

第3章

物联网安全基础 ——网络层关键技术

网络层也被称作数据传输层,位于感知层与应用层之间,负责将感知层采集的信息数据传输到应用层,并将应用层的控制信息等传递到感知层。物联网的网络层不限于计算机网络体系结构中 IP 所处的网络层协议栈。针对特定的接入、组网需要以及兼顾感知层硬件与应用层软件平台的需求,物联网的网络层发展出独特的技术与协议。本章分别就物联网的网络构建(接入和组网)及其相关技术和面向物联网应用的消息协议两方面,结合具体的技术、协议及其特点与这些技术、协议在物联网体系结构中的具体应用场景,对物联网网络层关键技术进行阐述。

3.1

物联网网络层概述

在物联网中,网络层也被称作数据传输层,位于感知层与应用层之间,负责将感知层采集的数据传输到应用层,并将应用层的控制信息等传递到感知层。具体而言,网络层承担了感知层设备和应用层系统间的寻址和路由选择,同时还具有连接的建立、保持以及终止等功能。

尽管都叫作网络层,物联网体系结构中的网络层与计算机网络体系结构中的网络层有所不同。在计算机网络体系结构的 TCP/IP 五层模型中,计算机网络各层的协议自顶向下被分为应用层、传输层、网络层、数据链路层和物理层。其中,应用层负责向网络应用程序交付它们能够接收的协议,常见的应用层协议包括超文本传输协议(HyperText Transfer Protocol, HTTP);传输层负责在应用程序端点之间传输应用层报文,主要包括传输控制协议(Transmission Control Protocol, TCP)和用户数据报协议(User Datagram Protocol, UDP);网络层负责将数据报(datagram)从一台主机移动到另一台主机,主要协议是网际互联协议(Internet Protocol, IP);数据链路层通过源和目的地之间的一系列路由器对数据报进行路由,主要协议包括以太网(Ethernet)协议等;物理层负责将整个帧从一个网络元素移动到邻近的网络元素,例如关于双绞线、同轴电缆、光纤等物理元素的协议^[36]。

物联网的网络层则不限于计算机网络体系结构中 IP 所处的网络层协议栈。实际上,物联网的网络层是建立在整个传统计算机网络体系结构之上的。针对特定的接入、组网

以及兼顾感知层硬件与应用层软件平台的需求,物联网的网络层发展出独特的技术与协议,如图 3-1 所示。

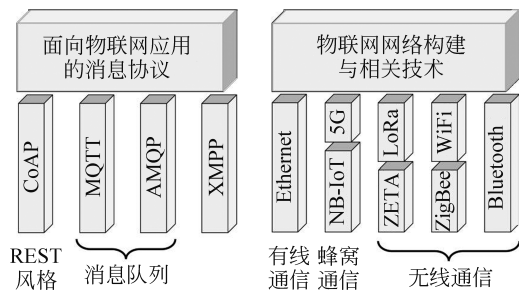


图 3-1 物联网网络层关键技术

本章分别就物联网的网络构建(接入和组网)及其相关技术和面向物联网应用的消息协议两方面,结合具体的技术、协议及其特点与这些技术、协议在物联网体系结构中的具体应用场景,对物联网的网络层关键技术进行阐释。对于传统计算机网络体系结构中涉及的 TCP/IP 协议栈,本章则不着重进行介绍。

3.2

物联网的网络构建与相关技术

物联网网络构建涉及物联网系统中设备间的组网技术与设备接入物联网局域网或接入互联网(Internet)的技术。这些技术依照通信方式可以分为有线通信、远距离蜂窝通信、远距离非蜂窝通信以及近距离通信。这些技术的标准通常对应于计算机网络中的物理层和数据链路层。

不同的通信技术涉及不同的网络协议与技术。常见的有线通信协议及技术包括以太网、通用串行总线(Universal Serial Bus,USB)、仪表总线技术(Meter Bus,MBus)等,常见的远距离蜂窝通信协议及技术包括第三代、第四代、第五代移动(3rd/4th/5th-Generation,3G/4G/5G)通信技术以及窄带物联网技术(Narrow Band Internet of Things,NB-IoT),常见的远距离非蜂窝通信协议及技术包括远距离无线电技术(Long Range Radio,LoRa)和 ZETA 协议族,常见的近距离通信协议及技术包括紫蜂协议(ZigBee)、无线保真(WiFi)技术、蓝牙(Bluetooth)与蓝牙低功耗(Bluetooth Low Energy,BLE)。

根据应用场景的不同,物联网系统所采用的通信技术及协议的不同,其组网方式也有所不同。对于依靠远距离蜂窝通信或有线通信的物联网系统,其设计与开发者不需要过多考虑系统的组网方法,或可以直接参照计算机网络的组网方法;对于通过网关接入互联网的设备,物联网系统的设计与开发者则需要依据设备及网关采用的协议构建无线传感器网络,再将其接入互联网。

3.2.1 5G

5G 指第五代移动通信技术(5th Generation Mobile Communication Technology),其

标准化计划由国际电信联盟(International Telecommunication Union,ITU)于2015年6月提出。

与4G网络不同,在5G蜂窝网络中,基站的功能被重构为两个功能单元:集中单元(Centralized Unit,CU)和分布单元(Distributed Unit,DU),如图3-2所示。其中,DU主要完成物理层功能,满足实时性需求;CU主要处理非实时的无线高层协议栈,同时也支持部分核心网功能下沉以及边缘应用业务的部署。

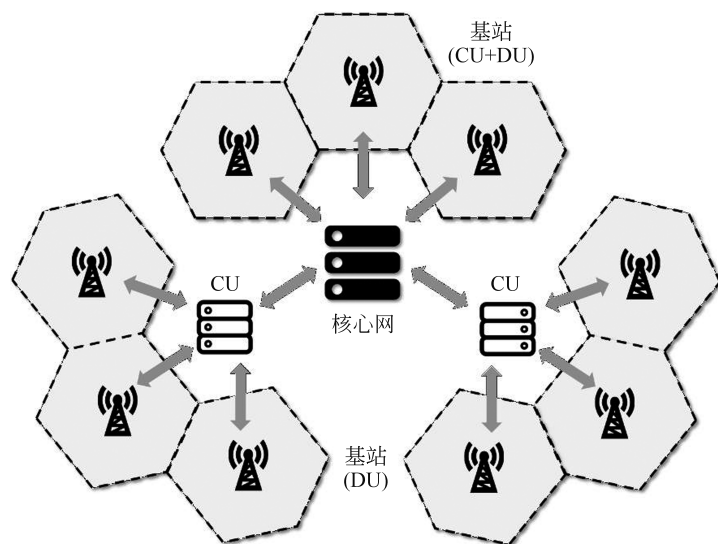


图 3-2 5G 蜂窝网络

5G 技术在提出时的目标是服务于以下 3 个场景：

(1) **增强型移动宽带**(enhanced Mobile BroadBand,eMBB)。提供更高的体验速率和更大的带宽接入能力,支持解析度更高、体验更鲜活的多媒体内容,下行峰值速率可达10Gb/s。

(2) **高可靠和低时延通信**(ultra-Reliable and Low Latency Communication,uRLLC)。提供高可靠、低时延信息交互能力,支持互联实体高度实时、高度精密和高度安全的业务协作,空口时延低于1ms,误码率低至 10^{-5} 量级。

(3) **海量机器类型通信**(massive Machine Type Communication,mMTC)。提供更高连接密度时优化的信息控制能力,支持多类型、高数量级物联网设备的连接,连接密度可达 $10^6/\text{km}^2$ 。

截至2021年,3GPP(3rd Generation Partnership Project,第三代合作伙伴计划)组织已经发布了Rel-15、Rel-16和Rel-17共3个版本的5G标准。其中,Rel-15和Rel-16已经被冻结,而Rel-17标准于2022年6月被正式冻结。此外,Rel-18标准已经于2021年年底完成立项。

Rel-15是5G的第一个标准,主要由LTE增强(LTE-Advance,LTE-A)、5G新无线(5G New Radio,5G NR)标准、5G核心网(5G Core Network,5GC)3部分组成。

LTE-A瞄准eMBB、uRLLC和mMTC三大场景进行功能扩展。针对eMBB场景,

LTE-A 支持 1024QAM 调制解调、增强型协同多点 (Coordinated Multiple Points, CoMP) 传输、8 天线波束赋形技术以及各种干扰抑制技术等; 针对 uRLLC 场景, LTE-A 优化了物理控制格式指示信道 (Physical Control Format Indicator Channel, PCFICH) 和短传输时间间隔 (Short Transmission Time Interval, Short TTI); 针对 mMTC 场景, LTE-A 在无人机终端检测/干扰检测方面和车联网 (Vehicle to Everything, V2X) 方面提出了新的要求, 对 LTE-M 和 NB-IoT 功能进行了增强。

5G NR 标准主要规范了 eMBB 和 uRLLC 两个场景。针对 eMBB 场景, 5G NR 定义了 3 类关键技术:

(1) 高频/超宽带传输。指定了两个频段范围, 分别是 FR1 (450MHz~6GHz, 单载波带宽为 100MHz) 和 FR2 (24.25~52.6GHz, 单载波带宽为 400MHz)。载波聚合 (Carrier Aggregation, CA) 和双连接技术, 可聚合 16 个载波, 以实现高速传输。

(2) 大规模多入多出 (massive Multiple Input Multiple Output, mMIMO)。采用数字和模拟混合波束赋形等技术, 在基站和终端支持更多天线单元, 从而在高频段实现大规模高速数据传输。

(3) 灵活的帧结构/物理信道结构。支持多个子载波间隔, 在频域上子载波间隔可以更宽, 在时域上 OFDM (Orthogonal Frequency Division Multiplexing, 正交频分复用) 符号可以更短, 以实现低时延传输; 还可灵活改变控制和数据信道的分配单元中的 OFDM 符号数量, 并可根据上下行业务比率灵活改变帧结构中的上下行时隙比。

针对 uRLLC 场景, 5G NR 采用宽子载波间隔并减少 OFDM 符号数量以降低时延, 定义了新的信道质量指示 (Channel Quality Indication, CQI) 和调制与编码策略 (Modulation and Coding Scheme, MCS) 标准以提升可靠性。

5G 核心网包含非独立组网 (Non-Standalone, NSA) 和独立组网 (Standalone, SA) 两种。NSA 采用双连接方法, 5G NR 的控制面锚定于 4G, 建立在 4G 核心网 EPC 上; SA 采用新建的 5G 核心网, 不依赖 4G。NSA 采用的 EPC 扩展方案, 相较于 4G EPC, 添加了 5G NR 的服务识别与控制功能。SA 采用的全新 5GC 设计则与 EPC 完全不同, 基于服务化、软件化结构, 通过网络切片、控制面/用户面分离等技术, 使网络定制化、开放化和服务化。

5G Rel-15 是 5G 的第一个标准, 内容上继承了 4G 技术。而 5G Rel-16 标准侧重于强化 uRLLC 场景功能, 在垂直领域进行了极大扩充 (可以看作在 mMTC 场景的扩展), 从工业互联网到车联网等, 拥有了更广泛的应用场景, 可进一步支撑物联网丰富的应用场景。Rel-16 标准中 5G 的垂直领域技术与应用如表 3-1 所示。

表 3-1 Rel-16 标准中 5G 的垂直领域技术与应用

技术	介 绍	应用场景
5G+TSN	时间敏感网络 (Time-Sensitive Networking, TSN) 指基于以太网架构的一套音频/视频传输标准, 对于实时性、时延、鲁棒性和资源管理有较高的需求。5G 的 uRLLC 需求与 TSN 有很高的契合度	工业互联网, 如工厂自动化、电网配电自动化等

续表

技术	介 绍	应用场景
NPN	非公共网络(Non-Public Network,NPN)指基于 5G 系统架构的专用网络。NPN 可分为非独立部署和独立部署两个模式。在非独立部署模式下,使用方基于 5G 切片与运营商共享 RAN、核心网控制面或端到端 5G 公网;在独立部署模式下,使用方自主部署从基站到核心网再到云平台的整个 5G 网络系统,可以在保证数据不泄露的情况下享受 5G 的低时延和高可靠性	有一定安全需求的企业与工业园区等
5G NR-U	工作于非授权频谱的 5G NR(5G NR in Unlicensed Spectrum,5G NR-U)指各个行业可以使用非授权的 5G 频段接入 5G 网络。类似于 NPN,5G NR-U 也包括两种模式:授权辅助接入(Licensed-Assisted Access,LAA)和独立组网(Stand alone,SA)。前者需要依赖于运营商的授权频谱,配合未授权频谱提升运营商网络容量和性能;后者不依赖于授权频谱,建立独立的 5G 专用网	商场、园区等 5G 网络;企业网络与工业互联网等各个垂直领域
5G LAN	5G 局域网支持在一组接入终端间构建二层转发网络,实现了终端组内数据交换和用户面路径选择。5G LAN 提供了组管理服务,使第三方可以创建、更新和删除组,以及处理网络中的 5G 虚拟网络配置数据和组成员终端的配置	构建公司局域网及虚拟专用网络;工业互联网等领域
5G V2X	V2X 实际上包括车与云端(Vehicle to Network,V2N)、车与车(Vehicle to Vehicle,V2V)、车与道路基础设施(Vehicle to Infrastructure,V2I)以及车与行人(Vehicle to Pedestrian,V2P)的连接。V2X 消息可以在基站和设备之间传输,也可以实现设备之间的直接通信。5G NR 可以支持更低的时延、更高的可靠性、更大的容量以提供更高级的 V2X 服务	车联网领域,将车与车、车与人、车与道路基础设施连接成网
5G NR 定位	利用 MIMO 多波束特性,定义了基于蜂窝小区的信号往返时间(Round Trip Time,RTT)、信号到达时间差(Time Difference of Arrival,TDOA)、到达角(Angle of Arrival,AoA)测量法、离开角(Angle of Departure,AoD)测量法等室内定位技术	工业自动引导车(Automated Guided Vehicle,AGV)、资产追踪等需要室内精准定位的场景

2022 年 3 月 5G Rel-17 标准进行了功能性冻结,该标准不仅在工作频率、载波聚合上进一步增强了 Rel-16,而且在 NB-IoT/eMTC 增强、扩展现实(Extended Reality,XR)领域拓展以及进一步的功耗降低等方面进行了优化。

(1) NB-IoT/eMTC 增强。研究 5G 及 NB-IoT/eMTC 的非地面通信(对空或对海)方案以应用于无人机、飞机、船只的通信。

(2) XR 领域拓展。XR 领域包括虚拟现实(Virtual Reality,VR)和增强现实(Augmented Reality,AR)。例如,5G 的高带宽、低时延特性可以帮助 VR 设备将图形运算功能分离到云端,从而使 VR 设备更加轻便。

(3) 进一步的功耗降低。将用户设备的天线数减半、删去不需要的 5G 技术等。此外,增加了无线资源控制(Radio Resource Control,RRC)的 Inactive 状态以支持小数据传输。

而根据已立项的 Rel-18 标准项目,Rel-18 会进一步改善网络切片接入功能;在工业互联网方面增强授时功能以保证时间同步,加强低功耗高精度定位功能;继续完善 V2X 的车载网络功能。同时,Rel-18 将继续拓展 5G 的垂直领域,智能铁路、智能电网以及智能家庭也将被囊括进来。Rel-18 的另一方向则是以在 5G 中传输 AI/ML 模型为目标,研究模型的流量特性与传输的性能需求。

5G 标准技术更新内容总结如表 3-2 所示。

表 3-2 5G 标准技术更新内容总结

标准版本	技术更新		
	增强型移动带宽	高可靠和低时延通信	海量机器类型通信
Rel-15	5G NR 的提出 - 高频高带宽通信 - mMIMO 技术 - 灵活的帧结构/物理通道结构	- 时隙 OFDM 符号数减少 - 全新 CQI 和 MCS 的定义	- V2X - 无人机终端检测 - eMTC/NB-IoT
Rel-16	- MIMO 增强 - 双连接/载波聚合增强 - IAB/移动性增强	- PDCCH 监视 - 多个 HARQ-ACK 支持无序 PUSCH 调度	- 工业物联网方向增强 (5G + TSN、5G NR 定位等) - V2X 完善
Rel-17	- 功耗降低 - 频率拓宽 - 载波聚合进一步增强	工业互联网可靠性提升	- XR 领域增强 - 空天地一体化建设
Rel-18	网络切片增强	垂直领域 uRLLC 增强	- 智能铁路 - 智能电网 - 智能家庭

3.2.2 NB-IoT

窄带物联网技术(NB-IoT)是 GSM/EDGE 无线接入网络(GSM/EDGE Radio Access Network,GERAN)工作组于 2015 年在 TR45.820 报告中提出的非后向兼容传统 GSM 系统的蜂窝物联网方案,可以在 200kHz 系统上支持窄带物联网技术。在 3GPP 的 RAN#70 会议上,NB-IoT 最终被确定为下行采用基于 15kHz 子载波间隔的 OFDMA (Orthogonal Frequency Division Multiple Access,正交频分多址接入)技术,上行采用 SC-FDMA (Single-Carrier Frequency Division Multiple Access,单载波频分多址接入)技术。

NB-IoT 网络由 NB-IoT 终端、基站和物联网核心网三部分组成。如图 3-3 所示,物联网核心网支持两种数据传输方案,用户面 EPS 优化(User Plane EPS Optimization)和控制面 EPS 优化(Control Plane EPS Optimization)。

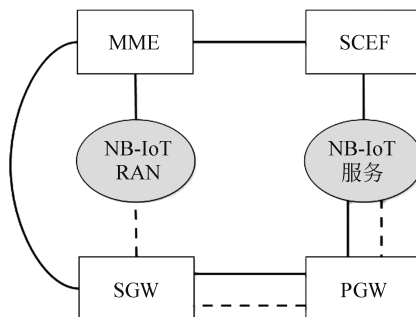


图 3-3 物联网核心网网络框架

物联网核心网网络框架如图 3-3 所示。其中,实线标识的为控制面 EPS 优化方案,虚线标识的为用户面 EPS 优化方案。MME 为移动管理实体(Mobile Management Entity),负责接入控制、移动管理等工作;SGW 为服务网关(Service Gateway),负责在 MME 的控制下进行数据包的路由和转发;PGW 为 PDN 网关(PDN Gateway),负责会话管理和承载控制、数据转发、IP 地址分配等工作。

在控制面 EPS 优化方案中,上行数据会从物联网接入网传输至 MME。而后,数据可通过 SGW 和 PGW 转发到物联网应用服务上,也可通过 SCEF 发送到物联网服务。下行数据传输路径与上行数据对应。其中,SCEF 传输方法是专门为 NB-IoT 而设计的,它仅支持非 IP 传输,可以将核心网的网元能力开放给各类业务应用,通过协议封装及转换实现与合作/自有平台对接,使网络具备多样化的运营服务能力。由于无须建立数据无线承载,控制面 EPS 优化方案适合非频发小数据包传输。

在用户面 EPS 优化方案中,上行数据会通过 SGW 和 PGW 发送给物联网应用服务。用户面 EPS 优化方案与传统数据流量传输相同,在无线载波上发送数据,支持 IP 和非 IP 数据包。尽管该方案在建立连接时会产生额外开销,但数据包序列传输更快。

由于不同场景对于设备实时性要求不同,NB-IoT 支持以下 3 种工作模式,以不同程度地降低功耗。

(1) 不连续接收(Discontinuous Reception, DRX)。在 DRX 模式下,NB-IoT 模块会在每一个 DRX 周期(通常为 1.28s 或 2.56s)监听一次寻呼信道,接收下行数据。DRX 模式的功耗比 eDRX 模式和省电模式高,适用于对实时性有一定要求的场景,例如共享单车的车锁及其他智能门锁。

(2) 扩展不连续接收(extended DRX, eDRX)。在 eDRX 模式下,模块会在每一个 eDRX 周期(通常为 20.48s 或 81.92s,最长可达 2.92h)内打开接收机,持续几个 DRX 工作循环再关闭。此外,eDRX 还支持周期动态调整,例如,NB-IoT 应用在跟踪宠物场景时,通常 NB-IoT 模块只需要每 2621~5242s 响应一次服务器的数据采集请求;但当宠物走失时,它可能需要将周期缩短到 20.48s。

(3) 省电模式(Power Save Mode, PSM)。在 NB-IoT 模块空闲一段时间后,会进入省电模式,此时,NB-IoT 模块关闭全部信号收发功能和接入层收发功能,仅保留注册状态存在于网络中。当 NB-IoT 模块需要发送数据时,不需要重新连接,只需要开启相关功能即可。处于省电模式的 NB-IoT 模块开启接收机的频率可能低至几天一次,因此功耗极低,仅为微安级。

NB-IoT 的 3 种工作模式对比如表 3-3 所示。

表 3-3 NB-IoT 的 3 种工作模式对比

模式	原 理	功耗	时延	适用场景
DRX	每个 DRX 周期监听一次寻呼信道,接收下行数据	较低	中等	共享单车车锁、智能门锁等
eDRX	每个 eDRX 周期打开一次接收机,持续几个 DRX 工作循环再关闭	低	高	宠物跟踪、物流监控、抄表等

续表

模式	原 理	功耗	时延	适用场景
PSM	关闭全部收发功能,在需要发送时开启相应功能。 打开接收机的频率低至几天一次	非常低	很高	远程煤气表、远程 水表、远程电表等

与其他远距离蜂窝技术相同,NB-IoT 由网络运营商代为构建网络。但与之不同的是,NB-IoT 的设计侧重于广覆盖、多连接、低模块成本、低功耗等方面。尽管 NB-IoT 在这些方面远胜于 4G 技术,然而其时延、传输速率以及移动性能等方面均远逊于 4G 技术。目前,NB-IoT 常被应用于上行数据需求量小、周期长(以小时、天计)的智能公用事业(如煤气表、水表、电表等)、智能农业、智能环境等领域^[37-38]。

3.2.3 LoRa

LoRa(远距离无线电)是由 Semtech 公司创建的低功率广域网(Low-Power Wide-Area Network,LPWAN)无线标准。LoRa 具有远覆盖距离、低功耗、低成本、支持多节点的特性。同时,LoRa 工作频段也较低,为 15MHz~1GHz,传输速率很低,通常低于 100kb/s。

LoRa 的组网有两个标准:LoRa 广域网(LoRaWAN)和 LoRa 无线网格网络(LoRaMESH)。在 LoRaWAN 标准中,组网方式为最常见的星状网。如图 3-4 所示,在 LoRaWAN 下,网络以 LoRa 网关为中心节点,其他终端设备则为终端节点,与中心节点相连。

在组网时,需要配置 LoRa 协议的传输速率、工作频率等参数,以保证终端设备和 LoRa 网关一致。通常,LoRa 网关支持节点主动上报和轮询唤醒两种接入模式。在节点主动上报模式下,终端设备会主动向 LoRa 网关发送数据,与 LoRa 网关进行配对;而在轮询唤醒模式下,LoRa 网关会根据上层指令发送消息,唤醒无法主动发送消息的终端设备,当需要唤醒的终端设备较多时,轮询周期较长,会导致较高的时延。

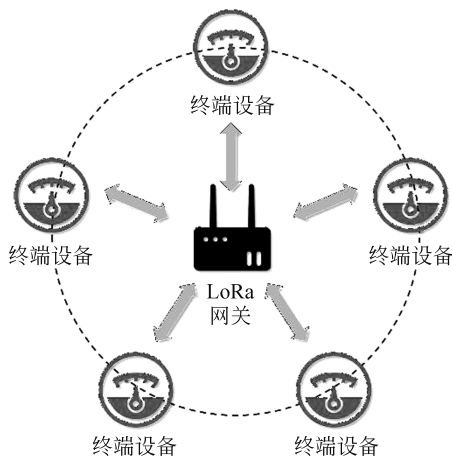


图 3-4 LoRaWAN 组网

星状网的 LoRaWAN 标准具有网络拓扑简单、稳定性高的优点,但在网络覆盖距离较大的情况下,星状网可能出现远端节点连接不稳定或无法连接的情况。此外,星状网使 LoRa 网关的负担较大,当终端节点很多时,由于同一时刻 LoRa 网关仅能处理一个节点发送的数据,网络可能会发生数据丢失^[39]。

为了处理更复杂的场景,提升连接距离,增强扩展性,LoRaMESH 应运而生。如图 3-5 所示,在 LoRaMESH 网络中,骨干网络取代了 LoRaWAN 中的中心节点。骨干网络由 LoRa 网关和 LoRa 路由器组成。LoRa 网关负责数据的处理与接入互联网;而

LoRa 路由器作为终端设备接入的中继,可以极大地延长传输距离,通过算法均衡网络传输,提升稳定性。

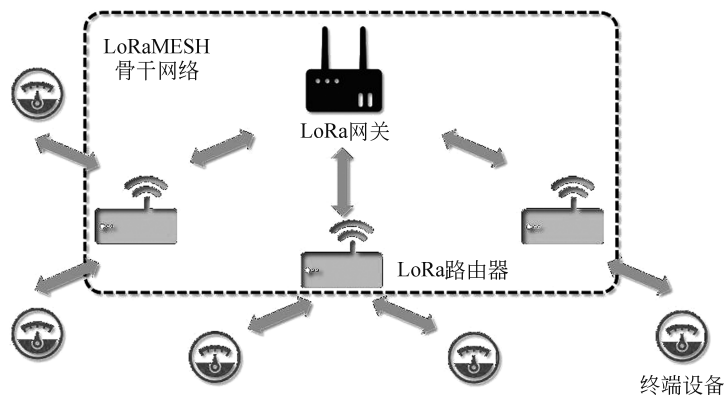


图 3-5 LoRaMESH 组网

LoRa 协议为了保证传输距离,采用了低频率的工作频段,配合扩频通信 (Spread Spectrum Communication, SSC) 技术提升抗干扰性能,增强隐蔽性,使用前向纠错 (Forward Error Correction, FEC) 编码技术提升可靠性。由于使用高扩展系数获得了信号增益,传输可靠性高,LoRa 协议不需要高发射功率,功耗也自然降低了。

扩频通信技术是 LoRa 协议的核心。通俗地说,扩频对信号带宽进行了扩展,降低了对于信噪比的需求。例如,传输数据流的基带带宽可能仅有 64kHz,即 64kb/s,通过扩频技术,传输信号的带宽被扩展到 5MHz 甚至更高。一方面,根据香农对信道容量的定义,在信号传输速率一定时,可通过提升带宽的方式降低对信噪比的要求;另一方面,扩频化码后的信道可以被同时分配给多个用户,从而提高利用率^[40]。

前向纠错编码技术指通过在待传数据序列中添加冗余信息的方式在接收端纠正传输过程中产生的错误码元,这也是 LoRa 协议中使用的一种通过牺牲传输速率提升可靠性的技术。

总的来说,LoRa 通信采用较低频段的信号,进一步通过 SSC 和 FEC 等技术以牺牲传输速率为代价提升可靠性,提升信号增益以降低功耗,因此保证了 LoRa 协议传输距离长、功耗低、成本低、终端设备寿命长等优点。

作为 LPWAN 技术的一种,LoRa 与 NB-IoT 的应用场景类似,以智能抄表为主。例如,在智能停车场中,可以在每个车位上部署 LoRa 通信的传感器,通过一个 LoRa 网关即可管理 1km 范围内的多个车位^[41];在智能农业场景,温度、湿度等数据也可以通过 LoRa 协议上传,低功耗、使用寿命长的 LoRa 传感器可以大幅降低成本。由于 LoRa 不需要第三方运营商运营,相较于 NB-IoT,使用者无须交付费用给运营商,使用成本更低,可以更好地满足隐私性需求。

3.2.4 ZETA

ZETA 是由我国厦门纵行科技信息技术有限公司自主研发的 LPWAN 技术产品^[42]。ZETA 是全球首个支持分布式组网、为嵌入式端智能提供算法升级的 LPWAN 通信

标准。

ZETA 在传统 LPWAN 的穿透性能基础上,进一步通过分布式接入机制实现部署,并为 Edge AI(端智能)提供底层支持,具有超低功耗、超大连接、超低成本、超广覆盖、超安全性等优势。具体来说,ZETA 通信设备电池供电使用寿命可达 3~5 年,覆盖范围达到 3~15km。

ZETA 网络架构在支持典型的星状拓扑的同时也实现了树状 MESH 网络。此外,ZETA 还设计了 3 个协议以满足不同物联网场景需求:

- (1) ZETA-P。低时延增强,主要面向业务流量不大的局域网场景。
- (2) ZETA-S。时频复用,主要面向业务流量较大的城域网场景。
- (3) ZETA-G。协议精简,成本较低,主要面向对成本敏感且有较大连接数量的场景。

ZETA 网络由接入点(Access Point,AP)、智能路由(可选)、终端和 ZETA 服务器组成,其网络结构如图 3-6 所示。

(1) AP。ZETA 自组网汇聚点,主要负责 ZETA 网络数据采集、时钟同步、夏季设备管理以及数据回传至服务器,支持远程全量升级、配置等功能。

(2) 智能路由。低功耗 MESH 智能路由节点,可以有效增加单站覆盖范围,便捷补充信号盲区,防止数据拥塞。

(3) 终端。数据透明传输模块,负责外界传感器集成,可以实现低功耗双向通信。

(4) ZETA 服务器。负责管理 ZETA 网络,支持协议解析、远程升级等功能。

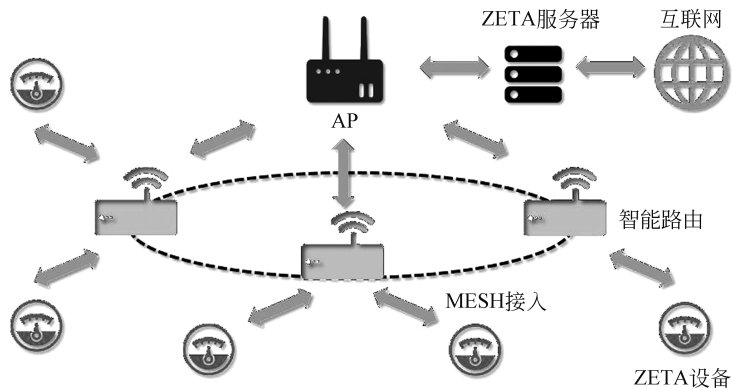


图 3-6 ZETA 网络结构

ZETA 的核心技术在于其独特的调制解调方法——Advanced M-FSK。它能够根据各种应用场景的不同速率要求进行自适应,结合了 Sigfox 协议窄带通信的优势,又具备 LoRa 协议的扩展性,配合 5G 技术可以在较小的带宽中达到较高的传输速率。

通常,M-FSK 技术的特点如下:

- (1) 调制信息只在相位上改变。在幅度不变时,峰值平均功率比(Peak to Average Power Ratio,PAPR)为 0,这意味着设备将保持低功耗特性。
- (2) 在发送功率不变时,带宽增加。
- (3) 保持符号相位连续,可以减少频谱泄漏。

Advanced M-FSK 对于 M-FSK 的参数进行了优化,使得发送信号更加简单,性能更优。同时,在接收方面,Advanced M-FSK 采用了更先进的接收技术,包括时频同步、数据解调和终端移动速度支持,提升了接收灵敏度。

作为对标 LoRa 的改良标准,ZETA 已经被应用于智能楼宇、智能物流、智能工业、智能农业以及智能城市等垂直领域中。其中,在智能物流方面,中国邮政在广西地区已经采用了可张贴在包裹信件上的 ZETag 云标签对贵重包裹进行全流程跟踪,全球首次在速递件上用物联网云标签实现实时轨迹跟踪服务。

3.2.5 蓝牙

蓝牙^[43]是一种无线通信技术标准,用来让固定设备与移动设备在短距离内交换数据,以形成个人局域网(Personal Area Network, PAN)。蓝牙使用短波特高频(Ultra High Frequency, UHF)无线电波,经由 2.4~2.485 GHz 的频段进行通信。蓝牙最早由爱立信公司于 1994 年提出,最初的设计是希望创建一个 RS-232 数据线的无线通信替代版本,能够连接多个设备,解决同步的问题。目前,蓝牙技术由蓝牙技术联盟(Bluetooth Special Interest Group, Bluetooth SIG)负责维护其技术标准。IEEE 曾经将蓝牙技术标准化为 IEEE 802.15.1,但目前已经不再继续使用。

截至目前,蓝牙已经经历了多个版本,如表 3-4 所示。蓝牙 5.0 于 2016 年 6 月发布,相较于上一个版本,极大地提升了传输距离和传输速度,支持室内定位导航功能,允许无须配对接收信标的数据,针对物联网进行了很多底层优化。

表 3-4 蓝牙版本

蓝 牙 版 本	发 布 时 间	最大传输速度	最大传输距离/m
蓝牙 1.0	1998	723.1kb/s	10
蓝牙 1.1	2002	810kb/s	
蓝牙 1.2	2003	1Mb/s	
蓝牙 2.0+EDR	2004	2.1Mb/s	10
蓝牙 2.1+EDR	2007	3Mb/s	
蓝牙 3.0+HS	2009	24Mb/s	10
蓝牙 4.0	2010	24Mb/s	50
蓝牙 4.1	2013		
蓝牙 4.2	2014		
蓝牙 5.0	2016	48Mb/s	300
蓝牙 5.1	2019		
蓝牙 5.2	2020		
蓝牙 5.3	2021		

注: EDR 是蓝牙 2.0 的增强数据速率(Enhanced Data Rate)技术,HS 是蓝牙 3.0 的高速(High Speed)技术。

此外,在蓝牙 4.0 版本中,蓝牙技术联盟还提出了蓝牙低功耗(Bluetooth Low Energy,BLE)协议。相较于蓝牙经典(Bluetooth Classic,BC)协议,BLE 协议的传输距离更短,空中传输速率更低,功耗更小,具体对比如表 3-5 所示。

表 3-5 蓝牙经典协议与蓝牙低功耗协议对比

对 比 项	蓝牙经典协议	蓝牙低功耗协议
频段	2.4GHz ISM 频段	2.4GHz ISM 频段
频道	79 个(间隔 1MHz)	40 个(间隔 2MHz)
数据传输速率	1~3Mb/s	125kb/s~2Mb/s
功耗	约 1W	约 0.05~0.5W
距离范围	100m	大于 100m

蓝牙协议按照各层所处位置,可以分为底层协议、中间层协议和顶层协议 3 类,如表 3-6 所示。其中,底层协议部分由射频协议、基带协议和链路管理协议组成,分别负责分配跳频信道、跳频与蓝牙数据和信息帧的传输以及连接、建立和拆除链路并进行安全控制;中间层协议完成数据帧的分解与重组、服务质量控制、组提取等功能,为顶层协议应用提供服务,并提供与底层协议的接口,包括主机控制接口协议、逻辑链路控制与适配协议、串口仿真协议、电话控制协议和服务发现协议;顶层协议包括对象交换协议、无线应用协议和音频协议。

表 3-6 蓝牙各层协议及作用

协议层	协 议 名	作 用
底层协议	射频协议	分配跳频信道(79 个,每个带宽为 1MHz)
	基带协议	负责跳频以及蓝牙数据和信息帧的传输
	链路管理协议	负责连接、建立和拆除链路并进行安全控制
中间层协议	主机控制接口协议	提供了统一访问蓝牙控制器的能力。主机控制器以 HCI 命令的形式提供了访问蓝牙硬件的不同模块的能力
	逻辑链路控制与适配协议	为高层提供面向连接和面向无连接的数据服务,实现协议复用、分段和重组、QoS 传输以及组抽象等功能
	串口仿真协议	供对 RS-232 串口的仿真,包括对数据信号线和非数据信号线的仿真。它既可以支持两个设备之间的多串口仿真,也可以支持多个设备之间的多串口仿真
	电话控制协议	支持电话功能(包括呼叫控制和分组管理),建立数据呼叫
	服务发现协议	用于动态地查询设备信息和服务类型,从而建立一条对应所需服务的通信信道
顶层协议	对象交换协议	用于红外数据链路上数据对象交换的会话层协议,不指定传输数据类型,只定义传输对象
	无线应用协议	由移动电话类的设备使用的无线网络定义的协议
	音频协议	用于传输音频并保证一定的音频质量

目前,蓝牙技术已经应用在上亿件产品中,遍布于车载网络、智能家居到医疗保健和计算机外设等领域。尤其是在可穿戴设备和计算机外设领域,蓝牙几乎独占了市场,例如蓝牙运动手环、蓝牙音箱、蓝牙耳机等。在短距离、点对点传输的场合,蓝牙具有明显优势。

3.2.6 ZigBee

ZigBee 也称紫蜂,是一种低速短距离传输的无线网络协议,底层是采用 IEEE 802.15.4 标准的媒体访问层与物理层^[44]。ZigBee 的主要特色有低速、低功耗、低成本、支持大量网络节点、支持多种网络拓扑、低复杂度、可靠、安全。

ZigBee 由 Honeywell 公司组成的 ZigBee 联盟(ZigBee Alliance)制定,从 1998 年开始发展,于 2001 年向电气与电子工程师协会(IEEE)提案,将其纳入 IEEE 802.15.4 标准,自此 ZigBee 技术渐渐成为各领域共同采用的低速短距离无线通信技术之一。

不同于大多数物联网网络协议,ZigBee 的协议栈除了 IEEE 802.15.4 规定的物理层和数据链路层,还包括网络层和应用层。尽管如此,ZigBee 仍然可以通过基于 IPv6 的低速无线个域网标准(IPv6 over IEEE 802.15.4,6LoWPAN)使用 IPv6 作为网络层协议接入传统的计算机网络。

下面介绍 ZigBee 协议物理层、数据链路层、网络层和应用层的协议栈。

(1) 物理层。IEEE 802.15.4 标准规定了 ZigBee 工作的频段、信道、速度以及数据单元的结构。物理层由物理层管理实体(Physical Layer Management Entity,PLME)提供两个服务:物理数据服务接入点(Physical Data SAP,PD-SAP)和物理层管理实体服务接入点(Physical Layer Management Entity SAP,PLME-SAP),主要为数据链路层的 MAC 子层提供服务,如数据的接口等。

(2) 数据链路层。数据链路层包含一个 MAC 层管理实体(MAC Layer Management Entity,MLME),负责维护和 MAC 子层相关的管理目标数据库。此外,MAC 子层还负责不同设备之间的无线数据链路的建立、维护、结束、确认的数据传输和接收。

(3) 网络层。ZigBee 的网络层称为 NWK 层(即网络层),主要负责网络的建立、网络地址分配、网络拓扑结构管理(星状、树状、网状)和网络路由管理。具体来说,NWK 层分为 NWK 层数据实体(NWK Layer Data Entity,NLDE)和 NWK 层管理实体(NWK Layer Management Entity,NLME)。其中,前者负责生成网络数据单元,指定路由拓扑和安全支持;后者负责配置新入网设备,建立新网络,管理设备加入和离开网络,以及邻居寻址和路由发现。

(4) 应用层。由应用支持子层(Application Support Sublayer,APS)、应用程序框架(Application Framework,AF)和 ZigBee 设备对象(ZigBee Device Object,ZDO)组成。APS 负责应用层和网络层之间的接口;AF 用于维持应用对象并进行数据收发;ZDO 为抽象化的网络端点,其功能是网络管理和维护,包括整个端点与网络的全部信息的查询。

ZigBee 与 LoRa 相同,在物理层采用了扩频技术,通过降低传输速率的方式提高了可靠性和传输距离,降低了功耗。ZigBee 的发射功率约为 1mW,且支持休眠模式,周期性进行侦听,进一步降低了功耗^[45]。

ZigBee 的另一个特点在于自身组网和路由的能力强。ZigBee 理论最大节点个数为 65 536,且任意节点之间均可进行通信。在有模块加入和撤出时,网络也可以快速自动修复^[46]。

ZigBee 协议由于功耗低、易于维护、可靠性高、覆盖范围较大,因此主要应用在自动抄表及工业控制领域。此外,鉴于其强大的自组网的能力,也被广泛应用于搭建无线传感器网络,可能涉及物流跟踪、建筑物监测、环境保护、医疗监护(传输病人的脉搏、血压等健康数据)^[47]及智能家居领域等。

3.2.7 WiFi

无线局域网(Wireless Local Area Network,WLAN)指应用无线通信技术将计算机设备互联构成的可以互相通信和实现资源共享的网络体系。WLAN 利用射频(Radio Frequency,RF)技术,使用电磁波在空中进行通信,以取代使用电缆的有线通信。WLAN 采用的最主要的标准是 IEEE 802.11,主要应用 WiFi 技术实现。

WiFi 也称无线热点或无线网络,是基于 IEEE 802.11 标准的一个 WLAN 技术,由无线以太网兼容性联盟(Wireless Ethernet Compatibility Alliance,WECA)推动制定^[48,49]。截至 2019 年,WiFi 已经公布了第 6 个版本。WiFi 版本如表 3-7 所示。

表 3-7 WiFi 版本

世 代	发 布 时 间	标 准	工 作 频 段	最高速率(半双工)
WiFi 1	1997 年	IEEE 802.11	2.4GHz	2Mb/s
WiFi 2	2000 年	IEEE 802.11b	2.4GHz	11Mb/s
WiFi 3	2003 年	IEEE 802.11a	2.4GHz	54Mb/s
		IEEE 802.11g	5GHz	
WiFi 4	2009 年	IEEE 802.11n	2.4GHz	600Mb/s
			5GHz	
WiFi 5	2013 年	IEEE 802.11ac	5GHz	6.9Gb/s
WiFi 6	2019 年	IEEE 802.11ax	2.4GHz	9.6Gb/s
			5GHz	

WiFi 相较于其他近距离无线通信技术,具有快速、高带宽的显著特点,通常支持 100~200m 的传输。WiFi 6 包括以下核心技术^[50]:

(1) OFDMA 频分复用技术。

WiFi 采用 OFDMA 数据传输模式,通过将子载波分配给不同用户并在 OFDM 系统中添加多址的方法实现多用户复用信道资源。其中,每个最小的子信道被称为资源单元(Resource Unit,RU),每个 RU 中至少包含 26 个子载波,用户是根据时频资源块 RU 区分出来的。如图 3-7 所示,信道的资源被分成一个个小的固定大小的时频资源块,即 RU,深色标出的则是某个用户在一定时间内占用的 RU。可见,用户的数据是承载在每一个

RU 上的。而从总的时频资源看,在每一个时间片有可能有多个用户同时发送;同时,在不同时间片上,同一用户占用的频率也可能是不同的。

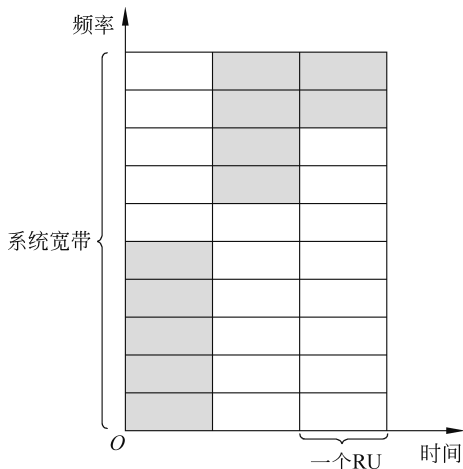


图 3-7 OFDMA 工作模式

相较于前 5 代 WiFi 使用的 OFDM 技术,OFDMA 具有以下优势:

- 更细的信道资源分配。在部分节点信道状态不太好的情况下,可以根据信道质量分配发送功率,更精细地分配信道时频资源。
- 提供更好的 QoS(Quality of Service,服务质量)。由于一个发送者只占据整个信道的部分资源,一次可以发送多个用户的数据,所以能够减少节点接入的时延。
- 更多的用户并发及更大的用户带宽。通过将整个信道资源划分成多个子载波(也可称为子信道),再将子载波按不同 RU 类型分成若干组,每个用户可以占用一组或多组 RU 以满足不同业务的带宽需求。

(2) DL/UL MU-MIMO 技术。

DL/UL MU-MIMO 分别指在数据下行链路(DownLink)和上行链路(UpLink)中采用多用户 MIMO(Multi-User MIMO,MU-MIMO)技术,可以提升信道容量和用户速率,适用于高带宽场景。

(3) 更高阶的调制技术(1024-QAM)。

WiFi 6 使用 1024-QAM 调制,在传输中,每个符号传输 10 位数据而非 256-QAM 的 8 位数据,使单条空间流数据吞吐量提升了 25%。1024-QAM 调制的应用取决于信道条件,更密的星座点距离需要更强大的 EVM(Error Vector Magnitude,误差向量幅度,用于量化无线电接收器或发射器在调制精度方面的性能)和接收灵敏度功能,并且对信道质量的要求高于其他调制类型。

(4) BSS 着色机制。

BSS 着色(BSS coloring)机制是一种同频传输识别机制。通过在物理层报文头中添加 BSS 着色字段对来自不同 BSS(Basic Service Set,基本服务集)的数据进行“染色”,为每个通道分配一种颜色,该颜色标识一组不应干扰的 BSS,接收端可以及早识别同频传输干扰信号并停止接收,避免浪费收发机时间。如果颜色相同,则认为是同一 BSS 内的干

扰信号,发送将推迟;如果颜色不同,则认为两者之间无干扰,两个 WiFi 设备可同信道同频并行传输。

(5) 扩展覆盖范围。

采用长 OFDM 符号发送机制,将每次数据发送持续时间从原来的 $3.2\mu\text{s}$ 提升到 $12.8\mu\text{s}$,可以降低终端丢包率。此外,WiFi 6 支持 2MHz 频宽的窄带传输,可以有效降低低频段噪声干扰,提升终端接收灵敏度,增加覆盖距离。

为了降低成本和功耗,WiFi 6 支持 2.4GHz 的频段以兼容老设备,增加覆盖范围。WiFi 6 提供了目标唤醒时间(Target Wakeup Time,TWT)功能调度资源,允许设备协商它们在何时或多久之后被唤醒、发送或接收数据、增加设备睡眠时间等,以降低功耗,提高电池寿命。

除了手机和计算机外,WiFi 目前已经广泛地应用于物联网系统中,尤其是家用的智能家居场景以及智能安防领域。例如,在智能安防领域中,通过 WiFi 协议通信的远程安保摄像头可以弥补有线传输的不足,降低网络的复杂度。随着 WiFi 6 的公布,WiFi 技术也能够适用于更高密度、更高带宽需求的场景,例如电子教室这样有上百位学生的大型授课场景,需要高密度、高数据量的上下行视频。

3.2.8 以太网

以太网是目前应用最普遍的计算机局域网技术,其技术标准由 IEEE 802.3 标准规定^[51,52],后者规定了包括物理层的连线、电子信号和介质访问层协议的内容。

目前,使用最广泛的是交换式以太网,这种网络使用交换机设备以连接不同的计算机,速率最高可以达到 10 000Mb/s(称为万兆以太网)。过去的经典以太网采用总线拓扑,如图 3-8 所示。而交换式以太网为了减少冲突、提高网络速度和最大化使用效率,使用交换机进行网络组织和连接,将以太网的拓扑结构改变为星状,如图 3-9 所示。而在逻辑层面上,以太网仍然采用总线拓扑和带冲突检测的载波监听多路访问(Carrier Sense Multiple Access/Collision Detection,CSMA/CD)的总线技术。

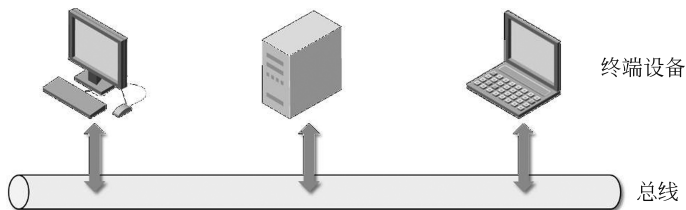


图 3-8 总线拓扑结构

CSMA/CD 是以太网的核心技术,它规定了多台计算机共享一个通道的方法。这项技术起源于 20 世纪 60 年代由夏威夷大学开发的 ALOHAnet,它使用无线电波作为载体。CSMA 协议要求站点在发送数据之前先监听信道。如果信道空闲,站点就可以发送数据;如果信道忙,则站点不能发送数据。但是,如果两个站点都检测到信道是空闲的,并且同时开始传送数据,那么这几乎会立即导致冲突。另外,站点在监听信道时,听到信道是空闲的,但这并不意味着信道真的空闲,因为其他站点的数据此时可能正在信道上传

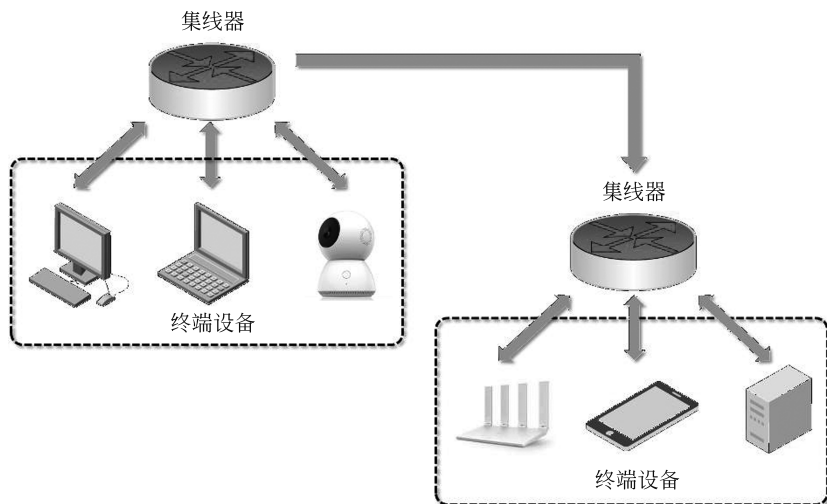


图 3-9 交换式以太网结构

送,但由于传播时延,信号还没有到达正在监听的站点,从而引起对信道状态的错误判断。CSMA/CD 则是对 CSMA 进一步的改进,使发送站点在传输过程中仍继续监听信道,以检测是否存在冲突。如果两个站点都在某一时间检测到信道是空闲的,并且同时开始传送数据,则它们几乎立刻就会检测到有冲突发生。如果发生冲突,信道上可以检测到超过发送站点本身发送的载波信号幅度的电磁波,由此判断出冲突的存在。一旦检测到冲突,发送站点就立即停止发送,并向总线上发送一串阻塞信号,用于通知总线上通信的对方站点快速地终止被破坏的帧,可以节省时间和带宽。

以太网具有协议全面、通用性强、成本低的优点,在计算机网络、视频监控方面有着广泛的应用。

3.3

面向物联网应用的消息协议

为了向物联网消息平台、移动应用程序等物联网应用层应用提供更标准化的消息传输服务,物联网系统的设计与开发者会根据应用场景的需要选择不同的消息协议。这些消息协议通常对应于计算机网络中的应用层,例如 HTTP 及表征性状态转移 (Representational State Transfer, REST) 架构就可以在物联网系统中作为消息协议使用。考虑到物联网系统需求的多样性,在设计模式、服务质量等方面具有不同特征的消息协议应运而生。

3.3.1 MQTT

消息队列遥测传输 (Message Queue Telemetry Transport, MQTT) 协议是由 IBM 公司开发的轻量级机器间通信 (Machine to Machine, M2M) 网络协议^[53]。MQTT 协议采用发布/订阅模式,所有的物联网终端通过 TCP 连接到 MQTT 代理,代理则通过主题管理各个设备关注的通信内容,负责转发设备之间的消息。图 3-10 和图 3-11 展示了

MQTT 系统订阅和发布的例子。其中,终端用户和房间内的两台空调订阅了同一主题后,该用户通过代理向两台空调设备发送命令。

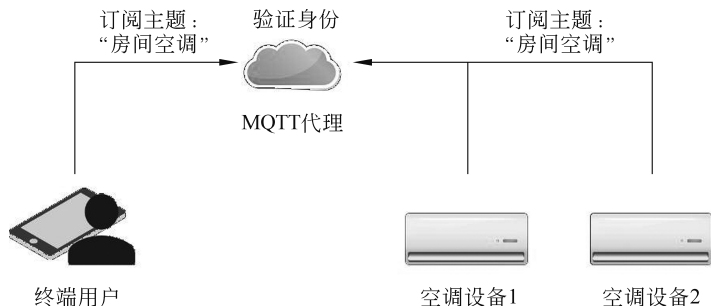


图 3-10 MQTT 系统订阅的例子

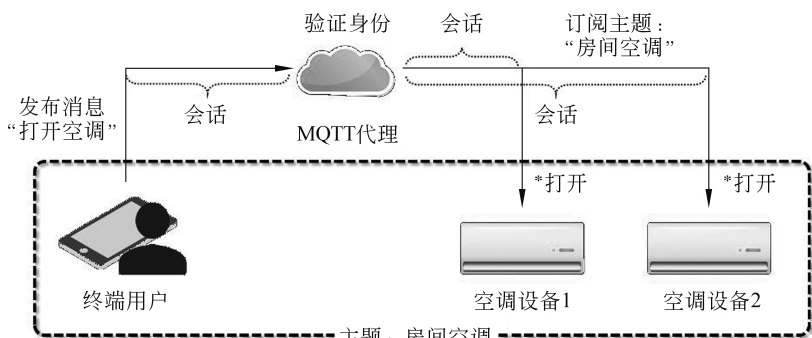


图 3-11 MQTT 系统发布的例子

如图 3-10 和图 3-11 所示的 MQTT 系统涉及了代理、客户机等不同实体以及消息、会话等概念。

(1) 代理(broker)。MQTT 代理是充当消息中介的服务器。通常代理部署在云端。除了管理主题和消息转发的功能外,不同平台在具体实现代理时还会配置一些扩展策略,包括触发规则、认证、访问控制等功能。例如,Eclipse 的 Mosquitto 消息代理工具可以通过 mosquitto_auth_plugin 开源插件实现客户访问主题的访问控制。

(2) 客户机(client)。即设备。客户机需要连接到代理,订阅同一主题后才能够进行消息交换。

(3) 身份(identity)。在 MQTT 系统中,每一台设备或终端由一个唯一的 ClientID 标识自身的身份。此外,一些平台及工具还支持通过用户名和口令、证书或者 JWT (JSON Web Token)等方式对身份进行认证。例如,阿里云的 MQTT 平台可以通过该平台提供的签名方式对设备的 ClientID 进行签名并以此对连接的客户机进行认证。

(4) 主题(topic)。主题定义了消息的内容或某一类消息的特征。在 MQTT 系统中,客户机根据订阅的主题收发消息。通过订阅特定的主题,客户机将接收任何该主题下其他客户机发布的消息。

(5) 消息(message)。MQTT 协议的消息由 3 部分组成:固定头、可变头和消息载荷。其中,固定头标识了数据包类型及数据包的分组类标识,其中,数据包的类型包括连

接(CONNECT)、连接确认(CONNACK)、订阅(SUBSCRIBE)、订阅确认(SUBACK)等;可变头由数据包类型决定,包括该类型消息的信息字段;消息载荷为消息的内容,包括MQTT PUBLISH 消息的发布内容等。

(6) 会话(session)。客户机与代理通过建立会话进行消息交换。每个会话都具有一个单独的 ID。

MQTT 协议主要在低带宽、不可靠的网络中提供基于云平台的远程设备的数据传输和监控,具有简单、轻量级、节省能源和带宽的特点。MQTT 最显著的优点在于它的路由机制支持一对一、一对多、多对多的发布,支持 3 种服务质量(QoS)以保证协议在不同网络条件下的适用性。

具体来说,在消息发布的 $QoS=0$ 时,发布方发送的 PUBLISH 消息会保证接收方至多收到一次,接收方在接收 PUBLISH 消息后不会回复,发送方也无法确定接收方是否收到了消息;在 $QoS=1$ 时,发布方发送的 PUBLISH 消息会保证接收方至少会收到一次,接收方在接收到消息后需要回复一条 PUBACK 消息;在 $QoS=2$ 时,发布方发送的 PUBLISH 消息会保证接收方收到且只收到一次,接收方在接收到 PUBLISH 消息后需要回复一条 PUBREC 消息,而发送方需要对这条消息再回复一条 PUBREL 消息,最后接收方以一条 PUBCOMP 消息结束这一发布过程。

在不同场景下,客户机可以选择以不同的 QoS 接收或发布消息:

(1) $QoS=0$ 。客户机和代理之间的网络连接较稳定(不容易产生消息丢失)或系统可以接受丢失部分消息。例如,一个需要以较短时间间隔发布状态信息的传感器,即使发生一次或两次消息丢失,对于系统也不会有明显影响。

(2) $QoS=1$ 。客户机需要接收所有消息,可以处理重复消息,但网络条件不支持 $QoS=2$ 带来的额外开销。

(3) $QoS=2$ 。必须保证客户机接收所有消息,且客户机不希望处理重复消息,对消息的即时性要求不高,网络条件可以支持 $QoS=2$ 带来的额外开销。

目前,应用最广泛的 MQTT 协议是 2014 年发布的 MQTT 3.1.1 和 2017 年发布的 MQTT 5,后者在前者的基础上增加了属性(property)的概念与更多的功能,包括共享订阅、丰富的原因码(reason code)显示等^[54]。

3.3.2 CoAP

受限制的应用协议(Constrained Application Protocol, CoAP)是互联网工程任务组(Internet Engineering Task Force, IETF)的受限制的 RESTful 环境工作组(Constrained RESTful Environment Work Group, CoRE Work Group)在 Web 的 REST 架构的基础上,满足在受限环境的低功耗与低开销而设计的 M2M 应用层协议,最早可以追溯到 2014 年的 RFC 7252,并在此基础上进行了扩展。

CoAP 针对 M2M 应用程序进行了优化并实现了 REST 的子集。因此,它既内置了包括资源发现、多播支持和异步消息交换在内的 M2M 功能,又具有 HTTP 的诸多特点,且可以实现无状态的 HTTP 映射(构建代理服务器,实现通过 HTTP 访问 CoAP 资源或在 CoAP 上实现 HTTP 接口)。

不同于 HTTP、MQTT 等建立在 TCP 连接上的应用层协议,CoAP 封装在 UDP 上传输,最小消息长度仅有 4 字节。由于 UDP 不具有 TCP 的可靠性机制,CoAP 定义了需要确认消息 CON、不需要确认消息 NON、确认应答消息 ACK 和复位消息 RST 这 4 种消息类型以支持对于不同服务质量的需求。当需要可靠的消息传输时,客户端可以选择发送 CON 消息并等待服务器返回的 ACK 消息以确定服务器确实收到了消息;而当不需要可靠的消息传输,即客户端不需要考虑消息是否被服务器收到时,客户端只需要发送 NON 消息即可。

由于参考了 HTTP 的请求/响应模式,CoAP 具有 GET、PUT、POST 和 DELETE 4 种请求方法,响应也按照响应码首位分为 2.XX、4.XX 和 5.XX。其中,GET、PUT、POST、DELETE 方法分别用于获取、更新、创建和删除某一资源。状态码则按照首位区分:2.XX 表示客户端请求被成功接收并处理;4.XX 表示客户端请求有错误,包括服务器拒绝请求(4.03)、请求包含错误选项(4.02)等;5.XX 表示服务器在执行客户端请求时出错,如服务器内部错误(5.00)、服务器过载或维护停机(5.03)等。

同时,类似于 HTTP,CoAP 也采用 URI(Uniform Resource Identifier,统一资源标识符)对某一资源进行定位,结合上述 4 种方法以实现对指定资源的增删改查。在如图 3-12 所示的场景中,温度计通过 PUT 请求更新温度资源的内容,用户则通过 GET 请求查询温度计测量的温度,而服务器分别用 2.04 Changed 响应和 2.05 Content 响应表明资源被修改了以及具体的查询结果内容。

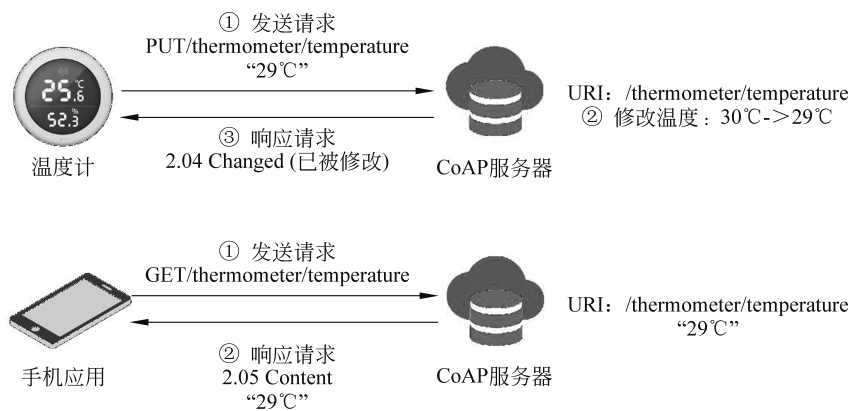


图 3-12 CoAP 请求/响应的场景示例

通常,请求采用 CON 或 NON 的消息类型进行传输;而响应则采用 CON、NON 类型或当 CON 类型的请求被快速处理完后以 ACK 类型的消息进行传输。具体来说,CoAP 消息模式可以分为携带模式、分离模式和非应答模式。在这 3 种模式下,完成一次请求/响应分别需要 1、2、1 次 RTT,具体过程如图 3-13 所示。

此外,CoAP 还通过选项(Option)字段标识代理、反向代理、资源路径等信息,类似于 HTTP 不同的头部(Header)。同时,CoAP 也支持服务发现、资源发现、多播等功能以适应更多的场景并提供更丰富的服务。由于 CoAP 支持的功能为 HTTP 的有限子集,因此可以通过一个正向代理很容易地实现这两个协议之间的映射。具体来说,包括以下两种情况: