第5章

网络连接层原理

连接物联设备需要多种技术，这些技术与传输数据量、传输距离及传输功率有关。此外，在更高的功能层可以选择多种方式对连接进行管理、防护和保护。本章简要介绍与连接设备有关的基本知识及其基本原理。如果读者从事过与网络相关的工作，可跳过本章内容。

5.1 网络基础知识

在计算机网络领域，开放式系统互连（Open Systems Interconnection，OSI）模型是一个概念模型，用于描述和规定电信系统或计算系统的通信功能，它与其依托的内部结构及技术无关，其目的是使用标准协议实现各种通信系统的互操作性。OSI模型把通信系统分为多个抽象层，在模型原始版本中，定义了7个功能层，如图5.1所示。

某一层服务其上方的一层，并由其下方的一层为它提供服务。例如，提供网络间无差错通信的层，需要其上方的应用提供所需的

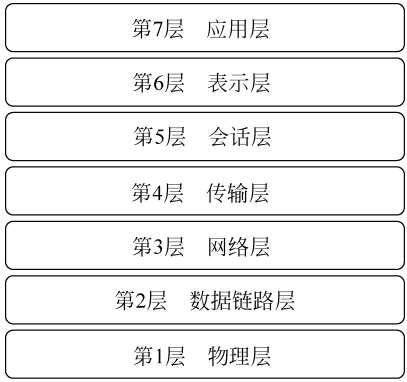

图 5.1　OSI 模型

路径，同时，它调用下一层发送和接收包含该路径内容的数据包。这个模型是理解从纯弱电层的连接一直到应用程序层的连接等不同连接方式的一个有效框架。

5.2　数据链路层

数据链路层提供节点到节点的数据传输，这是 2 个直接连接的节点之间的链路。它检测并能纠正物理层中出现的错误。它定义了用于在 2 个物理连接设备之间建立和终止一个连接的协议，并定义了它们之间数据流控制的协议。数据链路层负责控制网络中的设备如何获得对数据的访问和传输数据的权限，还负责识别和封装网络层协议，并控制差错校验和数据包同步。像以太网、Wi-Fi 和 ZigBee 等的连接技术都在数据链路层。

5.3　连接距离与功率

在物联设备无法与互联网物理连接的情况下(其原因与设备周边环境、地理位置或设备类型,如移动设备有关),则需要某种形式的无线技术。无线技术有多种选择：Wi-Fi、3G、4G、ZigBee、NFC、LoRaWAN、卫星通信等。如何选择取决于功耗、通信距离、数据通信速率、成本、天线尺寸及环境等几个基本原则。

图 5.2 给出了 4 种不同连接技术的连接距离和功耗之间的匹配关系。连接距离为 30～100m 的 Wi-Fi 需要的能量远远高于最大连接距离为 10m 的蓝牙和连接距离不到 0.1m 的 NFC。

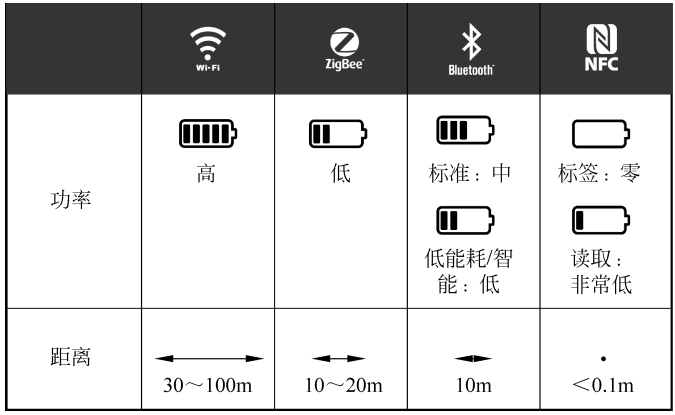

图 5.2　距离与功率

一般来说,无线信号以连接距离的平方为系数衰减,这意味着如果连接距离增加 1 倍,则需要增加 4 倍的功率,也就是需要容量

更大的电池。

一些应用程序可以在一个封闭的、专有的无线网络中运行。例如，麦克罗米特公司（McCrometer）的水位传感器使用 560～480MHz 的频段，这个频段已分配给此类通信。农场或供水地区可以从联邦通信委员会（FCC）购买部分该频段的占用许可，有效期为 10 年，覆盖半径为 32km。以这个频率通信，UHF（Ultra High Frequency）的连接距离可达到 1.6～19km，连接距离取决于所在地区的地形地貌。

5.4 连接距离与数据通信速率

另一种权衡是关于连接距离与通信速率的。通常，当通信频率上升时，可用带宽也会增加，但通信距离和越过障碍的能力会降低。与 900MHz 的装置相比，对于任意给定距离，2.4GHz 的装置约有 8.5dB 的额外路径损耗（3dB 是 50％的损耗）。

因此，通信频率越高，通信带宽容量越高，但需要更高的功率才能达到相同的通信连接距离；通信频率越低，带宽容量越低，但可实现较长距离的通信连接，如图 5.3 所示。然而，可惜的是，以较低的通信频率建立通信连接时，要获得相同的增益，则需要较大尺寸的天线，如图 5.4 所示。

环境对网络性能也有一定的影响，在阴雨天看卫星电视的人肯定知道这一点。通常，卫星电视的制造商会公布视线范围曲线。视线是指从天线 A 能看见天线 B，能看到天线 B 所在的建筑还不

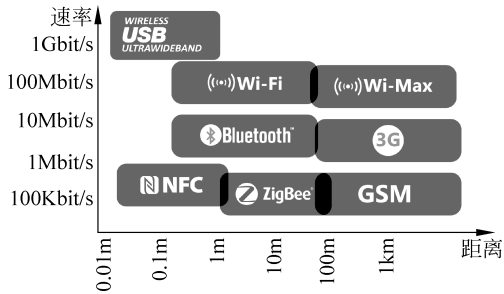

图 5.3　通信连接距离与数据通信速率

图 5.4　天线尺寸

够。对于在视线路径上的所有障碍物，会降低各个障碍物对应的视线曲线的等级，并且障碍物的形状、位置及个数都会对路径损耗产生影响。

5.5　应用层

物联网领域中最大的竞争领域之一也许是应用层，通过应用层人们可以很容易地把新设备连接到网络，同时把数据接入各种

数据采集体系，如图 5.5 所示。这些将在下一章讨论。无论是做咖啡壶的，还是制造发电机的，需要面对一些实施决策问题。有统计表明有 100 多家供应商从事此领域，有如此多的终端应用要解决，就平台而言有如此广泛的技术和数据需求，因此，参与其中商家的数量并不令人惊讶。参与其中的新公司有阿雷伦特公司（Arrayent）、艾拉网络公司（Ayla Networks）及爱普电气公司（Electric Imp），它们专注于低成本的消费产品，如热水器、邮件打戳器、洗衣机、车库开门器和可穿戴医疗设备。

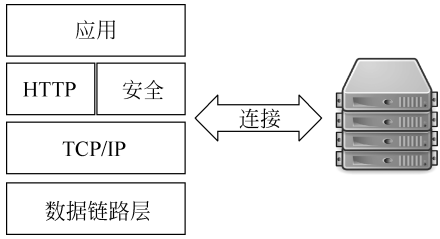

图 5.5　应用层

一些公司更关注纵向市场，如电力行业的银泉网络公司（Silver Spring Networks）。银泉公司提供 ZigBee 无线技术及更高层的连接协议。还有一些规模较小的参与者已经被规模较大的参与者收购，成为更大的物联网框架的一部分，如阿克塞达公司（Axeda）被 PTC 公司收购，2lemetry 公司被亚马逊公司收购。

此外，也有像阿帕雷奥公司（Appareo）那样较传统的供应商参与其中。阿帕雷奥公司为 AGCO 提供技术。阿帕雷奥公司还使其连接解决方案向下兼容，以支持旧的农业设备增加处理恶劣环境下数据的功能，这种环境远比家居环境恶劣得多。其中一些公司还把移动流量包打包成一揽子解决方案的一部分。ZTR 公司就是

一个很好的例子，它起步于列车控制领域。

5.6　网络安全

网络安全从身份验证开始，通常使用用户名和密码，被称为单因素身份验证。但随着人们对网络安全的日益重视，许多网络实行双因素身份验证，这种身份验证方式需要使用本人实际持有的物品。它可能是一个特殊用途的装置，或者就像经常看到的，可以是一部手机，它从应用程序接收编码来再次进行身份验证。

一旦通过身份验证，防火墙就执行访问策略，如网络用户可以访问哪些服务。防火墙根据一系列安全规则监测和控制流入和流出的网络流量。它们通常在一个可信的、安全的内部网络和一个外部网络（如互联网）之间建立一个屏障，这个外部网络被认为是不安全的或不可信的。

防火墙也越来越多地用于检查网络上传输的潜在有害内容，如计算机蠕虫（worms）病毒和特洛伊木马（Trojans）病毒。防病毒软件或入侵防护系统有助于检测和禁止此类不良软件的活动。另外，防火墙也记录网络流量，以便审查和以后的进一步分析。

在连接层，加密用于保护被传输的数据，因为在物理层上没有办法保护连接并防止攻击者看到传输的数据。加密靠的是发送者和接收者之间共享的一组密钥，假设在没有大量计算机资源的情况下，尝试每个密钥的暴力攻击都不会成功。虽然加密传输可以提供额外的安全性，但是目前密钥的访问控制变得与网络安全同

等重要。

随着风险因素的增加，越来越多的物联设备被接入网络并因此而公开，人们对网络安全的创新需求只会增加。目前，大多数已有的技术是针对 IoP 开发的。设备并非是人类，那么，为什么针对构建的集成访问管理（Integrated Access Management，IAM）应用程序能适用于物联网呢？像 Uniquid 公司那样的软件公司已在为物联网构建 IAM，没有人会期望牵引车、基因测序仪、铲车每 90 天更改一次密码（确保添加一个特殊字符）或回答安全问题。又比如，血液分析仪会选择什么样的检测模式作为它的常用模式呢？