构设备间的通信壁垒, 对周围设备的认知缺失, 导致异构设备不仅不能共融互惠, 反而相互竞争通信频段, 造成异构干扰 (cross-technology interference, CTI) [3, 4]. 例如, 共存于 2.4 GHz 频段的 Wi-Fi 和 ZigBee 设备在同时发送数据包时, 相互干扰彼此的信息传输, 导致通信效率急剧下降 [5, 6]. 另一方面, 不同的通信协议有各自的优势与不足. 如 Wi-Fi 技术具备传输效率高的特点, 但功耗较高. ZigBee 技术能耗小但传输速率低. 有效整合不同协议的优势以提高频谱资源的利用率以及无线通信的效率成为物联网领域的一个研究方向.

针对以上物联网发展趋势, 越来越多的研究人员开始关注使用不同协议的设备之间通信机制的建立 [7, 8], 即异构物联网直联通信. 异构物联网直联通信 (cross-technology communication, CTC) 指通过特殊的信息调制方式使采用不同通信协议的异构物联网设备实现直接通信, 该技术不需要额外的网关设备进行通信协议间的转化. 如图 1 所示, 在整个物联网体系中, 异构物联网直联通信技术使得网络构建更加灵活. 传统的通信技术只能使同构设备之间进行直接通信, 异构物联网直联通信技术打破了异构设备间的通信壁垒, 使得异构的设备之间互联互通, 从而可以整合不同协议的优势, 使异构设备相互协作 [9]. 此外, 与基于网关的异构设备间通信相比, 异构物联网直联通信技术减少了额外的硬件开销和通信时延, 使得异构设备可以通过协商使用共享的频谱资源, 避免信道竞争带来的数据传输冲突, 提升通信性能 [10, 11].

实现异构物联网直联通信, 也需要克服一些挑战. 首先, 异构物联网直联通信的发送端与接收端设备需要共享同一频段, 频谱资源的共享虽然导致了异构设备之间的互相竞争与干扰, 但也为异构设备间直接通信提供了机会. 其次, 异构的物联网设备采用不同的底层协议标准, 如 Wi-Fi 采用 IEEE 802.11 标准, ZigBee 采用 IEEE 802.15.4 标准, 不同标准所规定的调制解调方案不同, 物联网设备无法正确解调异构设备的数据包, 因此, 需要制定特殊的调制解调方案克服异构设备间不兼容的底层标准. 最后, 为了不影响物联网设备的正常通信, 以及加快相应技术的部署应用, 异构物联网直联通信技术要求通信机制对于硬件是透明的, 即不修改现有的硬件设施.

基于上述背景, 本文首先分析和总结异构物联网直联通信技术的研究现状; 在此基础上, 提出了实现异构物联网直联通信的关键技术: 数据包级、信号级和符号级的异构物联网直联通信技术; 之后, 介绍了所提相关技术在异构物联网设备共存场景下的抗干扰协调应用; 最后, 总结全文并展望了异构物联网直联通信技术的未来发展方向.

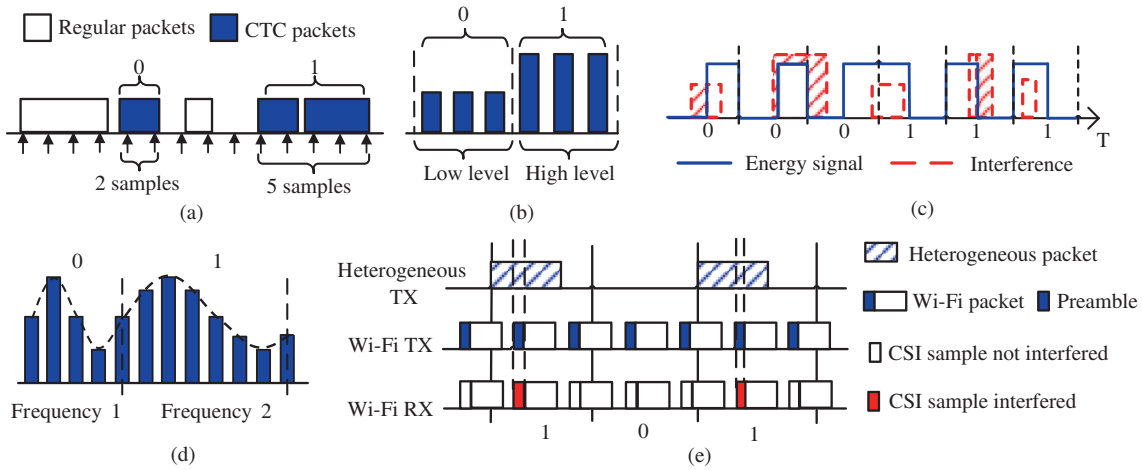

图 2 (网络版彩图) 现有的异构物联网直联通信调制方案

Figure 2 (Color online) Existing cross-technology communication modulation scheme. (a) Length of packets; (b) energy level of packets; (c) energy change; (d) energy envelope; (e) signal characteristics

2 研究现状

2.1 基于网关的异构通信

传统上, 异构无线设备之间进行通信时, 需要借助网关设备进行协议的转换 [12]. 然而, 异构设备利用网关进行间接通信存在固有的局限性. 首先, 利用网关会带来额外的硬件开销和部署任务, 这增加了异构设备间进行通信的成本. 其次, 基于网关的方案会产生大量经过网关的流量开销, 这进一步加剧了干扰, 并且容易导致由于网关节点压力过大造成单点故障. 第三, 网关必须提前部署, 这使得移动和临时的场景下, 异构设备通信变得困难. 第四, 由于引入了网关设备, 异构设备间端到端通信的时延增加, 进一步影响了网络性能 [13]. 网关方案固有的局限使得该方案在某些场景下难以适用, 为此, 研究人员尝试构建免网关的异构物联网直联通信.

2.2 免网关的异构物联网直联通信

由于具有不兼容的物理层, 异构无线设备无法相互解调彼此的信号, 然而设备能够通过信道感知的方法探测到信道中来自其他异构设备的数据包. 数据包在传输过程中表现为一段持续的高能量信号, 异构物联网直联通信的接收端可以通过感知并采样信道上的能量获取数据包的长度、能量和序列等特征 [14,15]. 据此, 研究人员利用数据包的不同特征进行信息的调制, 从而实现免网关的异构物联网直联通信, 如图 2 所示, 已有异构物联网直联通信研究所利用的数据包的特征有: 数据包长度、数据包能量水平和能量包络、数据包的信号特征等. 表 1 [8,14,16~23] 总结了现有基于数据包特征的异构物联网直联通信技术研究.

利用数据包长度进行调制. 数据包长度是无线数据包的共有特征. 如图 2(a) 所示, 数据包在传输过程中表现为一段持续的高能量信号, 数据包长度可由信号持续的时长衡量, 异构物联网直联通信的接收端可以通过感知并采样信道上的能量判断数据包长度. 基于数据包长度的异构物联网直联通信要求发送端和接收端遵循同一套定义了数据包长度与传输信息对应关系的映射表. 异构物联网直联通信时, 依据映射表, 发射端选择合适的数据包持续时间来调制信息, 接收端通过查表解码出对应信息. 利用数据包长度调制异构直联信息的思想简单且相对通用, 为利用数据包实现异构物联网直联通信开拓

表 1 现有基于数据包特征的异构物联网直联通信技术

Table 1 Summary of existing cross-technology communication based on packet patterns

Method	Transmitter and receiver	Modulation	Throughput
Esense [16]	802.11 → 802.15.4	Packet length	326 bps
HoWiES [17]	Wi-Fi → ZigBee	Packet length	–
LtFi [18]	LTE-U → Wi-Fi	Energy level	75 bps
WiZig [19]	Wi-Fi → ZigBee	Energy level	153.85 bps
StripComm [20]	Wi-Fi ⇄ ZigBee	Energy level	Wi-Fi → ZigBee: 1.1 Kbps
			ZigBee → Wi-Fi: 77.8 bps
Amphista [8]	ZigBee → Wi-Fi	Energy level	2.5 Kbps
ZigFi [21]	ZigBee → Wi-Fi	Channel state information	215.9 bps
DopplerFi [22]	BLE → Wi-Fi	Carrier frequency offset	6.5 Kbps
Gsense [23]	ZigBee → Wi-Fi	Packet interval & timing	–
B2W2 [14]	BLE → Wi-Fi	Energy envelope	BLE → Wi-Fi: 3.1 Kbps

了思路, 但它也存在一些问题. 除了用于异构物联网直联通信的数据包, 接收端也会感知到正常通信的数据包, 它们不存在明显差异, 接收端设备很难将它们区分开, 因此异构物联网直联通信容易受到正常通信的干扰. 为让接收端正确识别数据包, Chebrolu 等 [16] 提出的解决方案是在数据包长度选择上主动区分: 统计正常通信中数据包长度的频率分布, 选择出现频率低于阈值的长度用于异构物联网直联通信. 在这种方法中, 阈值设定得越低, 异构物联网直联通信的抗干扰能力就越强, 但可选的数据包长度范围减小, 通信效率降低. 另一个问题是可传递信息量受限. 可传递信息量受制于映射表的大小, 而映射表又受制于数据包长度的选择范围.

利用数据包能量水平进行调制. 可用于异构物联网直联通信的数据包特征还有能量水平. 已有工作中将能量水平用于信息调制的方法主要有 3 种: 多能级、能量变化、能量包络和能量间隔. 如图 2(b) 所示, 多能级的调制方法是将固定水平的能量与特定的比特信息相对应, 接收端感知能量水平后即可通过异构物联网直联通信协议预设的映射关系进行解调. 这种方法会受到信道中环境噪声的干扰, 为此, Guo 等 [19] 设计的 WiZig 根据信道条件, 动态、自适应地调整调制策略 (包括控制能量水平及接收窗口大小), 提升了环境噪声干扰下的通信性能. 如图 2(c) 所示, 使用能量变化, 如上升沿和下降沿直接调制异构物联网直联通信的 0/1 比特 [19], 可以避免单一数据包状态的不可靠性, 对噪声具有一定的抗干扰能力. 而且, 直接调制 0/1 比特能够减少接收端的解调步骤, 同时节省协议因信息映射占用的设备内存. 数据包组合成的能量包络, 是数据包能量水平的另一个重要特征. 如图 2(d) 所示, 利用此特征的异构物联网直联通信技术不是利用单个数据包的特殊能量水平进行调制解调, 而是对数据包组的能量包络进行调制, 使其具有更强的抗随机噪声的能力. Chi 等 [14] 设计的 B2W2 将能量包络模拟成离散正弦波, 通过正弦波的不同频率调制异构直联信息. Zhang 等 [23] 在数据包前加入特定的前导码, 前导码对应多个能量脉冲, 利用能量脉冲之间的间隔进行信息调制, 但实现该方案需要修改硬件, 限制了其在现有商用设备上的部署.

利用数据包信号特征进行调制. 虽然基于数据包长度和能量水平的调制方法在异构物联网直联通信中较为适用, 但也容易受到其他无线数据包的干扰. 为了缓解共存干扰, 提高低信噪比下的通信可靠性, 研究人员提出利用数据包的特殊信号特征构建异构物联网直联通信, 其中典型的信号特征包括: 信道状态信息 (channel state information, CSI) 和载波频偏 (carrier frequency offset, CFO). 在无线通

信中, 信道状态信息指通信链路的信道属性, 它描述信号在每条信道上传输所受到的影响. 信道状态信息包含在 Wi-Fi 数据包的前导码中, Wi-Fi 接收端可以根据信道状态信息值来计算出不同子载波上的相位与幅度信息. 由于信道状态信息 (CSI) 比接收信号强度 (received signal strength, RSS) 更容易获取并且精确度高, 因此利用信道状态信息进行异构物联网直联通信具有更强的鲁棒性. 信道状态信息可被用于实现非 Wi-Fi 协议的无线通信技术 (如 ZigBee、蓝牙) 到 Wi-Fi 的异构物联网直联通信. 如图 2(e) 所示, Wi-Fi 与其他协议发生信道重叠后, Wi-Fi 数据包前导码中的信道状态信息会产生明显变化. 于是, 依据信道状态信息, 正常与受到干扰的数据包即可被分别解调为异构直联信息的 0/1 比特 [21]. 在运用信道状态信息建立异构物联网直联通信时, 发射端需要合理选择发射功率, 避免触发载波侦听多路访问 (carrier sense multiple access, CSMA) 机制, 影响 Wi-Fi 的正常通信. 载波频偏是无线通信中的常见现象, 无线设备的非理想本地振荡器以及运动物体的多普勒效应都有可能导致载波频偏. 载波频偏也存在于诸如蓝牙的调频信号中. 研究人员观察到无线通信能够容忍的频率偏移远高于正常通信中存在的固有频偏, 于是 Wang 等 [22] 通过调节载波频率, 利用固有频偏以外的冗余频偏调制信息, 成功实现 Wi-Fi 到蓝牙的异构物联网直联通信.

综上所述, 虽然基于数据包的特征可以实现异构物联网直联通信, 但目前的解决方案存在较多问题: (1) 信道利用率和吞吐量较低; (2) 部分方案需要专用的硬件设备; (3) 部分方案引入了额外的数据包流量开销.

3 异构物联网直联通信技术

针对目前异构物联网直联通信技术研究现状和存在的问题, 本节提出了异构物联网直联通信技术框架, 如图 1(b), 包括数据包级的异构物联网直联通信技术、信号级的异构物联网直联通信技术和符号级的异构物联网直联通信技术. 数据包级的异构物联网直联通信利用数据包级的特征进行数据的调制, 由于数据包级的特征可以普遍地被异构的物联网设备感知, 所以很容易建立起双向的异构物联网直联通信, 但由于利用稀疏的数据包级特征进行信息的调制, 其吞吐量受到很大的限制. 信号级的异构物联网直联通信通过在发送端模拟接收端可识别的信号, 从而被接收端接收并解码, 这显著得提高了异构物联网直联通信的吞吐量. 但此类方法要求发送端设备的整体能力强于接收端, 因此不适用于性能较弱的发送端. 符号级的异构物联网直联通信利用细粒度的符号级的特征进行数据传输, 在提高吞吐量的同时, 适用性也进一步提高. 本节将分别详细阐述这 3 种异构物联网直联通信技术细节.

3.1 数据包级的异构物联网直联通信技术

本小节将已有的异构物联网直联通信研究归纳为数据包级的异构物联网直联通信技术, 并提出将普通的数据帧而非信标帧作为信息的载体, 吞吐量提升的同时不需要引入额外的数据包. 数据包级的异构物联网直联通信技术核心思想为, 发送端依据将要发送的数据控制数据帧的时间、长度等指标, 构建相应的可被异构设备感知的特征, 接收端通过信道感知并采样信道上的能量获取数据包的特征信息, 从而接收相应的数据.

基于数据包的时域特征进行调制. 本文基于数据包的时域特征, 通过改变周期性信标帧的时间, 将信标帧的时间偏移量作为信息载体, 实现了异构物联网直联通信, 但由于基于数量有限的信标帧, 信道利用率和通信吞吐量仍有很大的限制. 为此, 进一步将普通的数据包而非信标帧作为信息传输的载体, 如图 3(a), 利用普通的数据包时域特征进行调制, 将数据包的发送时间偏移到特定节点. 对于接收端, 通过累计一个周期内接收到的符号数量, 将整个周期中出现频率较高的符号作为最终的解码符号.

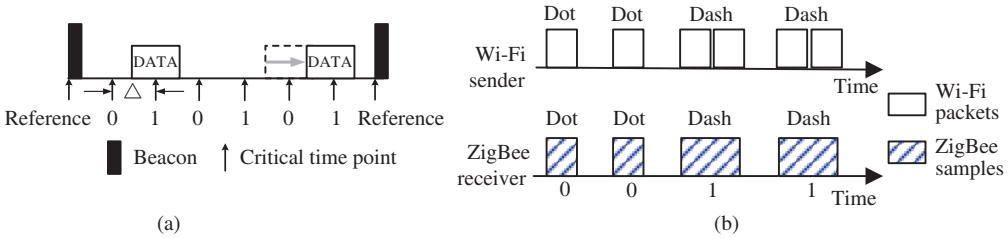

图 3 (网络版彩图) 数据包级的异构物联网直联通信调制方案

Figure 3 (Color online) Cross-technology communication of packet level. (a) Patterns of packet timing; (b) patterns of packet sequence

例如, 通过累计采样的接收信号强度指示 (received signal strength indication, RSSI), 发现较高的 RSSI 值都在时间点 “1” 附近, 因此发送数据包的时间点 “1” 的频率高于时间点 “0”, 将传输的信息解调为符号 “1”. 此外, 基于不同的发送周期, 接收端可以将采集到的信号进行分组解调. 因此可以实现多对一通信或者提高单路通信的传输速率.

基于数据包序列特征进行调制. 与基于单个数据包特征不同, 基于数据包序列特征的异构物联网直联通信将传输给异构设备的数据嵌入到数据包序列的分布特征中. 由于接收端需根据一组数据包的序列特征才能解调出相应的信息, 这种调制方式提高了异构物联网直联通信的抗干扰能力. 本文同时利用数据包的包长特征和包间间隔特征进行信息调制, 如图 3(b), 利用短数据包 (点) 和长数据包 (线) 组合调制 0/1 比特, 将信息编码成类似摩尔斯码的形式. 接收端通过感知信号能量特征进行信息的接收和解码. 基于数据包序列的特征, 不仅提高了信息传输的整体吞吐量, 也为提供可靠的异构物联网直联通信提供了方案.

3.2 信号级的异构物联网直联通信技术

信号级的异构物联网直联通信技术通过模拟异构无线通信协议相应的信号实现直接通信. 相比于利用粗粒度的数据包特征进行信息的调制, 信号级的异构物联网直联通信吞吐量得到很大的提升.

信号模拟是实现信号级异构物联网直联通信的主要方法, 其核心思想为, 在发送端通过控制数据包的有效载荷部分, 即模拟接收端的波形, 使得发送端的无线发射器产生能够被异构无线设备正确接收并解调的信号. 如图 4(a) 所示, 依据传输给接收端的信息所对应的物理层目标信号, 通过反向工程, 推导出可以通过发送端设备产生的最接近目标信号的数据包报文内容. 发送端发送数据包后, 有效载荷部分可以成功通过接收端的前导码检测, 从而被成功解调. 理论上, 基于信号模拟的异构物联网直联通信可以实现和接收端设备使用的无线技术同等的传输速率.

例如当实现 Wi-Fi 到 ZigBee 的异构物联网直联通信系统时, 在 Wi-Fi 发送端, 通过信号模拟的方式得到 Wi-Fi 帧的特殊的有效载荷, 使得有效载荷对应的射频波形类似于 ZigBee 信号的射频波形. 当这样的一个 Wi-Fi 帧被射频前端发送到信道中后, ZigBee 接收端将 Wi-Fi 帧的头部、前导码部分和尾部当做噪声忽略, 而有效载荷部分将成功地通过 ZigBee 的前导码检测, 即被视为合法的 ZigBee 数据帧, 并在 ZigBee 接收端解调相应的有效载荷. 其中信号模拟, 即得到具体的有效载荷的过程, 则需要依据传输给接收端的信息所对应的物理层目标信号, 通过反傅里叶变换、逆向的正交幅度调制, 以及逆向的信道编码等反方向流程, 推导出通过发送端设备可以产生的最接近目标信号的数据帧内容. 信号模拟存在一定程度的失真, 但 ZigBee 调制方式的冗余机制可以提升鲁棒性 [6]. 发送端发送数据帧后, 有效载荷部分可以成功通过接收端的前导码检测, 从而被成功解调. 在整个过程中, ZigBee 接收

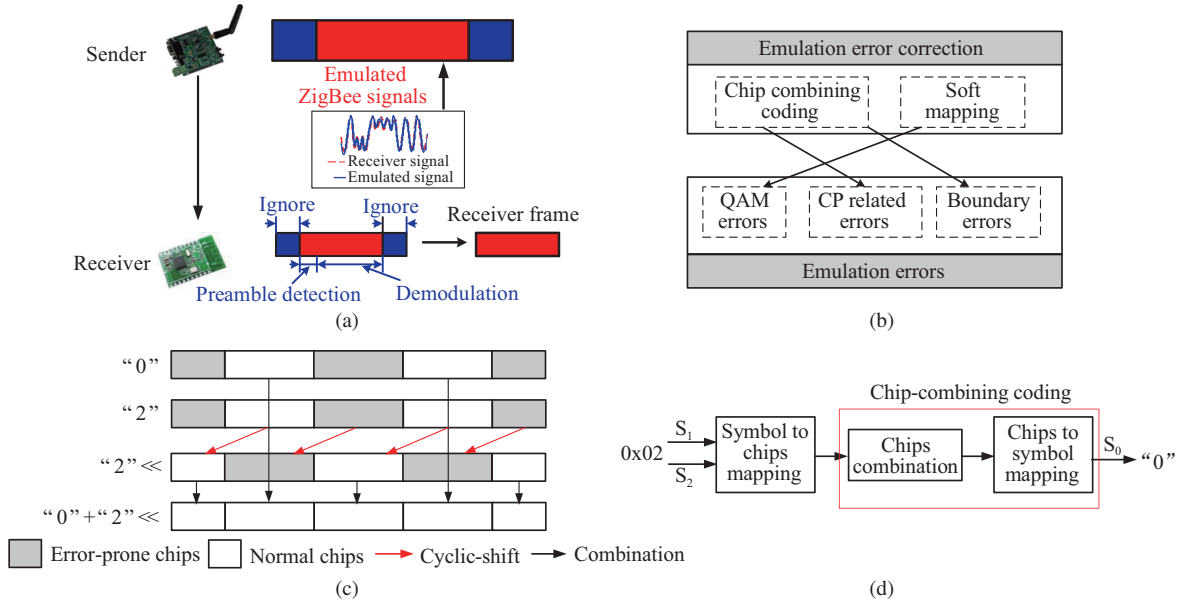

图 4 (网络版彩图) 信号级的异构物联网直联通信

Figure 4 (Color online) Cross-technology communication of signal level. (a) Cross-technology communication based on signal emulation; (b) recovery of emulation errors; (c) diagram of chip-combining coding; (d) decoding process

器不能区分发送方是 ZigBee 设备还是 Wi-Fi 设备, 因此整个方案对于硬件是透明的. 当实现蓝牙到 ZigBee 的异构物联网直联通信系统时, 利用蓝牙和 ZigBee 在调制解调方式上的相似性, 可以使用相位信息进行数据调制, 在蓝牙端可以模拟出被 ZigBee 接收器正确解调的信号. 此外, ZigBee 利用相位的正负进行信息调制, 这进一步增加了蓝牙到 ZigBee 基于信号模拟的异构物联网直联通信的鲁棒性.

信号模拟方式. 根据分析信号的角度不同, 可将信号模拟分为频域模拟和时域模拟两种. 频域模拟是在频域上模拟目标波形, 即将目标信号通过傅里叶变换转换到频域来映射相应的最近星座点, 这个过程由于时域到频域的转换会带来一定量化误差. 时域模拟是在时域上进行目标信号的模拟, 即在时域将目标信号的采样点与离散的星座点映射. 这很大程度降低了量化的误差, 甚至可以达到零误差. 可靠的信号模拟为信号级的异构物联网直联通信性能打好了基础.

信号模拟的误差与修正. 虽然基于信号模拟的异构物联网直联通信在提高异构设备间通信吞吐量方面取得了巨大成功, 但由于异构设备不兼容的底层标准以及硬件本身的限制, 信号模拟不可避免地会带来模拟误差, 因此通信可靠性有待进一步提高. 本文通过分析 Wi-Fi 到 ZigBee 基于信号模拟的异构物联网直联通信过程, 得到其信号模拟的误差来源, 如图 4(b), 包括正交幅度调制时的量化误差、循环前缀带来的部分符号错误, 以及信号分割与拼接带来的边界误差. 为消除量化误差, 本文在信号模拟阶段没有按照 IEEE 802.15.4 标准所规定的符号 – 码元映射关系, 而是采用软映射的方式, 即根据统计得到的模拟符号的码元概率分布, 制定新的符号到码元映射关系. 对于循环前缀带来的模拟错误和边界误差, 本文利用 IEEE 802.15.4 标准所规定的伪随机序列的循环移位特点, 制定了码元组合的编码方式. 如图 4(c), Wi-Fi 发送端想要通过信号模拟的方式发送符号 "0", 则在发送端同时发送符号 "0" 循环右移 8 个码元后的符号 (易错段的长度为 8 个码元), 对于此例为符号 "2". 对于 ZigBee 接收端, 由于硬件的限制, 无法直接获取到码元的信息. 如图 4(d), 经过 ZigBee 设备的初步解调, 得到符号 "0x02", 之后通过符号组合编码, 即将符号 "2" 循环左移 8 位后与符号 "0" 组合得到新的码元序

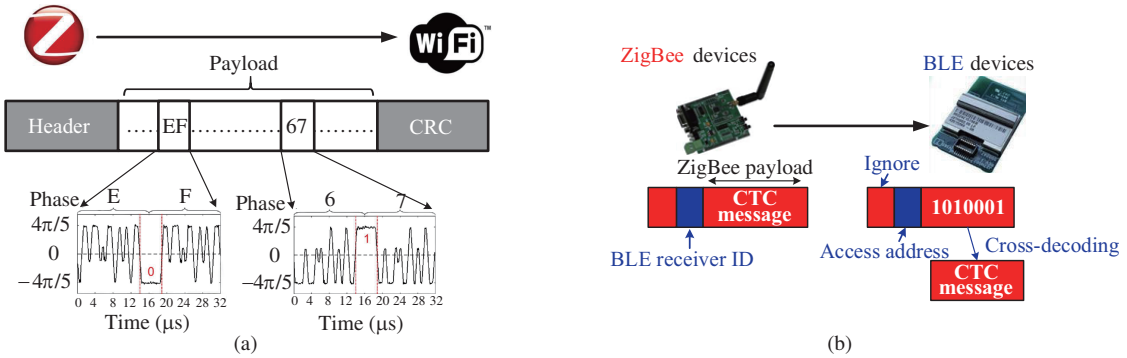

图 5 (网络版彩图) 符号级的异构物联网直联通信

Figure 5 (Color online) Cross-technology communication of symbol level. (a) Cross-technology communication based on symbol construction; (b) cross-technology communication based on cross decoding

列, 再通过符号 – 码元映射表, 可以将新的码元序列成功解码得到符号 “0”. 由此可见, 通过这种方案, 很大程度上提升了基于信号模拟的异构物联网直联通信可靠性, 并且没有修改相应的硬件条件. 基于信号模拟的异构物联网直联通信的另一个特点是, 发送端对于不同符号的模拟能力不同, 如 Wi-Fi 发送端对不同的 ZigBee 符号有着不同的模拟精度. 由于 ZigBee 报头中包含了重要的字段, 如同步字, 故可以利用特殊的报头来更好地进行信号模拟, 并利用相应的特定编码方式, 进一步提高整体的可靠性.

并行通信. 除了传输速率的大幅提升, 信号模拟还可以实现并行的异构物联网直联通信. 例如由于 Wi-Fi (20 MHz) 相比 ZigBee (2 MHz) 有更大的带宽, 所以在一个 Wi-Fi 帧里能够模拟两个不同频段的 ZigBee 帧, 多个工作在不同信道上的 ZigBee 接收器可以同时独立地接收和解调不同的模拟的数据帧, 从而实现两路并行的异构物联网直联通信, 达到两倍的总吞吐量和更高的频谱效率.

3.3 符号级的异构物联网直联通信技术

基于信号模拟的异构物联网直联通信在发送端生成可以直接被异构设备识别的信号, 从而极大地提高了异构物联网直联通信技术的吞吐量和实用性. 但是基于信号模拟的异构物联网直联通信技术在性能较强的发送端上才能实现, 例如 Wi-Fi 到 ZigBee 的异构物联网直联通信, 性能强的发送端支持复杂的调制方式为信号的模拟提供了很高的自由度. 而对于发送端能力弱的情况, 如 ZigBee 到 Wi-Fi 的异构物联网直联通信, 由于二者通信带宽差别较大, 信号模拟的方式并不适用. 本小节介绍基于细粒度的符号级特征的异构物联网直联通信技术, 主要包括符号构造和交叉解码两种机制.

符号构造机制. 基于符号构造的异构物联网直联通信技术的思想为: 首先, 分析信号在异构设备端产生的可以被识别的特征, 如 ZigBee 设备发送特殊的字符时, 其信号在 Wi-Fi 设备端可以产生持续的相位特征; 然后, 基于分析得到的特征, 发送端通过符号编码方式, 控制有效载荷的内容, 使得发送端调制的信号可以在异构接收端产生易于被检测识别的特征, 从而被接收端成功解调. 例如, 利用基于符号构造的方式实现从 ZigBee 到 Wi-Fi 的异构物联网直联通信系统, 如图 5(a) 所示. 通过观测 ZigBee 信号在 Wi-Fi 设备端产生的特点, 发现 ZigBee 设备在发送符号 “EF” 和 “67” 的时候, 其信号在 Wi-Fi 接收端会产生一段持续稳定的相位, 分别为 $+4\pi/5$ 和 $-4\pi/5$, 这两组符号产生的稳定相位差达到 $8\pi/5$, 是所有可能出现的相位差中的最大值. 尽管 Wi-Fi 设备不能解码 ZigBee 设备发出的信号, 但其容易检测到持续出现的稳定相位信息, 因此, 两种特殊的相位信息可用于代表由 ZigBee 发送给 Wi-Fi 设备的 0/1 比特. 对于 ZigBee 发送端, 通过控制有效载荷部分, 将待发送的比特信息转换为 (6,

表 2 各类型异构物联网直联通信技术对比

Table 2 Comparison of different types of cross-technology communication technologies

Communication type	Throughput	Spectrum efficiency	Parallel communication	Bi-directional communication	Universality
Packet-level	Low	Low	No	Yes	High
Signal-level	High	High	Yes	No	Low
Symbol-level	High	High	–	No	Middle

7) 或 (E, F) 完成编码, 由于一个 ZigBee 符号为 4 位比特, 两个符号组合可以表示为一个字节, 因此 ZigBee 发送端将发送的比特信息嵌入到一个字节中, 其理论吞吐量为 ZigBee 标准的 1/8. 对于 Wi-Fi 接收端, 在空闲监听机制下, 只需要检测相位的正负即可解码相应的比特. 由于通过符号构造, 0/1 比特对应的相位分别为 $+4\pi/5$ 和 $-4\pi/5$, 因此允许存在一定的误差, 通过设定阈值, 可以有效降低噪声的干扰, 进一步提高异构物联网直联通信的可靠性.

交叉解码机制. 在接收端基于交叉解码的异构物联网直联通信将相对复杂的调制工作置于接收端. 其设计思想为, 如图 5(b) 所示, 发送端发送正常的无线信号, 接收端先将接收到的信号解调得到初步的比特信息, 然后以发送端符号为单位进行交叉解码, 得到发送端原本发送的消息. 交叉解码方法的可行性在于, 通过对接收端比特流的观察, 发现其中能够反映出一些所解调信号的内在特征, 比如振幅、频率、相位等. 与利用信号模拟的方式相同, 交叉解码机制将复杂的工作置于能力较强的设备端, 发送端和接收端都不需要进行硬件的修改, 因此很容易部署到已有的大量物联网设备. 例如, 基于交叉解码的方式实现 ZigBee 到蓝牙的异构物联网直联通信. 由于蓝牙和 ZigBee 在调制方式上具有相似性, 分别采用偏移四相相移键控 (OQPSK) 和高斯频移键控 (GFSK) 进行调制, 而频移和相移可以互相转化, 因此蓝牙设备可以把 ZigBee 信号解调成对应比特序列, 但由于蓝牙带宽为 ZigBee 带宽的一半, 蓝牙设备将两个码元对应的的 ZigBee 信号解调得到一个码元. 通过分析采样偏移与相移的关系, 可以得到 ZigBee 符号与蓝牙解码得到的比特序列的映射关系, 因此通过交叉解码校正, 可以成功得到发送端发送的信息.

3.4 小结

本节分别详细介绍了异构物联网直联通信的关键技术: 数据包级、信号级和符号级的异构物联网直联通信技术. 由于数据包级的特征可以较普遍地被异构的物联网设备感知, 数据包级的异构物联网直联通信技术很容易建立起双向的异构物联网直联通信, 但由于一个数据包的持续时间一般在毫秒级别, 其吞吐量受到一定的限制. 信号级的异构物联网直联通信技术通过在发送端模拟接收端可识别的信号, 实现异构物联网直联通信, 其数据传输速率理论上可以达到原无线通信技术的标准. 但信号级的异构物联网直联通信要求发送端设备的整体能力强于接收端, 不适用于性能较弱的发送端. 符号级的异构物联网直联通信技术利用细粒度的符号特征进行数据传输, 可以实现弱发送端到强接收端的较高速率的异构物联网直联通信.

表 2 对这 3 类异构物联网直联通信的性能进行了总结和对比. 从该表可以看出, 在数据传输速率和频谱利用率方面, 数据包级的异构物联网直联通信小于信号级和符号级的异构物联网直联通信, 这是因为数据包级异构直联采用粗粒度的数据包级的特征进行信息调制, 根据香农定理, 信号级和符号级的异构物联网直联通信技术的理论吞吐量更高; 在并行传输方面, 数据包级的异构物联网直联通信不支持并行传输; 在双向通信方面, 由于数据包级的特征普遍存在于无线网络协议中, 而信号级和符号级的异构物联网直联通信需要根据不同的无线网络协议采取特定的策略, 因此数据包级的异构物联

网直联通信更具有普适性, 更容易制定双向对称的异构物联网直联通信机制. 在实际应用场景中, 研究人员可以根据具体的无线通信设备和不同的应用需求, 采取相应的异构物联网直联通信技术.

4 异构物联网直联通信技术的应用示例

异构物联网直联通信的实现不仅为打破异构设备间的通信壁垒提供了机遇, 也为整合不同协议的优势, 改善现有物联网设备应用提供了新的思路. 例如, 异构物联网直联通信技术为降低能耗提供了新的机遇: 不同的无线通信设备的功耗差别很大, 一般情况下, Wi-Fi 设备的最大传输功率为 100 dBm, 而 ZigBee 设备的最大传输功率为 0 dBm. 通过利用异构物联网直联通信技术, 可以在能耗较高的物联网设备中嵌入能耗较低的异构通信模块, 使得高能耗设备的部分不必要的耗能工作交给低功耗的异构模块. 如对于移动应用中广泛使用的 Wi-Fi 模块, 在扫描状态、待机模式、唤醒后连接 Wi-Fi AP 时, 它不进行任何实际的通信, 但仍处于活动状态且消耗能量. 因此可以使用异构物联网直联通信技术, 将 Wi-Fi 模块的部分操作委托给一个低功率的 ZigBee 模块. 当没有数据包发送和接收时, Wi-Fi 模块将被关闭, 而 ZigBee 模块负责扫描网络, 并在检测到 Wi-Fi AP 或 AP 欲将与设备通信时唤醒 Wi-Fi 模块. 通过这样一个 Wi-Fi-ZigBee 异构物联网直联通信方案, 可以有效地减少 Wi-Fi 模块的能耗, 提高移动应用的性能.

此外, 异构物联网直联通信技术打破了原有技术的一些固有限制, 为异构物联网设备共存场景下的信道协调、减少异构设备间的通信干扰, 以及异构设备数据的收集提供了解决方案. 本节详细介绍异构物联网直联通信技术在这方面的应用.

4.1 基于异构共融的抗干扰协调

为了避免或消除设备间的相互干扰, 现行的无线局域网通用标准 IEEE 802.11 采用了载波监听多路访问/冲突避免的争用型频谱访问控制协议. 此外, IEEE 802.11 还设计了请求发送/清除发送协议 (request to send/clear to send, RTS/CTS) 用以减少隐藏节点所造成的干扰影响. 低速率无线个人局域网标准 IEEE 802.15.4 中采用了直接序列展频技术. 该技术使用多个码片来表示一位 0 或 1 信息, 把原来较窄频转化为具有较宽频的低功率频率, 从而增加抗干扰能力. 蓝牙技术标准中则采用了跳频技术. 采用该技术的发送设备和接收设备按照预先设定的一组频段进行跳变, 并在相应的频段上传送讯号. 跳频技术有效避免了设备间在同一频段上的冲突, 从而改善无线链路的传输质量并降低干扰. 然而传统的抗干扰协调机制往往针对同构网络设计, 并不适用于多种设备共存的异构网络.

相比于传统的单频段单协议方案, 认知无线电技术在频谱的利用上体现出极高的灵活性. 该技术通过感知其所在环境的频谱使用情况, 充分利用空闲频段, 从而在提高频谱利用率的同时避免了设备间的干扰 [24~29]. 机会式和覆盖式频谱共享是认知无线电技术中两种高效利用频谱的方式 [30~34]. Luo 等 [32] 指出在下垫式频谱共享中, 次级用户的传输功率需被严格限制在干扰传输功率下, 以保护主用户的传输质量. 在干扰消除方面, 华盛顿大学 (University of Washington) 的 Halperin 等 [35] 提出的干扰消除信号处理技术使单个接收器能够区分并成功接收来自多个非同步信号源的并发信号. 对于异构设备间的信道协调, 研究人员提出了多种被动信道协调方案 [36~41], 通过间接的频谱感知、扫描等方法来预测估计共享频谱上各种设备的信道使用信息, 根据信道状态来调整传输策略. 例如根据采样的信号强度指示 (RSSI) , 估计突发 Wi-Fi 流量并预留可用空白区域 [38]. 然而, 这些都是利用干扰避免或者从干扰中恢复信号的思路, 没有在占用信道前进行通信协商 [42, 43].

异构物联网直联通信技术打破了异构设备间的通信壁垒, 使得异构设备间具有直接沟通的能力.

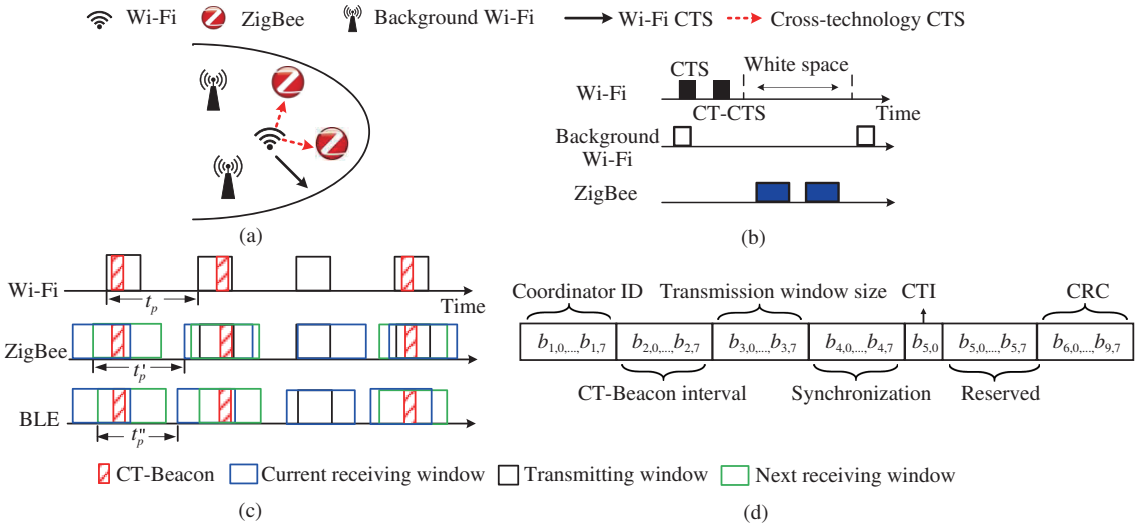

图 6　(网络版彩图) 基于异构共融的抗干扰协调机制

Figure 6　(Color online) Anti-interference coordination mechanism based on cross-technology communication. (a) The scenario; (b) coordination based on CT-CTS; (c) global cooperation based on CT-Beacon; (d) CT-Beacon format

而异构设备间沟通能力的获得, 使其不仅仅局限于通过感知周边信道环境来被动的协调设备间的信道使用, 而是可以主动的协商信道使用方案. 基于信道模型被动获取的信道环境信息以及异构直联主动获取的信道协调需求, 可以构建如图 6(b) 所示的基于异构共融的抗干扰协调机制. 在如图 6(a) 所示的 Wi-Fi 和 ZigBee 设备共存的场景中, 利用异构物联网直联通信技术可以建立异构设备间的请求发送/清除发送 (RTS/CTS) 机制. 一方面, RTS/CTS 机制可以通过设置阈值有效地解决信道使用碎片化的问题. 另一方面, 异构物联网直联通信技术的实现使 RTS/CTS 机制不仅仅局限于 Wi-Fi 设备之间. 异构设备间的 RTS/CTS 机制可以帮助 Wi-Fi 和 ZigBee 设备高效地协商信道使用从而有效避免设备间干扰.

如图 6(b) 所示, Wi-Fi 设备发送异构直联 CTS (图中以 CT-CTS 标示) 请求使用一段时间的信道, 该段空闲信道将被赋予周围的 ZigBee 设备使用. 这是由于 Wi-Fi 发送的 CT-CTS 本身可被图中的 Wi-Fi 设备接收, 这些背景 Wi-Fi 设备在接收到 CT-CTS 将会空出信道. 而 CT-CTS 又可被 ZigBee 设备解码, 因而 ZigBee 设备得知该空闲信道将被赋予自身使用. 异构直联 CTS 技术可以有效地避免 Wi-Fi 和 ZigBee 设备之间因相互抢占信道造成的干扰, 使异构设备高效地共享频谱资源.

4.2　基于异构共融的全局协调

Wi-Fi 和蓝牙设备的媒体访问控制层 (media access control, MAC) 分别采用载波侦听多路访问 (CSMA) 和时分多址接入 (time division multiple access, TDMA) 方案. ZigBee 设备可以使用这两种方案来访问网络. 然而, 基于 CSMA 的方案可能会以随机时间延迟异构物联网直联通信数据包的传输, 基于 TDMA 的方案只在一个固定的时隙接收数据包. 此外, 不同设备之间的时钟漂移使得蓝牙和 ZigBee 等低占空比设备更不容易接收到异构物联网直联通信的数据包. 考虑到这些因素, 如何设计一个异构 MAC 方案, 在保证网络性能的情况下, 使 Wi-Fi 节点发送的数据包能够成功被 ZigBee 和蓝牙设备接收是一个关键而又困难的问题.

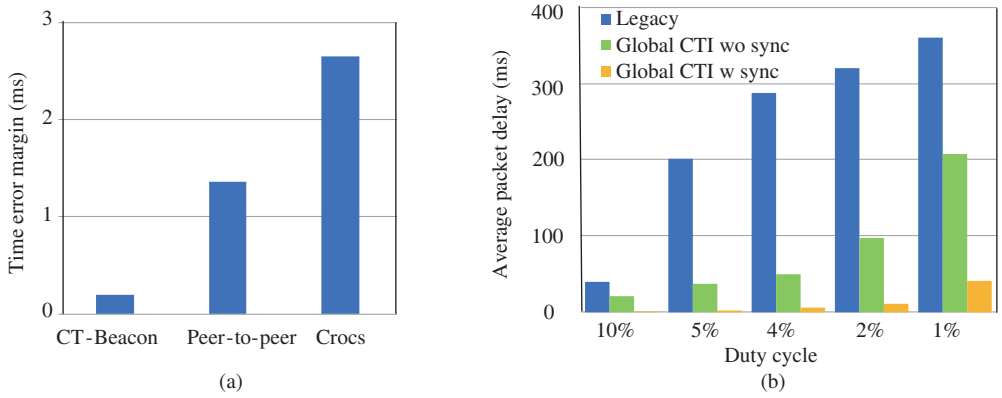

图 7 (网络版彩图) 基于异构共融的全局协调实验评估

Figure 7 (Color online) Experimental evaluation of global coordination based on cross-technology Beacon. (a) Synchronization time error margin for different schemes. "CT-Beacon" means the proposed global coordination scheme, "peer-to-peer" refers to the PHY communication approaches among a single pair of technologies; (b) average packet delay with different schemes. "legacy" refers to the scheme without global CTI coordination

为此, 本文提出了一种统一的媒体访问控制 (MAC) 方法, 实现了全局协调异构设备进行信息传输和接收, 从而很大提高了通信效率. 具体地, 如图 6(c) 所示, 该方案设计了 CT – 信标 (cross technology Beacon, CT-Beacon) 用来协调异构物联网直联通信消息的传输和接收. 对于 Wi-Fi 发送器和 ZigBee, BLE 接收器, 通过设置信息发送和接收窗口, 使得异构的设备在这些窗口内进行异构物联网直联通信消息的传输和接收. 通过周期性的接收 CT – 信标并相应地调整接收窗口的开始时间, 可以大大降低由于数据包延迟或时钟漂移而导致的接收端错过异构物联网直联通信消息的概率. 并且该方案不会给异构网络带来显著的带宽和能量开销.

对于 CT – 信标, 通过设计其数据包的格式, 可以实现异构设备的全局同步和协调. 如图 6(d) 所示, 第 1 个字节表示协调器的 ID 号, 该协调器可以与 ZigBee、蓝牙和其他 Wi-Fi 设备通信. 第 2 个字节表示 CT – 信标间隔 (单位是 ms), 最大 CT – 信标间隔是 127 ms. 第 3 个字节用于表示传输窗口长度 (单位是 100 μs), 最大传输窗口是 12.7 ms. 后面的两个字节用于特定的应用程序. 例如, 一个字节用于设置全局同步的间隔; 1 位用于抗异构干扰协调, 7 位保留为未来使用. 最后是 4 字节的 CRC, 用于保证 CT – 信标的可靠传输.

当进行全局同步时, 可以在 CT – 信标中设置时间戳, 并将同步消息置于 CT – 信标后. 当进行全局抗异构干扰协调时, Wi-Fi 协调器向 Wi-Fi、ZigBee 和蓝牙设备发送一个全局 CTS 数据包, 以保留一段无 Wi-Fi 干扰的空白空间, 该协调信息在 CT – 信标之后发送. 设备可以通过比特 $b_{5,0}$ 判断有无可用的无 Wi-Fi 干扰通道, 如图 6(d) 所示. 若 $b_{5,0}=0$, 则 CT – 信标后没有无 Wi-Fi 干扰周期, 因此 ZigBee 和蓝牙设备可转为休眠模式以节约能耗. 若 $b_{5,0}=1$, 则将发送一个抗异构干扰协调的数据包, 该数据包包含一个 CTS 消息以及信道保留消息. 一旦其他 Wi-Fi 节点接收到 CTS, 它们将在 CTS 指定的一段时间内停止访问网络. 而 Zigbee 和蓝牙设备将使用保留的空间进行数据传输.

本文对 ISM 频段中采用不同通信协议的主流物联网设备: Wi-Fi、ZigBee 和蓝牙设备进行全局协调的实验以及评估. 对于全局时间同步, 本文使用 Wi-Fi 设备作为协调器来传输异构直联通信消息进行异构设备间的时间同步. 如图 7 所示, 实验结果表明, 基于 CT – 信标的统一媒体访问控制方案使得异构设备平均时间同步误差在 0.2 ms 以内. 与采用传统的媒体访问控制方案 Crocs [9] 相比, 时间同步误差减少到十三分之一. 对于全局的抗异构干扰信道协调, 数据包平均时延降低到九分之一. 通过统一

的媒体访问控制方案, 低功耗的 ZigBee 和蓝牙设备更容易检测到没有被 Wi-Fi 设备占用的空闲信道, 从而增加了信道资源的利用率.

4.3 异构物联网设备数据的收集

基于异构物联网直联通信技术, 可以实现异构设备数据的直接收集, 而不需要经过网关等中间设备. 例如, 使用一个 Wi-Fi 网卡直接收集来自异构设备的数据.

当异构设备的数据包与正在传输中的 Wi-Fi 数据包碰撞后, 经过 Wi-Fi 接收端的解调, 异构的数据包内容仍然存在. 经过波形重建和解码等过程, 可以重新获取相应的异构数据包内容. 具体地, 该技术将 Wi-Fi 网卡解调得到的数据作为输入, 经过编码比特重建和子载波映射, 可以得到相应的频域数据, 然后通过反傅里叶变换, 可以成功得到对应的时域波形. 由于 Wi-Fi 网卡的解调过程中丢弃奇偶校验码和循环前缀部分, 重建的波形会丢失一少部分波形片段. 基于波形丢失的位置特点, 可以分别在符号层面和码元层面调整相应的解码策略, 从而得到正确的数据包. 整个过程中没有修改 Wi-Fi 网卡的硬件部分, 因此兼容现有的 Wi-Fi 商用网卡, 并且该技术可以重建多种不同协议的波形, 具有普适性. 该技术使得 Wi-Fi 设备可以同时接收并解码来自多个不同的异构设备的数据包, 很大提升了从异构设备收集数据包的效率.

5 总结与展望

异构物联网直联通信技术相比于传统的利用网关进行异构设备间间接的通信, 其在减少硬件开销和加快应用部署等方面有很大的优势. 本文从数据包级、信号级、符号级 3 个层面分析和探讨了异构物联网直联通信关键技术和解决方案. 数据包级的异构物联网直联通信利用数据包的长度、能量水平, 以及序列特征等数据包信息进行调制, 很容易实现双向的异构物联网直联通信. 信号级和符号级的异构物联网直联通信通过信号模拟、交叉解码等方式直接生成或者解码异构物联网直联通信的物理层符号, 其数据传输速率理论上可以达到原无线通信技术的标准. 然而, 目前异构物联网直联通信还有若干关键技术亟待研究.

一是各层异构物联网直联通信协议的配合. 要将异构物联网直联通信技术真正应用在某一个场景中, 除了本文介绍的异构物联网直联通信技术, 还需要上层包括链路层、网络层、应用层等相应协议的改进与支持, 各层协议间相互配合才能使得整个网络体系及应用系统更加灵活高效 [44]. 例如, 传统的链路层采用接收信号强度指示 (RSSI) 和信噪比 (signal noise ratio, SNR) 对链路质量进行检测, 但由于异构物联网直联通信双方的协议存在差异, 这些衡量指标不再适用, 为此需要研究链路层跟踪信道状态、检测链路质量的新方案 [45]. 基于物理层的异构物联网直联通信特点, 调整上层通信协议, 从而达到较好的应用性能, 是未来研究需要解决的一个重要问题.

二是通信安全. 虽然异构物联网直联通信为物联网的发展带来了新思路, 但是不可避免地, 异构物联网直联通信也会带来通信安全方面的问题. 例如, 数据包级的异构物联网直联通信对于信道中的能量信息比较敏感, 当对其进行干扰攻击时, 异构物联网直联通信的可靠性会大大降低 [46, 47]. 另外, 当 ZigBee 设备与 Wi-Fi AP 通过异构物联网直联通信技术进行通信的时候, ZigBee 设备更容易受到远程攻击. 由此, 随着异构物联网直联通信技术越来越成熟, 通信安全方面的研究需求也更加迫切.

参考文献

1 Zhao Z H, Wu X X, Zhang X, et al. ZigBee vs WiFi: understanding issues and measuring performances of their

coexistence. In: Proceedings of the 33rd IEEE International Performance Computing and Communications Conference (IPCCC'14), Austin, 2014
2 Zhang X Y, Shin K G. Enabling coexistence of heterogeneous wireless systems: case for zigbee and wifi. In: Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'11), 2011. 1–11
3 Zhang X Y, Shin K G. Cooperative carrier signaling: harmonizing coexisting WPAN and WLAN devices. IEEE/ACM Trans Netw, 2013, 21: 426–439
4 Yang P L, Yan Y B, Li X Y, et al. Taming cross-technology interference for Wi-Fi and ZigBee coexistence networks. IEEE Trans Mobile Comput, 2015, 15: 1009–1021
5 Huang J, Xing G L, Zhou G, et al. Beyond co-existence: exploiting wifi white space for zigbee performance assurance. In: Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP'10), Kyoto, 2010. 305–314
6 Liang C J M, Priyantha N B, Liu J, et al. Surviving Wi-Fi interference in low power zigbee networks. In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems (SenSys'10), Zurich, 2010. 309–322
7 Wang W, He S Y, Sun L, et al. Cross-technology communications for heterogeneous IoT devices through artificial Doppler shifts. IEEE Trans Wirel Commun, 2019, 18: 796–806
8 Chi Z C, Li Y, Huang Z C, et al. Simultaneous Bi-directional communications and data forwarding using a single ZigBee data stream. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'19), Paris, 2019. 577–585
9 Yu Z H, Jiang C K, He Y, et al. Crocs: cross-technology clock synchronization for Wi-Fi and ZigBee. In: Proceedings of International Conference on Embedded Wireless Systems and Networks (EWSN'18), Madrid, 2018. 135–144
10 Wang E, Liu X, Yao Y, et al. CRF: coexistent routing and flooding using Wi-Fi packets in heterogeneous IoT networks. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'19), Paris, 2019. 19–27
11 Wang W, Xie T T, Liu X, et al. ECT: exploiting cross-technology concurrent transmission for reducing packet delivery delay in IoT networks. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'18), Honolulu, 2018. 369–377
12 Jin T, Noubir G, Sheng B. WiZi-Cloud: application-transparent dual ZigBee-WiFi radios for low power Internet access. In: Proceedings of IEEE INFOCOM 2011, Shanghai, 2011. 1593–1601
13 Chi Z C, Huang Z C, Yao Y, et al. EMF: embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'17), Atlanta, 2017
14 Chi Z C, Li Yan, Sun H Y, et al. B2W2: N-way concurrent communication for IoT devices. In: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys'16), Stanford, 2016. 245–258
15 Sankhe K, Muncuk U, Naderi M Y, et al. Talking when no one is listening: piggybacking city-scale IoT control signals over LTE. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'18), Honolulu, 2018. 1547–1555
16 Chebrolu K, Dhekne A. Esense: energy sensing-based cross-technology communication. IEEE Trans Mobile Comput, 2013, 12: 2303–2316
17 Zhang Y F, Li Q. HoWiES: a holistic approach to ZigBee assisted Wi-Fi energy savings in mobile devices. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'13), Turin, 2013. 1366–1374
18 Gawlowicz P, Zubow A, Wolisz A. LtFi: cross-technology communication for RRM between LTE-U and IEEE 802.11. 2017. arXiv: 1707.06912
19 Guo X Z, Zheng X L, He Y. WiZig: cross-technology energy communication over a noisy channel. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'17), Atlanta, 2017
20 Zheng X L, He Y, Guo X Z. StripComm: interference-resilient cross-technology communication in coexisting environments. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'18), Honolulu, 2018. 171–179
21 Guo X Z, He Y, Zheng X L, et al. ZigFi: harnessing channel state information for cross-technology communication. IEEE/ACM Trans Netw, 2020, 28: 301–311
22 Wang W, He S Y, Sun L, et al. Cross-technology communications for heterogeneous IoT devices through artificial Doppler shifts. IEEE Trans Wirel Commun, 2019, 18: 796–806
23 Zhang X Y, Shin K G. Gap sense: lightweight coordination of heterogeneous wireless devices. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM'13), Turin, 2013. 3094–3101

24 Akyildiz I F, Lee W Y, Chowdhury K R. CRAHNs: cognitive radio ad HOC networks. Ad Hoc Netw, 2009, 7: 810–836
25 Akyildiz I F, Lee W Y, Vuran M C, et al. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Comput Netw, 2006, 50: 2127–2159
26 Devroye N, Mitran P, Tarokh V. Achievable rates in cognitive radio channels. IEEE Trans Inform Theory, 2006, 52: 1813–1827
27 Haykin S. Cognitive radio: brain-empowered wireless communications. IEEE J Sel Areas Commun, 2005, 23: 201–220
28 Liang Y C, Zeng Y H, Peh E C Y, et al. Sensing-throughput tradeoff for cognitive radio networks. IEEE Trans Wirel Commun, 2008, 7: 1326–1337
29 Stevenson C, Chouinard G, Lei Z D, et al. IEEE 802.22: the first cognitive radio wireless regional area network standard. IEEE Commun Mag, 2009, 47: 130–138
30 Duong T Q, Bao V N Q, Zepernick H J. Exact outage probability of cognitive AF relaying with underlay spectrum sharing. Electron Lett, 2011, 47: 1001–1002
31 Hong S S, Mehlman J, Katti S. Picasso: flexible RF and spectrum slicing. ACM SIGCOMM Comput Commun Rev, 2012, 42: 37–48
32 Luo L P, Zhang P, Zhang G C, et al. Outage performance for cognitive relay networks with underlay spectrum sharing. IEEE Commun Lett, 2011, 15: 710–712
33 Rayanchu S, Shrivastava V, Banerjee S, et al. FLUID: improving throughputs in enterprise wireless LANs through flexible channelization. IEEE Trans Mobile Comput, 2012, 11: 1455–1469
34 Yang L, Hou W, Cao L L, et al. Supporting demanding wireless applications with frequency-agile radios. In: Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI'10), 2010. 65–80
35 Halperin D, Anderson T, Wetherall D. Taking the sting out of carrier sense: interference cancellation for wireless LANs. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 2008. 339–350
36 Yi P Z, Iwayemi A, Zhou C. Developing ZigBee deployment guideline under WiFi interference for smart grid applications. IEEE Trans Smart Grid, 2011, 2: 110–120
37 Cavalcanti D, Das S, Wang J, et al. Cognitive radio based wireless sensor networks. In: Proceedings of the 17th International Conference on Computer Communications and Networks (ICCCN'08), St. Thomas, 2008
38 Huang J, Xing G L, Zhou G, et al. Beyond co-existence: exploiting Wi-Fi white space for ZigBee performance assurance. In: Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP'10), Kyoto, 2010. 305–314
39 Shi L X, Bahl P, Katabi D. Beyond sensing: multi-GHz realtime spectrum analytics. In: Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI'15), Oakland, 2015. 159–172
40 Yu R, Zhang Y, Gjessing S, et al. Cognitive radio based hierarchical communications infrastructure for smart grid. IEEE Netw, 2011, 25: 6–14
41 Zhou X, Zhang Z B, Wang G, et al. Practical conflict graphs for dynamic spectrum distribution. ACM Sigmetrics Perform Evaluation Rev, 2013, 41: 5–16
42 Yan Y B, Yang P L, Li X X, et al. ZIMO: building cross-technology mimo to harmonize ZigBee SMOG with WiFi flash without intervention. In: Proceedings of the 19th Annual International Conference on Mobile Computing and Networking, Miami, 2013. 465–476
43 Yan Y B, Yang P L, Li X Y, et al. WizBee: wise ZigBee coexistence via interference cancellation with single antenna. IEEE Trans Mobile Comput, 2014, 14: 2590–2603
44 Wang S, Yin Z M, Li Z J, et al. Networking support for physical-layer cross-technology communication. In: Proceedings of the 26th International Conference on Network Protocols (ICNP'18), Cambridge, 2018. 259–269
45 Wang W G, Zheng X L, He Y, et al. AdaComm: tracing channel dynamics for reliable cross-technology communication. In: Proceedings of the 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON'19), Boston, 2019
46 Chen G L, Dong W. Jamcloak: reactive jamming attack over cross-technology communication links. In: Proceedings of the 26th International Conference on Network Protocols (ICNP'18), Cambridge, 2018. 34–43
47 Zhang X N, Huang P, Guo L K, et al. Hide and seek: waveform emulation attack and defense in cross-technology communication. In: Proceedings of the 39th International Conference on Distributed Computing Systems (ICDCS'19), Dallas, 2019. 1117–1126

The key technologies of cross-technology communication

Dongjiang CAO[1], Shuai WANG[1*], Runqun XIONG[1], Yunhuai LIU[2], Junzhou LUO[1] & Tian HE[1*]

1. *School of Computer Science and Engineering, Southeast University, Nanjing* 211189*, China*;
2. *Center for Data Science, Peking University, Beijing* 100871*, China*
* Corresponding author. E-mail: shuaiwang@seu.edu.cn, tianhe@seu.edu.cn

Abstract With the development of the Internet of Things (IoT), a variety of wireless communication technologies have come up to meet the requirements of different applications in communication range, energy consumption, delay, and others. Because of the heterogeneity and communication barriers of different wireless communication technologies, heterogeneous devices can not communicate directly with each other. Due to the lack of information interaction, widely deployed heterogeneous IoT devices suffer from severe interference and the competition of spectrum resources. Moreover, the communication barriers between heterogeneous devices also limit information sharing and resource integration, and it needs extra overhead using the gateway to realize the communication between heterogeneous devices. Therefore, the research on cross-technology communication is put forward. It does not need gateways as the intermediate device for protocol conversion, which provides direct communication and satisfies the requirement of communication between heterogeneous devices. This paper first systematically analyzes and surveys the research status of cross-technology communication. On this basis, the key technologies of cross-technology communication are proposed, including packet level, signal level, and symbol level. Then, the proposed technologies are demonstrated for the anti-interference coordination application in the field of the coexistence of heterogeneous IoT devices. Finally, the prospects for cross-technology communication are discussed and concluded.

Keywords Internet of Things, wireless network, cross-technology communication, wireless communication protocol, digital modulation

Dongjiang CAO received his B.S. degree from the School of Computer Science and Engineering, Southeast University, China, in 2020. He is a M.S. candidate at the School of Computer Science and Engineering, Southeast University. His research interests include Internet of Things and data science.

Shuai WANG received his Ph.D. from the Department of Computer Science and Engineering at the University of Minnesota in 2017. He received his B.S. and M.S. degrees from Huazhong University of Science and Technology, China. He is currently a professor at the School of Computer Science and Engineering in Southeast University. His research interests include Internet of Things, cyber physical systems, data science, and wireless networks and sensors.

Tian HE is currently a professor at the School of Computer Science and Engineering in Southeast University. He is the recipient of the NSF CAREER Award (2009), McKnight Land-Grant Chaired Professorship (2011), George W. Taylor Distinguished Research Award (2015), China NSF Outstanding Overseas Young Researcher I and II (2012 and 2016), and eight best paper awards in international conferences including MobiCom, SenSys and ICDCS. He has served a few general/program chair positions in international conferences and on many program committees and also has been an editorial board member for six international journals including ACM Transactions on Sensor Networks, IEEE Transactions on Computers, and IEEE/ACM Transactions on Networking. He is an ACM&IEEE Fellow. His research includes wireless networks, networked sensing systems, cyber-physical systems, real-time embedded systems, and distributed systems.

Junzhou LUO received a Ph.D. degree in computer networks from Southeast University, Nanjing, in 2000. Currently, he is a full professor at the School of Computer Science and Engineering in Southeast University, Nanjing, China. Professor Luo is a member of IEEE and ACM, as well as co-chair of the IEEE SMC Technical Committee on Computer Supported Cooperative Work in Design, and chair of ACM SIGCOMM China. His research interests include next-generation networks, protocol engineering, network security, cloud computing, and wireless LAN.