第3章 无线局域网集成技术

本章学习目标

- 熟悉 Wi-Fi 标准、接入方式、关键技术和 Wi-Fi6；
- 熟悉 ZigBee 标准、协议框架和各层规范；
- 熟悉 5G 移动通信的应用场景、网络部署和新空口等相关技术；
- 熟悉 NB-IoT 和 LoRa 窄带物联网标准和技术；
- 熟悉无线移动局域网的安全技术。

无线网络正在从人和人连接，向人与物以及物与物的连接迈进，万物互联是必然的趋势。众多的网络互联场景层出不穷，各种技术不断涌现，从短距离无线技术到远距离无线技术，包括万众瞩目的 5G 移动通信都蓬勃发展。无线网络安全问题和技术也与时俱进。

3.1 概　　述

近年来，物联网、移动互联网、大数据和云计算迅猛发展，这逐步改变了社会的生产方式，大大提高了生产效率和社会生产力。根据不同的需求，产生了各种短距离和长距离无线通信技术。

短距离局域网无线通信技术代表有 Bluetooth（蓝牙）、Wi-Fi、NFC（Near-Field Communication，近场通信）、ZigBee、UWB（Ultra Wide Band，超宽带）。

远距离广域网无线通信技术包括 GSM、CDMA、LTE 等移动网络通信技术以及各种低功耗广域网（Low Power Wide Network，LPWAN）技术，典型代表有 NB-IoT 和 LoRa。

LPWAN 物联网技术又可以划分为非授权频段和授权频段技术。非授权频段物联网技术包括 LoRa、Sigfox 等。授权频段物联网技术包括 eMTC（Enhance Machine Type Communication）、NB-IoT 等。

4G 改变生活，5G 改变社会。全球的 5G 部署正在如火如荼地进行。华为、爱立信、诺基亚、中兴在全球 5G 市场上进行着激烈的角逐。

无线移动局域网的安全问题和技术也越来越重要，本章主要介绍了无线加密技术、认证技术以及典型安全协议。

本章主要介绍 Wi-Fi、ZigBee、5G、NB-IoT、LoRa 以及无线移动局域网的安全等技术。

3.2 Wi-Fi 技术

无线局域网(WLAN)是计算机与无线通信技术相结合的产物,它使用无线信道来接入网络,为通信的移动化、个人化和多媒体应用提供了潜在的手段,并成为宽带接入的有效手段之一。

3.2.1 Wi-Fi 概述

1. 无线局域网标准

(1) IEEE 802.11 无线局域网标准。IEEE 802.11 标准定义了单一的 MAC 层和多样的物理层,其物理层标准主要有 IEEE 802.11b/a/g/n。

(2) IEEE 802.11b。IEEE 802.11b 标准是 IEEE 802.11 协议标准的扩展,1999 年 9 月正式通过。它可以支持最高 11Mb/s 的数据速率,运行在 2.4GHz 的 ISM 频段上,采用的调制技术是 CCK。

(3) IEEE 802.11a。IEEE 802.11a 工作在 5GHz 频段上,使用 OFDM 调制技术可支持 54Mb/s 的传输速率。

(4) IEEE 802.11g。2003 年 7 月,802.11 工作组批准了 IEEE 802.11g 标准,IEEE 802.11g 在 2.4G 频段使用 OFDM 调制技术,使数据传输速率提高到 20Mb/s 以上; IEEE 802.11g 标准能够与 IEEE 802.11b 的 Wi-Fi 系统互相联通。

(5) IEEE 802.11n。IEEE 802.11n 计划将 WLAN 的传输速率从 IEEE 802.11a 和 IEEE 802.11g 的 54Mb/s 增加至 108Mb/s 以上,最高速率可达 320Mb/s。IEEE 802.11n 计划采用 MIMO 与 OFDM 相结合,使传输速率成倍提高。IEEE 802.11n 标准全面改进了 IEEE 802.11 标准,不仅涉及物理层标准,同时也采用新的高性能无线传输技术提升 MAC 层的性能,优化数据帧结构,提高网络的吞吐量性能。

2. 无线局域网组件

无线网络的硬件设备主要包括 4 种,即无线网卡、无线 AP、无线路由和无线天线。当然,并不是所有的无线网络都需要这 4 种设备。事实上,只需几块无线网卡,就可以组建一个小型的对等式无线网络。当需要扩大网络规模时,或者需要将无线网络与传统的局域网连接在一起时,才需要使用无线 AP。只有当实现 Internet 接入时,才需要无线路由。而无线天线主要用于放大信号,以接收更远距离的无线信号,从而延长无线网络的覆盖范围。

(1) 无线 AP。无线接入点或称无线 AP(Access Point),如图 3-1 所示,其作用类似于以太网中的集线器。当网络中增加一个无线 AP 之后,即可成倍地扩展网络覆盖直径。另外,也可使网络中容纳更多的网络设备。通常,一个 AP 可以支持多达 80 台计算机的接入。

无线 AP 都拥有一个或多个以太网接口,用于无线与有线网络的连接,可以将安装双绞线网卡的计算机与安装无线网卡的计算机连接在一起,从而实现无线与有线的无缝融合。借助于 AP 可接入固定网络的特性,还可以将分散布置在各处的无线 AP 利用双绞线连接在一起,实现无线漫游。另外,借助于 AP,还可以实现若干固定网络的远程廉价连接,既无须架设光缆,也无须考虑由施工而可能带来的各种麻烦。

(2) 无线路由器。无线路由器(如图 3-2 所示)事实上就是无线 AP 与宽带路由器的结

合。借助于无线路由器,可实现无线网络中的 Internet 连接共享,实现 ADSL、Cable Modem 和小区宽带的无线共享接入。如果不购置无线路由,就必须在无线网络中设置一台代理服务器才可以实现 Internet 连接共享。

图 3-1　无线 AP

图 3-2　无线路由器

无线路由器也通常拥有一个或多个以太网接口。如果家庭中原来拥有安装双绞线网卡的计算机,可以选择多端口无线路由器,实现无线与有线的连接,并共享 Internet。否则,可只选择拥有一个以太网端口的无线路由器,从而节约购置资金。

(3) 其他无线产品。远程供电模块用于借助双绞线为无线网桥提供远程供电,避免线缆随着距离延长而导致的信号衰减,从而便于无线网桥的部署。

无线打印共享器直接连接打印机的并行口,从而实现无线网络与打印机的连接,使无线网络中的计算机能够共享打印机。如图 3-3 所示为无线打印共享器。除此之外,还有无线摄像头(如图 3-4 所示),用于远程无线监控等。

图 3-3　无线打印共享器

图 3-4　无线摄像头

3.2.2　无线局域网的接入方式

目前,无线局域网的接入方式主要有以下 4 种:无线对等网络、独立无线网络、接入以太网的无线网络和无线漫游的无线网络。

1. 无线对等网络

无线对等网络方案通常只使用无线网卡。因此,仅为每台计算机插上无线网卡,就可以

实现计算机之间的连接，构建成最简单的无线网络，它们之间可以相互直接通信。无线对等网络方案最适用于组建小型的办公网络和家庭网络（如图 3-5 所示）。

2. 独立无线网络

独立无线网络，是指无线网络内的计算机之间构成一个独立的网络，无法实现与其他无线网络和以太网络的连接，如图 3-6 所示。独立无线网络使用一个无线访问点 AP 和若干无线网卡。

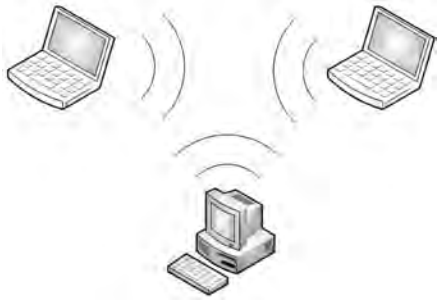

图 3-5　无线对等网络

图 3-6　独立无线网络

独立无线网络方案与对等无线网络方案非常相似，所有的计算机中都安装有一块网卡。所不同的是，独立无线网络方案中加入了一个无线访问点 AP。无线访问点类似于以太网中的集线器，可以对网络信号进行放大处理，一个工作站到另外一个工作站的信号都可以经由该 AP 放大并进行中继。因此，拥有 AP 的独立无线网络的网络直径将是无线对等网络有效传输距离一倍，在室内通常为 60m 左右。

3. 接入以太网的无线网络

当无线网络用户足够多时，应当在有线网络中接入一个无线接入点 AP，从而将无线网络连接至有线网络主干。AP 在无线工作站和有线主干之间起网桥的作用，实现了无线与有线的无缝集成，既允许无线工作站访问网络资源，同时又为有线网络增加了可用资源。

该方案适用于将大量的移动用户连接至有线网络，从而以低廉的价格实现网络直径的迅速扩展，或为移动用户提供更灵活的接入方式（如图 3-7 所示）。

4. 无线漫游的无线网络

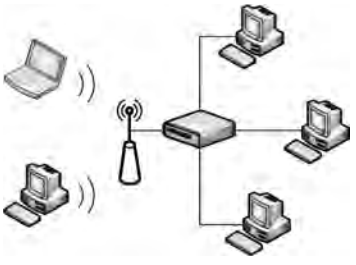

图 3-7　接入以太网的无线网络

无线漫游的无线网络中访问点作为无线基站和现有网络分布系统之间的桥梁。当用户从一个位置移动到另一个位置时，以及一个无线访问点的信号变弱或访问点由于通信量太大而拥塞时，可以连接到新的访问点，而不中断与网络的连接。这种方式与蜂窝移动电话非常相似，将多个 AP 各自形成的无线信号覆盖区域进行交叉覆盖，实现各覆盖区域之间无缝连接。所有 AP 通过双绞线与有线骨干网络连接，形成以固定有线网络为基础，无线覆盖为延伸的大面积服务区域，所有无线终端通过就近的 AP 接入网络，访问整个网络资源。蜂窝覆盖大大扩展了单个 AP 的覆盖范围，从而突破了无线网络覆盖半径的限制，用户可以在 AP 群覆盖的范围内漫游，而不会和网络失去联系，通信不会中断。

使用无线蜂窝覆盖结构具有以下优势：增加覆盖范围，实现全场覆盖；实现众多终端用户的负载平衡；可以动态扩展，系统可伸缩性大；对用户完全透明，保证覆盖场内服务无间断。

由于多个 AP 信号覆盖区域相互交叉重叠，因此，各个 AP 覆盖区域所占频道之间必须遵守一定的规范，邻近的相同频道之间不能相互覆盖，否则会造成 AP 在信号传输时的相互干扰，从而降低 AP 的工作效率。在可用的 11 个频道中，仅有三个频道是完全不覆盖的，它们分别是频道 1、频道 6 和频道 11，利用这些频道作为多蜂窝覆盖是最合适的(如图 3-8 所示)。

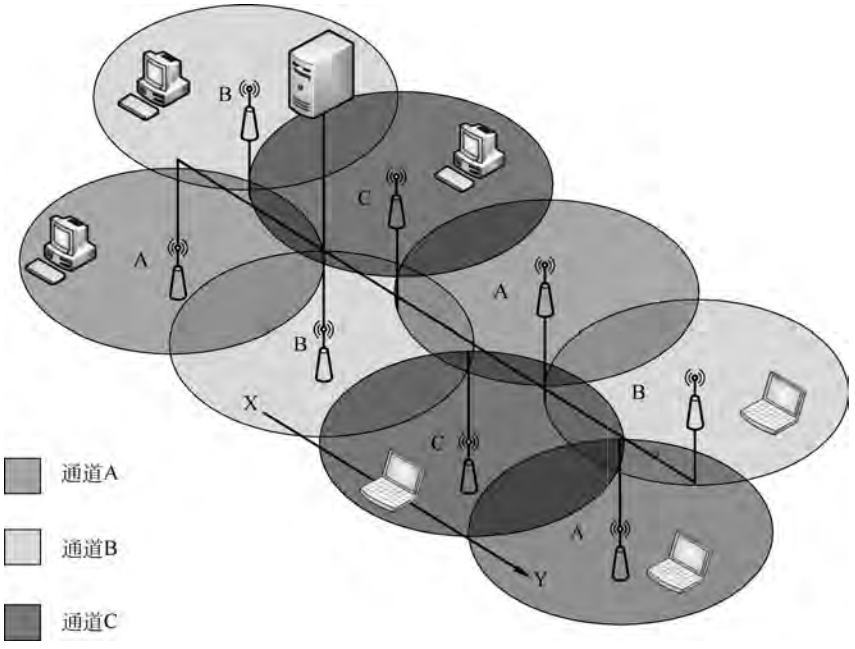

图 3-8　无线漫游的无线网络

由于无线蜂窝覆盖技术的漫游特性，使其成为应用最广泛的无线覆盖方案，适合在学校、仓库、机场、医院、办公室、会展中心等不便于布线的环境使用，快速简便地建立起区域内的无线网络，用户可以在区域内的任何地点进行网络漫游，从而解决了有线网络无法解决的问题，为用户带来了最大的便利。

无线局域网络在大楼之间、餐饮及零售、医疗、企业、仓储管理、货柜集散场、监视系统、展示会场等场所有较为广泛的应用。无线局域网络发展前景十分广阔。

3.2.3　Wi-Fi 关键技术

随着无线局域网技术的应用日渐广泛，用户对数据传输速率的要求越来越高。但是在室内，这个较为复杂的电磁环境中，多径效应、频率选择性衰落和其他干扰源的存在使得实现无线信道中的高速数据传输比有线信道中困难，WLAN 需要采用合适的调制技术。

IEEE 802.11 无线局域网络是一种能支持较高数据传输速率(1～54Mb/s)，采用微蜂窝结构的自主管理的计算机局域网络。其关键技术有 DSSS/CCK 技术、PBCC 技术和 OFDM 技术。每种技术皆有其特点，扩频调制技术正成为主流，而 OFDM 技术由于其优越的传输性能成为人们关注的新焦点。本节重点介绍 OFDMA、MU-MIMO 和 1024QAM，其

他关键技术，如空分复用及着色技术等，读者可以参考其他相关资料。

1. OFDMA

正交频分多址（Orthogonal Frequency-Division Multiple Access，OFDMA）是从 OFDM 演进来的，最早应用于 4G LTE 通信技术，后来被引入 Wi-Fi6 标准中。在此之前的几代 Wi-Fi 技术中，处理每个用户发送数据的时候（无论数据包的大小）都会占用整个通信信道。除此之外，在 Wi-Fi 网络中还需要传输大量的管理帧与控制帧，虽然此类帧数据包小，但要占用整个信道，以维持整个 Wi-Fi 系统的正常运作，就像一辆大货车只拉了一件小货品。而 Wi-Fi6 使用了 OFDMA 技术后，在频域上可以将无线通信信道划分为多个子信道（子载波），将最小的子信道称为“资源单位（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，形成一个个频率资源块，每个用户数据承载在每个资源块上，而不是占用整个通信信道，从而实现在每个时隙内有多个用户同时并行传输，不必排队等待、相互竞争，既提升了效率，又降低了排队等待时延。因此，OFDMA 特别适合传输大量小数据包的多用户场景，例如物联网或语音等。

Wi-Fi6 标准里采纳了这种新技术来提高频谱的利用效率，以 160MHz 的带宽为例，最多可以分成 74 个资源单元，同时供 74 个用户并发。

2. MU-MIMO

多进多出（Multiple-Input Multiple-Output，MIMO）技术最早起源于 Wi-Fi，并应用于 Wi-Fi4，之后又被应用于 Wi-Fi5 与 LTE。

多用户的多进多出（Multi-User MIMO，MU-MIMO）技术最早用于 Wi-Fi5 的 IEEE 802.11ac wave 2 阶段，但只支持 AP 到终端的下行传输过程，其 AP 结点可以同时向多个支持 MU-MIMO 的客户端发送数据包，解决了之前无线 AP 一次只能和一个终端通信的问题。Wi-Fi6 保持了这一技术，并进一步增强，在 Wi-Fi6 里增加了支持上行（Uplink MU-MIMO）传输，而且最多支持 8×8 的天线，即最多支持 8 个 1×1 用户的并发上行或下行。

总的来说，OFDMA 与 MU-MIMO 分别从频率空间和物理空间两方面提高多路并发处理能力，从而带来了多路并发处理能力，进而带来了整体网络性能和速度的极大提高，全面优化用户和应用体验，更好地适应万物互联以及高带宽、多并发场景应用。Wi-Fi6 标准允许 OFDMA 和 MU-MIMO 同时使用，但不要将二者的应用场景混淆。OFDMA 支持多用户通过细分信道（子信道）来提高并发效率，MU-MIMO 支持多用户通过不同的空间流来提高吞吐量。

OFDMA 与 MU-MIMO 技术特性对比如表 3-1 所示。

表 3-1　OFDMA 与 MU-MIMO 的技术特性对比

OFDMA	MU-MIMO
提升效率	提升容量
降低时延	每个用户速率更高
适合低速带宽应用	适合高带宽应用
适合小包报文传输	适合大包报文传输

3. 1024QAM

正交振幅调制（Quadrature Amplitude Modulation，QAM）是数字信号的一种调制方

式。QAM调制实际上是幅度调制和相位调制的组合,相位+幅度状态定义了一个数字或数字的组合。比如16QAM的星座图,信息"1100"可用相位2250、振幅25%的组合来表示。每一个星座点对应一个一定幅度和相位的信号,这个信号再被上变频到射频信号发射出去。

IEEE 802.11ax标准的目标是增加系统容量、降低时延、提高高密度多用户的效率。IEEE 802.11ac最大支持256QAM,单位信号可以表达8b(256)的信息。IEEE 802.11ax引入了更高阶的编码,即1024QAM,单位信号可以表达10b(1024)的信息。从8b到10b,提升了25%,与256QAM相比,1024QAM单条空间流的数据吞吐量提高了25%。

由于1024QAM信息密度增加,对信号质量的要求也更高,因此该技术在无线环境较好、距离较近的场景中才能充分发挥优势,如信号良好的小型办公室、会议室等。

3.2.4 Wi-Fi6

1. 不同Wi-Fi的区别

Wi-Fi1到Wi-Fi6命名规范:802.11ax=Wi-Fi6、802.11ac=Wi-Fi5、802.11n=Wi-Fi4、802.11g=Wi-Fi3、802.11a=Wi-Fi2、802.11b=Wi-Fi1。新一代Wi-Fi6的主要特点在于速度更快、延时更低、容量更大、更安全、更省电等。

1)速度更快

Wi-Fi6与Wi-Fi5都支持相同的信道带宽。频段方面Wi-Fi5只涉及5GHz,而Wi-Fi6则覆盖2.4/5GHz,完整涵盖低速和高速设备。调制模式方面,Wi-Fi6支持1024QAM,高于Wi-Fi5的256QAM,数据容量更高,意味着更高的数据传输速度。此外,Wi-Fi6加入了新的OFDMA技术,支持多个终端同时并行传输,有效提升了效率并降低延时,这也就是其数据吞吐量大幅提升的秘诀。

2)延时更低

这主要归功于同时支持上行与下行的MU-MIMO和OFDMA新技术。上一代Wi-Fi5标准即支持MU-MIMO技术,但是仅支持下行。而Wi-Fi6则同时支持上行与下行MU-MIMO,这意味着移动设备与无线路由器之间上传与下载数据时都可体验MU-MIMO,进一步提高无线网络带宽利用率。Wi-Fi6采用了OFDMA技术,它是Wi-Fi5所采用的OFDM技术的演进版本,将OFDM和FDMA技术结合,在利用OFDM对信道进行父载波化后,在部分子载波上加载传输数据的传输技术。

3)容量更大

Wi-Fi6还引入了BSS Coloring着色机制,标注接入网络的各个设备,同时对其数据也加入对应标签,传输数据时也就有了对应的地址,直接传输到位而不会发生混乱。MU-MIMO技术允许多终端共享信道,使多台手机/计算机一起同时上网,从此前低效的排队顺序通过方式变成为"齐头并进"的高效方式。再结合OFDMA技术,Wi-Fi6网络下的每个信道都可进行高效率数据传输,提升多用户场景下的网络体验,可以更好地满足Wi-Fi热点区域,多用户使用,并且不容易卡顿,容量更大。

4)更安全

Wi-Fi6无线路由器设备若需要通过Wi-Fi联盟认证,必须采用WPA 3安全协议,安全性更高。WPA 3是2018年年初Wi-Fi联盟发布的新一代Wi-Fi加密协议,是目前广泛使用的WPA 2协议的升级版本,安全性进一步提升,可以更好地阻止强力攻击、暴力破解等。

5）更省电

Wi-Fi6 引入了 Target Wake Time(TWT)技术，允许设备与无线路由器之间主动规划通信时间，减少无线网络天线使用及信号搜索时间，这也就意味着能够一定程度上减少电量消耗，提升设备续航时间。

2. Wi-Fi 分布式网络部署架构

Wi-Fi Mesh 和 Wi-Fi6 是 Wi-Fi 领域内不同的两种技术，Wi-Fi6 在基础技术上通过 1024QAM、OFMDA、MU-MIMO、BSS Coloring 和 TWT 等多项创新科技，获得了更高的网速、更多联网设备下的低时延、更强的抗干扰能力、更省电等多方面进步。而 Mesh 技术经过近年来的发展，也趋于成熟，尤其是 EasyMesh 协议的推出，使得不同品牌路由器之间的互联成为可能，更重要的是，Mesh 技术可以增强对复杂户型、大户型等房屋 Wi-Fi 信号的覆盖，从而满足用户在室内无缝切换、不间断上网方面的刚需。

集合了 Mesh、Wi-Fi6 技术的 Wi-Fi6 分布式路由器，不仅信号强、覆盖好，而且安装起来非常简单，对用户的技能要求相对 WDS(Wireless Distribution System) 低得多。美国网件公司(NETGEAR)在 2019 年的 IFA 国际电子消费展上展示了具备 Mesh 功能的 Wi-Fi6 产品，国内包括 360、华硕、TP-Link 等多家公司也陆续推出了类似的产品。

目前主流的 Mesh 路由器在传输过程中，采用的是 2.4 GHz +5 GHz +5 GHz 的三频段收发，其中一个 5 GHz 频段是 Mesh 专门用来回传的，因此不会占用本身的网络带宽。可以说，Wi-Fi6 + Mesh 的组网方式会逐渐普及。

3. Wi-Fi6 应用场景

1）承载 4K/8K/VR 等大宽带视频

Wi-Fi6 技术支持 2.4G 和 5G 频段共存，其中，5G 频段支持 160MHz 频宽，速率最高可达 9.6Gb/s 的接入速率，其 5G 频段相对干扰较少，更适合传输视频业务，同时通过 BSS 着色技术、MIMO 技术、动态 CCA 等技术降低干扰，降低丢包率，带来更好的视频体验。

2）承载网络游戏等低时延业务

网络游戏类业务属于强交互类业务，在宽带、时延等方面提出了更高的要求，对于 VR 游戏，最好的接入方式就是 Wi-Fi 无线方式，Wi-Fi6 的信道切片技术提供游戏的专属信道，降低时延，满足游戏类业务特别是云 VR 游戏业务对低时延传输质量的要求。

3）智慧家庭智能互联

智慧家庭智能互联是智能家居、智能安防等业务场景的重要因素，当前家庭互联技术存在不同的局限性，Wi-Fi6 技术将给智能家庭互联带来技术统一的机会，将高密度、大数量接入、低功耗优化集成在一起，同时又能与用户普遍使用的各种移动终端兼容，提供良好的互操作性。

4）行业应用

Wi-Fi6 作为新一代高速率、多用户、高效率的 Wi-Fi 技术，在行业领域中有广泛的应用前景，如产业园区、写字楼、商场、医院、机场、工厂。

3.3 ZigBee 技术

随着通信技术的快速发展，短距离无线通信技术已经成为通信技术中的一大热点。工业控制自动化、家居智能化等短距离无线通信技术应用领域都需要具备低成本、近距离、组

网能力强等优点的无线互联技术,ZigBee就是在这样的背景下应运而生的。

3.3.1 ZigBee标准概述

ZigBee这个名字来源于蜂群的通信方式:蜜蜂之间通过跳Zigzag形状的舞蹈来交互消息,以便共享食物源的方向、位置和距离等信息。由于蜜蜂体积小,所需能量小,所以人们用ZigBee技术来代表这种近距离、低成本、体积小、低功耗、低复杂度、低数据速率的无线通信技术。它采用直接序列扩频(DSSS)技术,工作频率为868MHz、915MHz或2.4GHz,都是无须申请执照的频率。该技术的突出特点是应用简单、电池寿命长、组网能力强、可靠性高以及成本低。主要应用领域包括工业控制、消费性电子设备、汽车自动化、农业自动化和医用设备控制等。

ZigBee技术是基于IEEE 802.15.4无线标准开发的,IEEE 802.15.4定义了两个底层,即物理层和媒体接入控制(Media Access Control,MAC)层。ZigBee联盟则在IEEE 802.15.4的基础上定义了网络层和应用层。ZigBee联盟成立于2001年8月,该联盟由霍尼韦尔、Invensys、三菱、摩托罗拉、飞利浦等公司组成,并吸引了上百家芯片公司、无线设备公司和开发商的加入,其目标市场是工业、家庭以及医学等需要低功耗、低成本、对数据速率和QoS(服务质量)要求不高的无线通信应用场合。

3.3.2 ZigBee技术特点

目前ZigBee技术也已经比较成熟,对于ZigBee设备来说,它并没有太大的体积,不但成本较低而且还是模块化设计的硬件,从开支上有了很大的节约。从整体的层面来看,ZigBee技术的特点主要表现如下。

1. 设备能量消耗低

基于正常的模式下,ZigBee网络结点主要工作在数据采集环节,没有较大的数据传输量;在传输的速率方面,要显著低于其他网络传输的速度,因此没有较大的能量消耗。而且为了进一步减少能耗,每个结点都不会全天处于工作状态,在数据传输较少的时间段一般都是采用结点休眠模式。

2. 通信数据可靠传输

在ZigBee网络内部,采用了碰撞避免机制,同时为需要固定带宽的通信业务预留了专用时隙,避免了发送数据时的竞争和冲突,所以数据在进行传输的时候,就不会产生碰撞的情况。不论是接收还是发送数据,务必经过确认之后才会给予回复。结点模块之间具有自动动态组网的功能,信息在整个ZigBee网络中通过自动路由的方式进行传输,从而保证了信息传输的可靠性。

3. 网络接入容量大

ZigBee具备一个较大的网络接入容量,它可支持达65 000个结点。对于ZigBee来说,在传输的时候采用的是自组网的形式,在它逐级中转的终端结点信息就是经由路由结点而实现的,最终会到达协调器,进而形成一个巨大的网络系统。

4. 设备安全性

ZigBee提供了数据完整性检查和鉴权功能,加密算法采用通用的AES-128。

5. 时延短

ZigBee 针对时延敏感的应用做了优化，通信时延和从休眠状态激活的时延都非常短。

6. 成本低廉

对于 ZigBee 的通信频段来说，采取的通信频段是 2.4GHz 的，该频段在全球范围当中都是免费注册的，因此可以节约很大一部分成本。

3.3.3 ZigBee 协议框架

如图 3-9 所示，ZigBee 采用了分层的思想，其协议栈包括五层：物理层（PHY）、媒体访问控制层（MAC）、网络层（NWK）、应用层（APL）和安全服务提供层（SSP）。ZigBee 物理层和媒体访问控制层由 IEEE 802.15.4 标准规定，ZigBee 联盟在 IEEE 802.15.4 的基础上定义了网络层和应用层，应用层包含应用支持子层（APS）、ZigBee 设备对象（ZDO）以及厂商自定义的应用对象。ZigBee 协议利用安全服务供应商（SSP）向网络层和应用层提供数据加密服务。

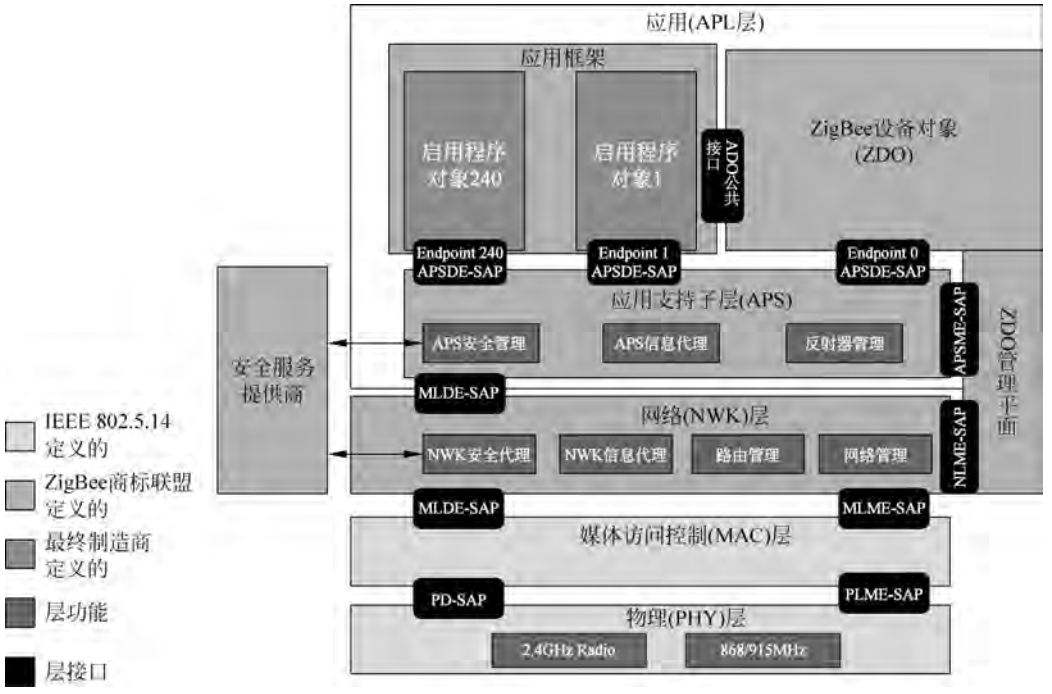

图 3-9　ZigBee 协议框架图

IEEE 802.15.4 有两个 PHY 层，运行在两个不同的频率上：868/915MHz 和 2.4GHz，分别支持 20kb/s、40kb/s 和 250kb/s 的传输速率。IEEE 802.15.4 MAC 层使用 CSMA/CA 冲突避免机制对无线信道访问进行控制，负责物理相邻设备间的可靠连接。

1. 网络层

网络层是协议栈的核心层，它负责网络的建立、设备的加入、路由搜索、消息传递等相关功能。

2. 应用层

应用层主要负责把不同的应用映射到 ZigBee 网络上,具体功能包括:安全与鉴权,多个业务数据流的会聚,设备发现,服务发现。它是由应用支持子层(APS)、应用框架和 ZigBee 设备对象(ZDO)构成。APS 层主要负责对等设备间数据传输与绑定表的建立和维护。ZDO 则负责定义设备在网络中的角色,发现设备以及它们所提供的服务。

3. 安全层

安全层用于保证网络中的便携设备不会意外泄漏其标识以及其他结点不会俘获传输中的信息。

3.3.4 ZigBee 各层规范

IEEE 802.15.4 采用 OSI/RM 的方法定义了低速无线个域网(LR-WPAN)结构。每一层负责标准规定的部分网络功能,并为其上层提供服务。

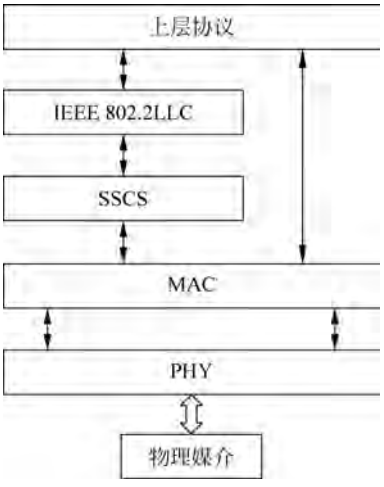

图 3-10 协议栈框架

IEEE 802.15.4 定义了物理层(PHY)和介质访问控制层(MAC),PHY 层包含射频器和控制机制,MAC 层规定了媒体访问控制方法。如图 3-10 所示,网络上层协议(包括网络管理,路由层以及应用层)利用链路层的服务来完成其功能。IEEE 802.2 逻辑链路控制层(Logic Link Control,LLC)通过特别服务汇聚子层(Service Specific Convergence Sublayer,SSCS)访问 MAC 子层。

1. 物理层

IEEE 802.15.4 的物理层规范实现的功能基本上与 OSI 参考模型的物理层相对应,只是个别地方做了改动。因为物理层位于设备结点的最底层,功能是实现并保障信号的有效传输,所以物理层会涉及与信号传输有关的各个方面,包括如何发生信号、怎样发送与接收信号,数据信号采用哪种传输编码机制、选择同步或者异步传输等。物理层的作用是在一条物理传输媒体上,实现数据链路实体之间透明地传输各种数据的比特流,并且为上层提供服务。服务包括:物理连接的建立、维持与释放、物理服务单元的传输、物理层管理、数据编码。

IEEE 802.15.4 标准的物理层处于射频收发器和 MAC 子层之间,它为射频信道和 MAC 子层都提供了接口。物理层的主要功能分为数据服务和管理服务两部分,其中,负责管理服务的部分称为物理层管理实体(Physical Layer Management Entity,PLME),该实体通过调用物理层的管理功能函数,为物理层管理服务提供其接入口。数据服务主要负责数据的接收和发送,管理服务主要负责射频收发器的激活和休眠、空闲信道评估、信道能量检测、信道的频段选择、链路质量指示等。

2. MAC 层

IEEE 802.15.4MAC 层负责相邻设备间的单跳数据通信。它负责建立与网络的同步,支持关联和去关联以及 MAC 层安全,它能提供两个设备之间的可靠链接。

MAC 协议的主要功能有：协调器产生网络信标、信标同步、支持关联和解关联、CSMA/CA 信道访问机制、处理和维护 GTS 机制、在两个对等 MAC 实体之间提供可靠链路等功能。

在基于竞争的信道接入方式当中，载波侦听多址机制（CSMA）得到了广泛的应用。CSMA 机制又分为两种：CSMA/CD 和 CSMA/CA，前者是载波侦听多址/冲突监测，若监测到信道接入冲突，则进行重传，这适用于有线网络，而相对于比较难监测到冲突的无线信道来说，只能采取冲突避免的方式，即 CSMA/CA。CSMA/CA 机制的基本思想是，如果某结点监测到当前信道不可用（即可能出现冲突），则该结点对数据发送进行一定的随机延时处理，延时完毕之后再进行信道监测，若信道仍不可用，则加大延时的长度，如此循环，直至数据发送成功或者尝试次数超过设定的最大值。

3. ZigBee 网络层

1）网络层概述

ZigBee 网络层需要提供一些必要的函数确保 ZigBee 的 MAC 层正常工作，并且为应用层提供合适的服务接口。为了向应用层提供其接口，网络层提供了两个必需的功能服务实体，分别为网络层数据服务实体（NLDE）和网络层管理实体（NLME）。图 3-11 给出了网络层各组成部分和接口。

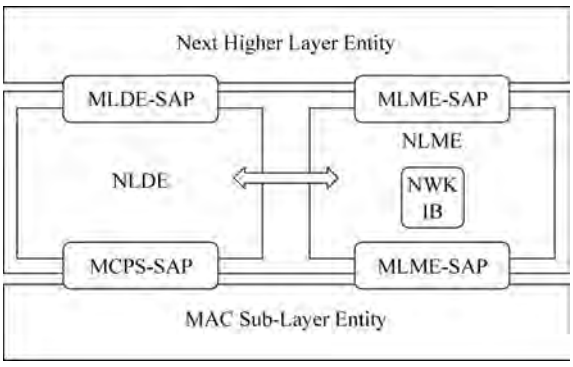

图 3-11　网络层参考模型图

2）网络层数据实体

网络层数据实体为数据提供服务，在两个或者更多的设备之间传送数据时，将按照应用协议数据单元（APDU）的格式进行传送，并且这些设备必须在同一个网络中，即在同一个内部个域网中。

网络层数据实体提供如下服务。

（1）生成网络层协议数据单元（NPDU）：网络层数据实体通过增加一个适当的协议头，从应用支持层协议数据单元中生成网络层的协议数据单元。

（2）指定拓扑传输路由，网络层数据实体能够发送一个网络层的协议数据单元到一个合适的设备，该设备可能是最终目的通信设备，也可能是在通信链路中的一个中间通信设备。

（3）安全：确保通信的真实性和机密性。

3）网络层管理实体

网络层管理实体提供网络管理服务，允许应用与堆栈相互作用。网络层管理实体应该

提供如下服务。

(1) 配置一个新的设备：为保证设备正常工作的需要，设备应具有足够的堆栈，以满足配置的需要。配置选项包括对一个 ZigBee 协调器或者连接一个现有网络设备的初始化的操作。

(2) 初始化一个网络：使之具有建立一个新网络的能力。

(3) 连接和断开网络。具有连接或者断开一个网络的能力，以及为建立一个 ZigBee 协调器或者路由器，具有要求设备同网络断开的能力。

(4) 寻址：ZigBee 协调器和路由器具有为新加入网络的设备分配地址的能力。

(5) 邻居设备发现：具有发现、记录和汇报有关一跳邻居设备信息的能力。

(6) 路由发现：具有发现和记录有效地传送信息的网络路由的能力。

(7) 接收控制：具有控制设备接收状态的能力，即控制接收机什么时间接收、接收时间的长短，以保证 MAC 层的同步或正常接收等。

4) 网络层功能

ZigBee 网络层的主要功能有：构建一个新网络，设备加入已存在的网络，已加入网络的设备从网络中退出，路由功能。

(1) 新建网络。

网络设备上电后，无线协议栈各层首先进行初始化，然后通过网络请求原语来启动一个新的网络，仅当具有协调器能力且当前还没有与网络连接的网络设备才可以建立一个新的网络。组网开始时，网络层首先向 MAC 层请求分配协议所规定的信道，或者由 PHY 层进行有效信道扫描，网络层管理实体等待信道扫描结果，然后根据扫描情况选择可允许能量水平的信道。找到合适的信道后，为这个新的网络选择一个网络标识符(PAN ID)，PAN ID 可由网络形成请求时指定，也可选择一个随机的 PAN ID(除广播 PAN ID0xFFFF 外)，PAN ID 在所选信道中应该是唯一的。PAN ID 一旦选定，无线网络协调器将选择 16 位网络地址 0x0000 作为自身短地址，同时进行相关设置，完成设置后，通过 MAC 层发出网络启动请求，返回网络形成状态。

(2) 设备加入网络。

设备加入网络功能就是通过与已加入网络的协调者或路由器设备建立连接来实现的。当设备与某一网络协调者或路由器连接后，将形成父子关系，前者为子设备，后者为父设备。

当子设备接收到加入网络命令后，如果子设备已经同网络连接，则返回出错标志，否则尝试连接网络协调者或路由器。首先，子设备要获取具有允许连接能力的网络协调者或路由器的地址信息。其次，在获取了要加入的父设备信息后，子设备向父设备发送连接请求命令。父设备接收到连接命令后，检查当前资源是否能够再接收新设备。若资源满足后，父设备将存储子设备地址，并为子设备分配 16 位的网络地址，同时向连接请求子设备发送有未处理数据的 Ack 应答帧；若资源不满足，则直接发送无未处理数据的 Ack 应答帧。子设备在一段时间内等待接收来自父设备的 Ack 应答帧，接收到后判断父设备是否有本设备的未处理数据，若无或在指定时间内未接收到 Ack 应答帧则退出；若有则向父设备发送数据请求命令，父设备接收到该命令后，发送缓存的连接响应命令帧。子设备接收到后，更新其设备网络地址、PAN ID、父设备地址信息等参数，此时子设备就完成了加入 PAN 的整个过程。

(3) 地址分配。

网络中任一结点都含有唯一的 64 位 IEEE 地址(长地址)以及可分配的 16 位短地址,短地址在信息传输之前就已经被分配完成。网络协调器给自己分配短地址为 0x0000,网络深度为 0,给其子设备分配网络深度为 1,对于多跳网络则深度大于 1。为了最小化网络流量,同时简化设备结构,降低成本和设备功耗,ZigBee 网络层采用了分布式地址分配方案,短地址的分配由参数确定:网络的最大深度,每个父设备能最多连接子设备的数目,每个路由器能最多连接子路由器的数目。

设备地址分配完成后,设备之间通信主要依靠地址信息进行通信,为了延长电池的寿命,如果设备处于同一网内,数据传输一般可采用短地址,这样既可以缩小数据包的大小,同时还可以缩短数据在设备中间的传送时间,减小电量消耗,延长电池寿命。如果设备处于通信范围内不同子网内,则可根据 PAN ID 和短地址进行通信。

(4) 已入网设备退出网络。

对于已连接网络的设备主要有两种从网络中断开连接的方式:子设备自身主动要求断开连接,父设备要求某一子设备从网络中断开连接。

① 子设备自身主动要求断开连接:子设备首先检查自身是否已经加入网络,并且父设备是否与要断开连接的对象相同;接着子设备组织断开连接请求命令帧,并发送给父设备;注意按照 ZigBee 协议规定,子设备在发送了断开连接请求命令后,无论父设备是否做出断开连接响应,子设备均将其父设备信息清空,表示子设备已经从网络中退出;当父设备成功接收到断开连接请求命令时,在其邻居表中检查是否存在该子设备,若存在则将该子设备从邻居表中移除。

② 父设备要求某一子设备从网络中断开连接:父设备首先检查要断开连接的对象是否在其邻居表中,若在则生成断开连接请求命令帧,并发送给指定子设备;与子设备主动要求断开连接一样,无论父设备是否收到子设备的应答,都将该子设备从邻居表中移除;当子设备成功接收到断开连接命令后,将父设备信息清空。

(5) 路由功能。

ZigBee 网络层路由功能主要包括记录最佳有效路由、维护路由表、为上层初始化路由选择以及路由修复。其中,路由选择是根据路由成本进行度量,路由成本为组成路由的多跳链路成本之和。链路成本的获取是通过记录基于 IEEE 802.15.4 的 MAC 层和 PHY 层所提供的每一帧的链路质量(LQI)值,根据此链路成本大小进行路由选择,数据传递时选择低链路成本的路由设备作为目的设备进行跳转。

如果要求设备具有路由功能则必须提供路由算法,网络层协议设计了一套基本路由算法。基本路由设备首先检查与目的地址相对应的路由表入口,然后根据在该入口中所找到的下一跳地址,发送数据帧。如果该设备没有与目的地址相对应的路由表入口,则检查网络层帧头控制域中的路由选择子域;如果该选择子域为 1,则设备将根据链路成本算法进行路由选择;如果该选择子域的值为 0,则设备就会使用分级路由的方法选择路由。

4. ZigBee 应用层

ZigBee 应用层由三个部分组成:应用支持子层(APS)、ZigBee 设备对象(ZDO)和制造商定义的应用对象。

从应用角度看,通信的本质就是端点到端点的连接,端点之间的通信是通过称为簇的数

据结构实现的,每个接口都能接收或发送簇格式的数据。一共有两个特殊的端点,即端点0和端点255。端点0用于整个ZigBee设备的配置和管理。应用程序可以通过端点0与ZigBee协议栈的其他层通信,从而实现对这些层的初始化和配置。附属在端点0的对象被称为ZDO,应用层通过ZDO对网络层参数进行配置和访问。端点255用于向所有端点的广播,端点241～254是保留端点。所有端点都使用APS提供的服务,APS为数据传送、安全和绑定提供服务,能够适配不同且相互兼容的设备。

1) ZigBee应用支持子层APS

APS提供了这样的接口:在网络层和上层实体(NHLE)之间,从ZigBee设备对象到供应商应用对象的通用服务集。这个服务由两个实体实现:APS数据实体(APSDE)和APS管理实体(APSME)。图3-12描述了APS子层的构成和接口。

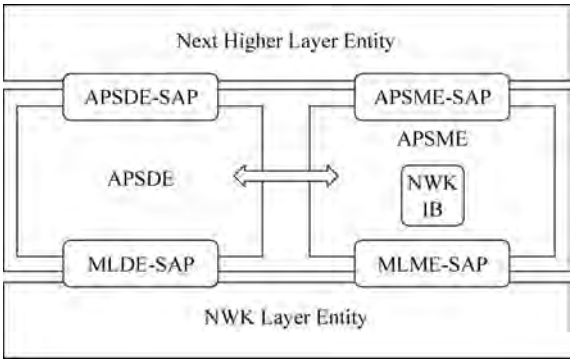

图3-12　应用支持子层参考模型图

(1) APS数据实体(APSDE)。

APSDE向网络层提供数据服务,并且为ZDO和应用对象提供服务,完成两个或多个处于同一个网络中的设备之间传输应用层PDU。

APSDE将提供如下服务。

① 生成应用层的协议数据单元(APDU):APSDE将应用层协议数据单元加上适当的协议帧头生成应用子层的协议数据单元。

② 绑定:两个设备服务和需求相匹配的能力。一旦两个设备绑定了,APSDE将可以把从一个绑定设备接收到的信息传送给另一个设备。

③ 组地址过滤:提供了基于终点组成员的过滤组地址信息的能力。

④ 可靠传输:比从网络层仅通过端对端的传输增加了可靠性。

⑤ 拒绝重复:提供传送的信息不会被重复接收。

⑥ 支持大批量的传输:提供两个设备间顺序传输大批量数据的能力。

⑦ 碎片:当消息的长度大于单个网络层帧时,可以分割并重组消息。

⑧ 流控制:APS提供避免传输消息淹没接收者的措施。

⑨ 阻塞控制:APS层使用“尽力”原则,提供措施避免传输消息淹没中间网络。

(2) APS管理实体(APSME)。

APSME提供管理服务支持应用程序,其应具有基于两个设备的服务和需求将它们匹配的连接起来的能力,该能力称为绑定服务。APSME还应具有能力来构建和维护绑定表

来存储这些信息。

另外，APSME 还提供如下服务。

① 应用层信息库管理：读取与设置设备应用层信息库属性的能力。

② 安全：与其他设备通过使用安全密钥建立可信关系的能力。

2) ZigBee 设备对象

ZigBee 设备对象(ZDO)在应用对象、设备 profile 和 APS 之间提供了一个接口。ZDO 位于应用框架和应用支持子层之间，它满足所有在 ZigBee 协议栈中应用操作的一般需要。ZDO 还有以下作用。

(1) 初始化应用支持子层，网络层、安全服务规范和除了应用层中端点 1～240 以外的 ZigBee 设备层。

(2) 从终端应用中集合配置信息来确定和执行发现、安全管理、网络管理，以及绑定管理。

3.4 5G 技术

3.4.1 5G 概述

1. 5G 和 3GPP

第五代移动通信技术(5th Generation Mobile Communication Technology，5G)是具有高速率、低时延和大连接等特点的新一代宽带移动通信技术，是实现人机物互联的网络基础设施。2015 年 10 月，国际电信联盟无线电通信部门(ITU-R)正式确定了 5G 的法定名称是“IMT-2020”。

从 3G 系统开始，到 4G、5G 系统，3GPP(3rd Generation Partnership Project，第三代合作伙伴计划)协议一直是移动制式的“圣经”。3GPP 协议演进的过程就是移动制式从 3G 系统演进到 4G、5G 系统的过程。从本质上来说，3GPP 就是一个行业协会。5G 的协议规范是由 3GPP 来制定，可以从 3GPP 的网站 www.3gpp.org 获得。

互联网(Information Technology，IT)、通信网(Communication Technology，CT)和物联网(Internet of Things，IoT)起源于不同的技术，遵循不同的互通标准，成长于不同的应用场景。随着业务需求的不断发展，移动网和互联网逐渐走到了一起，成为移动互联网；与此同时，将物联网融入现有移动网的呼声也与日俱增。移动互联网和物联网成为 5G 产生和发展的最主要动力。

5G 需要完成承接移动网、增强互联网、使能物联网的使用，实现 CT、IT、IoT 这“三 T”的深度融合。

2. 5G 三大场景

从最终用户的角度看，5G 的三个场景特征就是：干活快、不拖沓、挤不爆；用专业术语讲就是：超越光纤的传输速度(Mobile Beyond Giga)、超越工业总线的实时能力(Real-Time World)以及全空间的连接(All-Online Everywhere)。

(1) eMBB(enhanced Mobile BroadBand，增强移动带宽)场景。

大流量移动宽带业务，如高清视频业务，是 4G、5G 乃至 6G 的主要应用，主要的信息交

互对象是人与人或人与视频源。在5G的支持下,用户体验速率可提升至1Gb/s,峰值速度甚至达到20Gb/s,用户可以轻松实现在线4K/8K视频以及VR/AR视频。因此,用户数据业务流量还将爆发式增长,这会极大地释放远程智能视觉系统的需求,会出现层出不穷的新的行业应用。

(2) uRLLC(Ultra-Reliable Low Latency Communications,高可靠低时延连接)场景。

这个场景是物联网中的一个重要场景。像车联网、工业远程控制、远程医疗、无人驾驶等的特殊应用,对时延和可靠连接的要求比较严格。时延过大,将会导致严重的事故;可靠性低,将会造成财产损失。

在这样的场景下,连接时延要达到10ms以下,甚至是1ms的级别。对很多远程应用来说,操作体验能达到"零"时延,才会有很强的既视感和现场感。

(3) mMTC(massive Machine-Type Communications,海量机器类通信)场景。

这个场景也是物联网中的一个重要场景,针对的是大规模物联网业务,如智慧城市、智慧楼宇、智能交通、智能家居、环境监测等场景。

这类业务场景对数据速率要求较低,且时延不敏感,但对连接规模要求比较高,属于小数据包业务,信令交互比例较大,海量连接可能导致信令风暴。在5G时代,每平方千米的物联网连接数将突破百万,连接需求将覆盖社会、工作和生活的方方面面。5G的海量连接能力是渗透到各垂直行业的关键特性之一。

5G的三个场景就是我们选取5G网络架构技术和无线技术的出发点和归宿。5G网络构架技术和无线技术,最终要满足三个场景的需求。三个场景的行业应用发展又会进一步促进5G网络架构技术和无线技术的向前发展。

3. 5G组网方式

5G是移动通信网部署的大势所趋,但4G仍是当前网络设备的主流。建设和部署5G网络包括两个部分:无线接入网(Radio Access Network,RAN)和核心网(Core Network,CN)。无线接入网主要由基站组成,为用户提供无线接入功能。核心网主要为用户提供互联网接入服务和相应的控制管理等功能。

5G网络部署方式有两种:非独立组网模式(Non-Stand Alone,NSA)和独立组网模式(Stand Alone,SA)。

1) NSA

NSA指的是使用现有的4G基础设施,进行5G网络的部署。基于NSA架构的5G载波仅承载用户数据,其控制信令仍通过4G网络传输。在NSA组网中,大多是以LTE为锚点来实现5G NR(New Radio)与LTE(Long Term Evolution,长期演进)的双连接。

2) SA

SA指的是新建5G网络,包括5G基站、5G回程链路以及5G的核心网。SA组网在引入了全新网元与接口的同时,还将大规模采用网络NFV、SDN等新技术,并与5G无线侧的关键技术结合,其协议开发、网络规划部署及互通互操作所面临的挑战是巨大的。

将4G和5G组网部署方式结合起来考虑,在3GPP协议上提出了8个选项。其中,选项1、2、5、6是独立组网,选项3、4、7、8是非独立组网。非独立组网的选项3、4、7还有不同的子选项。在这些选项中,选项1是4G网络的结构。选项6和选项8仅是理论上存在的部署场景,不具有实际部署价值。

4. 5G 应用

1）5G 基础业务类型

5G 的基本业务类型，从大的方面，可以分为移动互联网和物联网类。移动互联网类包括 5 种基本业务类型，物联网业务（含采集类和控制类）包括 2 种基本业务类型，如表 3-2 所示。

表 3-2　5G 基础业务类型

网　　络	类　　型	业　　务
移动互联网	流类	音频播放、视频播放、高清视频会话类
	会话类	语音类、视频通话、虚拟现实交互类
	交互类	浏览类、位置类、交易类、搜索类、游戏类、增强现实、虚拟现实传输类
	传输类	邮件类、下载类、上传类消息类
	消息类	SMS 类、MMS 类、OTT 消息
物联网	采集类	低速采集、高速采集控制类
	控制类	时延敏感、时延非敏感

2）端管云架构

5G 应用解决方案架构的设计思路就是“端管云”架构。任何 5G 应用，都可以套用这个架构。

从“端管云”的作用来看，“端”就是人、物和 5G 网络的界面和接口，是信息发送的源结点，也可以是信息接收的目的结点。人类的信息接收和发送，物联网感知层信息采集和控制命令接收都依赖于“端”侧。“管”就是 5G 网络，它满足了将“端”侧采集到的信息进行远距离快速传输和大范围共享的需求；“云”就是指平台层，借助“ABCD”（人工智能、区块链、云计算和大数据）技术满足随着连接数指数级增长带来的数据分析和计算的需求。

3）常见 5G 应用

4G 以前，移动制式上的应用主要属于个人消费型。个人消费型的应用也将在 5G 能力的助力下继续迅猛发展。跨界融合是 5G 应用的关键词，垂直行业是 5G 施展网络能力的关键。5G 会逐步完成产业型应用场景的全覆盖。

各行各业的信息交互场景和业务需求，与 5G 的管道能力相组合，会产生各行各业的专用的产业型应用，如智能电网、智能物流、智慧医疗、工业物联网；也可以产生许多行业共用的智能型应用，如车联网、VR ＋ AR、无人机、智慧城市等。

3.4.2　5G 新空口

为了应对 5G 新场景的挑战，系统化地提出了 5G 新空口的理念和关键使能技术，全面覆盖基础波形、多址方式、信道编码等领域。下面介绍三大空口物理层技术：F-OFDM、SCMA 和 Polar 码。F-OFDM 是实现统一空口的基础波形，结合灵活的 Numerology 参数集以实现空口切片；SCMA 和 Polar 码在 F-OFDM 的基础上，进一步提升了连接数、可靠性和频谱效率，满足了对 5G 的能力要求。因此，这三大物理层关键技术成为构建 5G 新空口理念的基石。

1. 新波形 F-OFDM(Filtered OFDM)

基础波形的设计是实现统一空口的基础,同时兼顾灵活性和频谱的利用效率。4G 的 OFDM 虽然较好地解决了令人头疼的码间串扰问题,但 OFDM 最大的问题就是不够灵活。未来不同的应用对空口技术的要求迥异。

例如,毫秒级时延的车联网业务要求极短的时域符号 Symbol 和调度时间间隔 TTI,这就需要频域较宽的子载波间隔;而物联网的多连接场景中,单传感器传送数据量极低,对系统整体连接数要求很高,这就需要在频域上配置比较窄的子载波间隔,而在时域上,符号的长度以及调度时间间隔都可以足够长,这时不需要考虑码间串扰问题,不需要再引入循环前缀(Cyclic Prefix,CP),同时异步操作还可以解决终端省电的问题。

F-OFDM 能为不同业务提供不同的子载波时频资源配置。不同带宽的子载波之间,本身不再具备正交的特性了,就需要引入保护带宽。在 LTE 中使用 OFDM,就需要 10%的保护带宽。F-OFDM 增加了空口资源接入的灵活性,频谱利用率会不会因为保护带宽的增加而降低呢?灵活性与系统开销看起来就是一对矛盾。通过使用优化的滤波器,F-OFDM 可以把不同带宽子载波之间的保护频带最低做到单个子载波带宽,频谱利用率当然不会降低。

如果将系统的时频资源理解成一节火车车厢,采用 OFDM 方案生产的话,就相当于火车上只能提供一种固定大小的硬座(子载波带宽)。所有人,不管胖子瘦子、有钱没钱,都只能坐同样大小的硬座。这显然不科学也不够人性化,无法满足人民日益增长的物质文化需要。而 5G 采用 F-OFDM,就相当于可以根据乘客的需求进行座位的灵活定制,硬座、软座、硬卧、软卧、包厢都可以选用,想怎么调整都行,这才是自适应的和谐号列车。

总结一下:F-OFDM 在继承了 OFDM 的全部优点(频谱利用率高、适配 MIMO 等)的基础上,又克服了 OFDM 的一些固有缺陷,进一步提升了灵活性和频谱利用效率,是实现 5G 空口切片的基础技术。

2. 新多址技术 SCMA(Sparse Code Multiple Access)

F-OFDM 解决了业务灵活性问题,还要考虑如何利用有限的频谱,提高资源利用率,容纳更多用户,提升更高吞吐率。有限空间的火车里,如何装更多的人?

要提高资源利用率,哪些域的资源能够进一步复用?我们想到了 LTE 时代没有重用的码域资源。SCMA 技术,引入稀疏码本,通过码域的多址实现了频谱效率的 3 倍提升,相当于有限的火车座位上,坐了更多的用户。如同 4 个同类型的并排座位,坐 6 个人进去挤一挤,这就实现了 1.5 倍的频谱效率提升。

SCMA 的第一个关键技术就是低密度扩频。SCMA 的原理就是把单个子载波的用户数据扩频到 4 个子载波上,然后 6 个用户共享这 4 个子载波。之所以叫低密度扩频,是因为一个用户的数据只占用了其中两个子载波,另外两个子载波是空的。这也是 SCMA 中 Sparse(稀疏)的由来。如果不稀疏,就是在全载波上扩频,那同一个子载波上就有 6 个用户的数据,或者一个用户的数据占用 4 个子载波,冲突太厉害,无法准确解调用户的数据。

4 个座位(子载波)坐了 6 个用户之后,乘客之间就不严格正交了。这是因为每个座位有两个乘客了,没法再通过座位号(子载波)来区分乘客了。单一子载波上还是有 3 个用户

的数据冲突，怎么把一个子载波上的多个用户数据解调出来？

这就需要 SCMA 第二个关键技术：高维调制。因为传统的 IQ 调制只有两维：幅度和相位，高维体现在哪里？如果两个乘客挤在一个座位上，没法再用座位号来区分乘客，但如果给这些乘客贴上不同颜色的标签，结合座位号，还是可以把乘客给区分出来。稀疏码本就是贴在不同用户上的标签，相当于乘客身上不同颜色的标签。高维调制技术是指每个用户的数据在幅值和相位的基础上，使用系统分配的稀疏码本再进行调制，接收端又知道每个用户的码本，这样就可以在不正交的情况下，把不同用户的数据解调出来。

总结一下：SCMA 在使用相同频谱的情况下，通过引入码域的多址，大大提升了频谱效率，通过使用数量更多的载波组，并调整单用户承载数据的子载波（即稀疏度），频谱效率可以提升 3 倍以上。

3. 新编码技术 Polar Code

编码技术的终极目标是香农极限：信道编码的目标，是以尽可能小的开销确保信息的可靠传送。在同样的误码率下，所需要的开销越小，编码效率越高，自然频谱效率也越高。对于信道编码技术的研究者而言，香农极限是无数人皓首穷经、孜孜以求的目标。

香农定理只是说明这类编码存在，可并没有说明什么编码可以达到，这可苦了编码学家们，在过去的半个多世纪中提出了多种纠错码技术，例如 RS 码、卷积码、Turbo 码和 LDPC 码等，并在各种通信系统中进行了广泛应用，但是以往所有实用的编码方法都未能达到香农极限，直到 Polar 码横空出世。

Polar 码基本原理：2007 年，土耳其比尔肯大学教授 Erdal Arikan 首次提出了信道极化的概念，基于该理论，他给出了人类已知的第一种能够被严格证明达到香农极限的信道编码方法，并命名为极化码（Polar Code）。这一突破如一道闪电，划破漫长而又黑暗的夜空，在编码技术史上具有划时代的意义。Polar 码具有明确而简单的编码和译码算法。通过信道编码学者的不断努力，当前 Polar 码所能达到的纠错性能超过目前广泛使用的 Turbo 码和 LDPC 码。

要理解 Polar 码，首先要理解信道极化的概念。信道极化，顾名思义就是信道出现了两极分化，是指针对一组独立的二进制对称输入离散无记忆信道，可以采用编码的方法，使各个子信道呈现出不同的可靠性，当码长持续增加时，一部分信道将趋向于完美信道（无误码），而另一部分信道则趋向于纯噪声信道。事实上，Polar Code 在使用改进后的 SCL（Successive Cancelation List）译码算法时能以较低复杂度的代价，接近最大似然译码的性能。

总结下 Polar 码的优点，首先是相比 Turbo 码更高的增益，在相同的误码率前提下，实测 Polar 码对信噪比的要求比 Turbo 低 0.5～1.2dB，更高的编码效率等同于频谱效率的提升。其次，Polar 码得益于汉明距离和 SC 算法设计，因此没有误码平层，可靠性相比 Turbo 大大提升（Turbo 采用的是次优译码算法，所以有误码平层），对于 5G 超高可靠性需求的业务应用，能真正实现 99.999%的可靠性，解决垂直行业可靠性的难题。第三，Polar 码的译码采用了基于 SC 的方案，因此译码复杂度也大大降低，这样终端的功耗就大大降低了，在相同译码复杂度情况下相比 Turbo 码可以降低功耗 20 多倍，对于功耗十分敏感的物联网

传感器而言,可以大大延长电池寿命。

3.4.3 大规模 MIMO 技术

1. 大规模天线阵列

MIMO 就是"多进多出"(Multiple-Input Multiple-Output),多根天线发送,多根天线接收。Massive MIMO(大规模天线阵列,也称 Large Scale MIMO)是 5G 中提高系统容量和频谱利用率的关键技术。Massive MIMO 带来很大的阵列增益,能够有效提升每个用户的信号质量,提升数据速率和链路可靠性。我们可以从天线数和信号覆盖的维度两方面来理解。

1) 天线数

传统的 TDD 网络的天线基本是 2 天线、4 天线或 8 天线;而到了 5G,受益于高频段技术、芯片技术以及并行计算能力的突破性发展,天线的通道数目大幅度增加,Massive MIMO 通道数达到 64/128/256。

2) 信号覆盖的维度

传统的 MIMO 称为 2D-MIMO,以 8 天线为例,实际信号在做覆盖时,只能在水平方向移动,垂直方向是不动的,信号类似一个平面发射出去,而 Massive MIMO,是信号水平维度空间基础上引入垂直维度的空域进行利用,信号的辐射状是个电磁波束。Massive MIMO 是三维 3D-MIMO。

2. Massive MIMO 技术优势

大规模天线阵列的基础技术有三大类:大规模天线阵子阵列、多波束、多频段。

大规模天线,会给 5G 系统的性能带来哪些好处?不外乎增加系统覆盖、提高系统容量、提高用户峰值速率、增加链路质量。这些好处是由下面各种类型的增益带来的。

首先是阵列增益,大小和天线个数 M 的对数 $\lg(M)$ 强相关。在单天线发射功率不变的情况下、增加天线个数,利用各天线上信号的相关性和噪声的非相关性,使接收端通过多路信号的相干合并,获得平均信噪比(SNR)的增加,从而改善系统的覆盖性能。

还有分集增益。同一路信号经过不同路径到达接收端,利用各天线上信号深衰落的不相关性,减少合并后信号的衰落幅度,可以对抗多径衰落,从而减少接收端信噪比的波动。独立衰落的分支数目越大,接收端的信噪比波动越小,分集增益越大。分集增益,可以改善系统的覆盖,增加链路的可靠性。

空间复用增益。在相同发射功率、相同带宽的前提下,通过增加空间信道的维数,让多个相互独立的天线并行地发送多路数据流,可以提高极限容量和改善峰值速率。这个容量的增长和峰值速率的提升就是空间复用增益。

干扰抑制增益。在多天线收发系统中,空间存在的干扰有一定的统计规律性,利用信道估计的技术,选择合适的干扰抑制算法,可以降低接收端的干扰,提高信噪比。干扰抑制可以改善系统覆盖,提高系统容量,增加链路可靠性,但是对峰值速率没有贡献。

从理论上看,天线数越多越好,系统容量也会成倍提升。但是天线规模增大,对芯片计算能力、工艺水平的要求呈指数级增长,对同步精度的要求也会增加,付出的成本也会大幅提升,所以现阶段天线数目最大是 256 个。

5G Massive MIMO 天线的使用可以带来下列好处。

(1) 提供丰富的空间资源,支持空分多址 SDMA。

(2) 相同的时频资源在多个用户之间复用,提升频谱效率。

(3) 同一信号有更多可能的到达路径,提升了信号的可靠性。

(4) 抗干扰能力强,降低了对周边基站的干扰。

(5) 窄波束可以集中辐射更小的空间区域,减少基站发射功率损耗。

(6) 提高小区峰值吞吐率、小区平均吞吐率、边缘用户平均吞吐率。

3. Massive MIMO 场景部署方案

Massive MIMO 适用于城区宏蜂窝小区和微小区联合部署的场景。微小区为大部分用户提供服务,而中心基站部署大规模天线为微小区范围外的用户提供服务。中心宏基站对微小区进行控制和调度。

根据不同场景需求配置不同的广播和控制信道波束,以匹配多种多样的覆盖场景。

(1) 广场覆盖:近点使用宽波束,保证接入;远点使用远波束,提升覆盖。

(2) 高楼场景:使用垂直面覆盖比较宽的波束,提升垂直覆盖范围。

(3) 混合场景:既有广场又有高楼,采用水平、垂直覆盖角度都比较大的波束。

(4) 区间干扰场景:可以使用水平扫描范围相对窄的波束,避免强干扰源。

3.4.4 毫米波无线通信技术

1. 毫米波技术简介

顾名思义,毫米波是波长 (λ) 约为 1mm(更准确地说是 1～10mm)的电磁波。使用公式 $f=c/\lambda$ 将该波长转换为频率,其中,c 是光速,得出的频率范围为 30～300GHz。毫米波频段被国际电信联盟 ITU 指定为“极高频”(EHF) 频段。术语“毫米波”也经常缩写为“mmWave”。

全球 5G 网络频段分为 Sub-6GHz 和毫米波,而我国在 5G Sub-6GHz 网络建设基本成熟的情况下,将 5G 毫米波网络建设提上了日程。有些人可能会有疑问,既然 Sub-6GHz 和毫米波都能实现 5G,Sub-6GHz 已经成熟,为何要多此一举地建设毫米波呢?

其实毫米波与 Sub-6GHz 能形成互补关系,5G 毫米波的频段为 24～86GHz,是 Sub-6GHz 频段的 16 倍左右,因此传输速度和内容都会快很多;同样因为高频段,5G 毫米波的传播范围也比 Sub-6GHz 小很多。因此 5G 毫米波适合在车站、机场、体育场这些同一区域、同一时间、大量用户的场景使用,而 Sub-6GHz 适合在距离远且空旷的场合使用。

2. 毫米波优点和缺点

毫米波频率高、波长短,具有如下优点。

(1) 波束窄、方向性好,以直射波的方式在空间进行传播,典型的视距传输。在相同天线尺寸下毫米波的波束要比微波的波束窄得多。具有极高的空间分辨力、跟踪精度较高。在电子对抗中,通信系统使用毫米波窄波束,敌方难以截获。

(2) 可用频谱大、支持超大带宽。毫米波有上吉赫兹(GHz)的连续可用频谱。配合各种多址复用技术的使用可以极大提升信道容量,适用于高速多媒体传输业务。

(3) 由于频段高,干扰源很少,具有高质量、恒定参数的无线传输信道。

(4) 对沙尘和烟雾具有很强的穿透能力,几乎能无衰减地通过沙尘和烟雾。激光和红

外在沙尘和烟雾的环境中传播损耗相当大,而毫米波在这样的环境中却有明显优势。

(5) 天线尺寸很小,易于在较小的空间内集成大规模天线阵列。

毫米波的缺点也非常明显。

(1) 相对于微波来说,由于频率高,在大气中传播衰减严重。无线电波频率升高一倍,大气中的传播损耗增加6dB,所以毫米波在大气中衰减严重。降雨衰减大,降雨的瞬间强度越大、雨滴越大,所引起的衰减也就越严重。毫米波的单跳通信距离相对于微波来说较短。

(2) 毫米波器件加工精度要求高。与微波雷达相比,毫米波的元器件目前批量生产成品率低。再加上许多器件在毫米波频段均需涂金或者涂银,因此器件成本较高。

3. 毫米波5G应用场景

最适合部署5G毫米波的场景可以用四个字概括,"热点覆盖"。五个适合部署5G毫米波的场景如下。

(1) 企业室内场景:可以成为Wi-Fi的很好补充,下行链路突发数据可达5Gb/s,比Wi-Fi AP更快更方便。

(2) 大型场馆:例如体育场、音乐厅、展览馆等,高通在超级碗的案例说明,在大型体育场里,5G毫米波可以实现4G LTE二十倍的网络速率。

(3) 交通枢纽:例如地铁站、火车站、飞机场等。

(4) 固定无线接入:也就是用5G毫米波替代光纤实现高速宽带的接入,之前高通在乡村环境测试,用5G毫米波可以实现10km距离1Gb/s的高速连接。

(5) 工业互联网:工业制造环境里常常部署非常多的传感器,设备接入量大,工业控制对时延要求也极为严苛,5G毫米波大带宽、低时延、大容量、高稳定的特性,可以很好地满足工业互联网应用的各种需求。

3.4.5 同时同频全双工技术

同时同频全双工(Co-time Co-frequency Full Duplex, CCFD)技术是指通信系统的发射机和接收机使用相同的时频资源进行通信,即上下行信号可以在相同时间、相同频率里发送。通信结点实现同时同频双向通信,频谱资源的使用更加灵活,突破了现有的频分双工(FDD)和时分双工(TDD)模式。

为了避免发射机信号对接收机信号在频域或时域上的干扰,同频同时全双工技术采用了干扰消除的方法,减少传统TDD或FDD双工模式中频率或时隙资源的开销,从而将无线资源的使用效率提升近一倍。

所有同时同频发射结点对于非目标接收结点都是干扰源,同时同频的发射信号对本地接收机来说是强自干扰,尤其是在多天线及密集组网的场景下(当然仍存在相邻小区的同频干扰问题)。因此,同时同频全双工系统的应用关键在于发射端对接收端的自干扰的有效消除。

根据干扰消除方式和位置的不同,有三种自干扰消除技术:天线干扰消除、射频干扰消除和数字干扰消除。

1. 天线干扰消除

天线干扰消除的方法是指将发射天线与接收天线在空间分离,使得两路发射信号在接收天线处相位相差180°的奇数倍,这样可以使两路自干扰信号在接收点处对消。相位相差

180°，可以通过调整天线的布放位置实现，也可以通过在发射点或接收点安装相反转器件来实现。

2. 射频干扰消除

射频干扰消除的方法就是在发射端将发射信号一分为二，一路发射出去，另一路作为干扰参考信号，通过反馈电路将信号的幅值和相位调节后送到接收端，在接收端的信号中把干扰信号减去，实现自干扰信号的消除。

3. 数字干扰消除

数字干扰消除是将发射机的基带信号通过数字信道估计器和数字滤波器，在数字域模拟空中发射信号到达接收点的多径无线信号，在接收点完成干扰对消。

5G 要实现同一信道上同时接收和发送，主要有以下三大挑战。

(1) 电路板件设计。自干扰消除电路需满足宽频(大于 100MHz)和多 MIMO(多于 32 个天线)的条件，且要求尺寸小、功耗低以及成本不能太高。

(2) 物理层、MAC 层的优化设计问题。例如编码、调制、同步、检测、侦听、冲突避免、ACK 等，尤其是针对 MIMO 的物理层优化。

(3) 对全双工和半双工之间动态切换的控制面优化，以及对现有帧结构和控制信令的优化问题。

3.5 窄带物联网技术

以 LoRa、NB-IoT 为代表的低功耗广域网 LPWAN 技术近年来已经是物联网领域最热门的部分。

3.5.1 NB-IoT

1. NB-IoT 概述

NB-IoT(Narrow Band Internet of Things)是一种基于蜂窝的窄带物联网技术，也是低功耗广域物联网(LPWAN)的最佳连接技术之一，承载着智慧家庭、智慧出行、智慧城市等智能世界的基础连接任务，广泛应用于如智能表计、智慧停车、智慧路灯、智慧农业、白色家电等多个方面，是智能时代下的基础连接技术之一。

2020 年，NB-IoT 全球连接数超 1 亿。根据预测，这一技术将在未来 5 年实现 10 亿级连接，并持续保持增长趋势，推动物联网设备实现爆发性成长。

NB-IoT 技术标准最早是由华为和沃达丰主导提出来的，之后又吸引了高通和爱立信等一些厂家。从一开始的 NB-M2M 经过不断的演进和研究，在 2015 年的时候演进为 NB-IoT。在 2016 年的时候，NB-IoT 的标准就正式被冻结了。当然，NB-IoT 的标准依然在持续的演进当中，在 2017 年的 R14 当中就新增了许多特性，到了 R14 版本，NB-IoT 具有了更高的速率，同时也支持站点定位和多播业务。在 2020 年 7 月 9 日最新召开的会议上，NB-IoT 这项技术已经被正式接纳为 5G 的一部分了。但是由于现阶段的 NB-IoT 并不支持接入 5G 网络，所以该技术在后续还需要经过不断的演化和技术的演进才能进入 5G 网络当中。

2. NB-IoT技术特点和优势

1) 广覆盖(比GSM覆盖提高20dB)

NB-IoT与GPRS或LTE相比,在同样的频段下,最大链路预算提升了20dB,覆盖面积相当于扩大了100倍,并将提供改进的室内覆盖,即使在地下车库、地下室、地下管道等普通无线网络信号难以到达的地方也容易覆盖到。NB-IoT实现高覆盖的原因主要包括两个方面:①上行功率谱密度增强了17dB;②覆盖+编码为6～16dB。

2) 大连接

具备支撑海量连接的能力,NB-IoT基站的单扇区可支持超过5万个终端与核心网的连接,窄带技术,上行等效功率提升,大大提升信道容量。比现有2G、3G、4G移动网络用户有50～100倍容量提升。支持低延时敏感度、超低的设备资本、低设备功耗和优化的网络架构。

3) 低耗能(基于AA电池,使用寿命可超过10年)

NB-IoT可以让设备一直在线,通过减少不必要的信令、更长的寻呼周期及终端进入PSM(节能模式)状态等机制来达到省电的目的。

4) 低成本

低速率、低功耗、低带宽可以带来终端的低复杂度,便于终端做到低成本。同时,NB-IoT基于蜂窝网络,可直接部属于现有的LTE网络,运营商部署成本也比较低。

5) 授权频谱

NB-IoT可直接部属于LTE网络,也可以利用2G、3G的频谱重耕来部署,无论是数据安全和建网成本,还是在产业链和网络覆盖,相对于非授权频谱都具有很强的优越性。

6) 安全性

继承4G网络安全的能力,支持双向鉴权和空口严格的加密机制,确保用户终端在发送接收数据时的空口安全性。

3. NB-IoT网络体系架构

传统的LTE网络体系架构,其目的是给用户提供更高的带宽、更快的接入,以适应快速发展的移动互联网需求。但在物联网应用方面,由于UE数量众多、功耗控制严格、小数据包通信、网络覆盖分散等特点,传统的LTE网络已经无法满足物联网的实际发展需求。

NB-IoT系统网络架构和LTE系统网络架构相同,都称为演进的分组系统(Evolved Packet System,EPS)。EPS主要包括3个部分,分别是演进的核心系统(Evolved Packet Core,EPC)、基站(eNodeB,eNB)、UE。eNB基站负责接入网部分,即无线接入网。NB-IoT无线接入网由一个或多个基站eNB组成,eNB基站通过Uu接口(空中接口)与UE通信。EPC负责核心网部分,通过全IP连接的承载网络,对所有的基于IP的业务都是开放的,能提供所有基于IP业务的能力集。

NB-IoT典型的端到端组网,如图3-13所示,主要包括4部分:终端、接入网、核心网和云平台。其中,终端与接入网之间是无线连接,即NB-IoT,其他几部分之间一般是有线连接。

NB-IoT终端:用户终端UE,通过空口连接到基站eNodeB。

eNodeB无线网侧:包括两种组网方式,一种是整体式无线接入网(Singel RAN),其中包括2G/3G/4G以及NB-IoT无线网;另一种是NB-IoT新建网、主要承担空口接入处理、

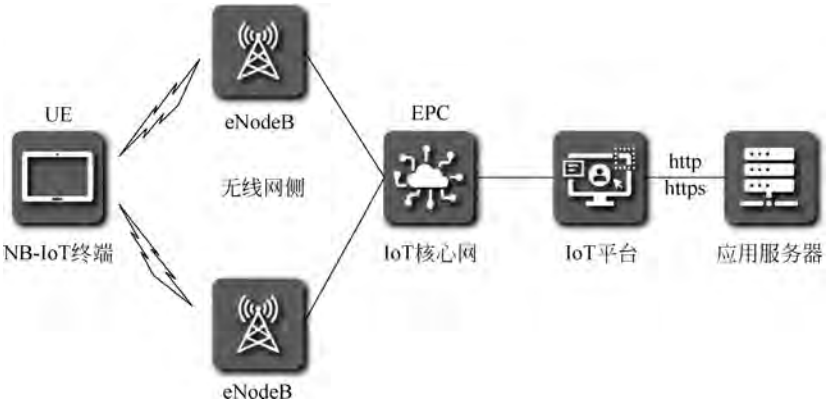

图 3-13　NB-IoT 端到端组网

小区管理等相关功能，并通过 S1-LITE 接口与 IoT 核心网连接，将非接入层数据转发给高层网元处理。这里，NB-IoT 可以独立组网，也可以与 E-UTRAN 融合组网。

IoT 核心网 EPC：EPC 承担与终端非接入层交互的功能，并将 IoT 业务相关数据转发到 IoT 平台进行处理。既可以独立组网，也可以与 LTE 共用核心网。

IoT 平台：汇聚从各种接入网得到的 IoT 数据，并根据不同类型转发至相应的业务应用进行处理。

应用服务器：是 IoT 数据的最终汇聚点，根据客户的需求进行数据处理等操作。

3.5.2　LoRa

1. LoRa 概述

LoRa 是 Long Range 的简称，意思是长距离通信，作为 LPWAN 通信技术的一种，是美国 Semtech 公司采用和推广的一种基于扩频调制技术（Chirp Spread Spectrum，CSS）的超远距离无线传输方案。

扩频技术是一种用宽带换取灵敏度的技术，Wi-Fi、ZigBee 等技术都使用了扩频技术，但是 LoRa 调制的特点是可以最大效率地提高灵敏度，以至于接近香农定理的极限。尤其是在低速率通信系统中，打破了传统的 FSK 窄带系统的实施极限。

LoRa Alliance 联盟与 2015 年由 Cisco、IBM 和 Semtech 等多家厂商共同发起创立。LA 联盟制定了 LoRa WAN 标准规范，主要完成的是 MAC 层规范以及物理层相关参数的约定。LoRa WAN 是为 LoRa 远距离通信网络设计的一套通信协议和系统架构。

CLAA（China LoRa Application Alliance）物联网生态圈是中国 LoRa 产业链的主导者。目前已经发展成为从 LoRa 芯片、模组、终端、系统集成商到解决方案提供商，以及互联网企业、电信运营商广泛参与的产业共同体。

2. LoRa 技术特点

1）远距离

现在已经有多家卫星公司吧 LoRa 发射到了近地卫星上，一般近地卫星距离地面 600～2000km。LoRa 传感器可以放置在地球的任意角落（室外屋顶不遮挡），都可以将数据传输到卫星上，并通过地面接收站，最终数据进入互联网和服务器中。

2) 抗干扰能力强

LoRa具有低于噪声20dB正常调解信号,而FSK理论上需要在噪声之上8dB才能保证调解。LoRa调制之所以有这么强的抗干扰能力,主要是因为Chirp调制在相干调解的时候可以把在噪声之下有用的LoRa信号聚集在一起,而噪声在相干调解后还是噪声。所以在一些信道干扰比较严重的区域,客户都会选择LoRa技术作为稳定通信的核心技术。

3) 低功耗

LoRa技术最主要的应用是物联网,而物联网对于终端设备的使用寿命的要求非常高。这就要求LoRa技术在应用时具有超低的功耗。超低功耗的实现主要由两方面决定,一方面芯片的硬件要具备低功耗,另一方面应用协议也要具备低功耗。

4) 大容量

LoRa WAN的网络容量决定因素很多,主要与以下几个参数相关:结点的发包频率、数据包的长度、信号质量及结点的速率、可用信道数量、基站/网关的密度、信令开销、重传次数等。LoRa WAN协议的大容量是部署广域网的必要条件,广域网为去碎片化提供了有力支撑。一般情况下,一个智慧城市的项目中,中大型城市需要几百个LoRa网关来实现室外全覆盖;在智慧社区的项目中,一个工业园区或一个住宅小区使用1~4个中小型LoRa网关可以实现全覆盖。

5) 按需部署、独立组网

LoRa就是一个"长Wi-Fi"技术,其部署特点与Wi-Fi非常相似。LoRa的部署过程也很简单,只需要选择一个网关部署位置,连接网线和电源线即可。在没有网线连接的地方可以利用运营商的4G网络或本地的Wi-Fi无线网络完成LoRa网络部署。

在实际的物联网应用中,在运营商信号覆盖比较差的地方,如密集的居民楼、井盖内或者复杂的地下管道,可以根据具体需求进行LoRa网络架设。

6) 轻量级、低成本

一个项目能否成功,成本是非常关键的因素。LoRa技术是一个轻量级的技术,LoRa WAN协议也是一个轻量级的物联网通信协议。LoRa硬件在设计之初就充分考虑到了物联网市场对成本的苛刻要求以及对整体部署的要求。

3. LoRa网络系统

LoRa WAN网络系统由4部分组成,分别是终端结点(End Nodes)、网关、网络服务器(Network Server)、应用服务器(Application Server),如图3-14所示。其中,终端结点也叫终端设备(End Device)、传感器(Sensor)或者结点(Nodes);网关也可以叫集中器(Concentrator)或者基站(Base Station)。由于LoRa WAN应用于物联网中,所以服务和连接的对象是终端结点,对应于移动通信网络中的用户(也叫移动台)。LoRa WAN中网关对应于移动通信网络中的基站;LoRa WAN中的网络服务器对应于移动通信网中的移动交换中心(MSC)或移动台辅助切换(MAHO);而LoRa WAN中的网关与网络服务器之间的连接方式采用3G/4G等移动通信网络或以太网网线连接的方式,对应于移动通信网络中的公众通信网(PSTN、PSDN)。根据应用和服务不同,LoRa WAN网络系统需要应用服务器的支持,它是LoRa WAN系统组成的必要部分,而移动通信网络中并非必要组成项。这是因为LoRa WAN的结点一定是为了满足某种业务而存在,几乎不存在没有服务业务而挂在网上的情况。这个情况与移动通信网络不同,移动通信服务的目的是让用户一直连接在

网络上，对于运行什么业务并不关心。这也是物联网的网络系统与移动通信网系统的重要差别之一。

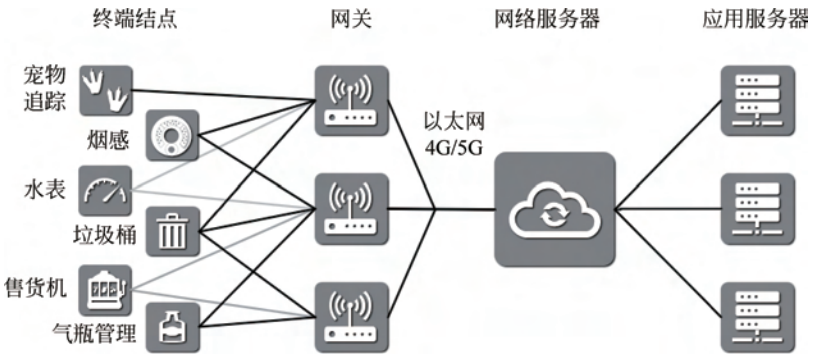

图 3-14　LoRa WAN 的系统组成

在 LoRa WAN 中，终端结点通过 LoRa 无线通信与网关连接，网关通过现有的有线/无线网络（以太网/蜂窝网）与网络服务器连接，网络服务器再通过以太网与应用服务器连接。一次通信过程可以是终端结点发起或由应用服务器发起，网关和网络服务器只是实现透传和网络管理的工作，与业务没有直接关系。LoRa WAN 网关只是不断接收结点发来的数据并传给网络服务器，而网络服务器会整理数据发往应用服务器；应用服务器收到结点的业务数据后，响应应答指令发往网络服务器，网络服务器管理网关下发命令到达原业务结点。

从 LoRa WAN 的系统与移动通信网系统的类比中，可以发现两个系统的构造非常相似，不过在网络连接上有以下几点不同。

（1）终端结点与网关的连接方式不同。从图中可以看出，有的终端结点（图中宠物追踪）与一个 LoRa WAN 网关的连接，有的终端结点（图中水表）同时连接两个网关，而有的终端结点（图中的垃圾桶）连接三个网关。这与移动通信网系统中一个用户连接一个网关的方式完全不同。

（2）网关与网关间的连接不同。在移动通信网中，每个区域的 MSC 管理 BSS 中的多个基站，而 LoRa WAN 网络系统中所有的网关之间是独立的，没有任何关系，不需要做频率分配，也不要做跨网管理。

（3）网关与网络服务器的连接不同。移动通信网中由于系统对于网络的稳定性要求很高，对于上下行通信延迟要求非常高，一般通过光纤交换进行快速数据交互，其延迟在几毫秒；而 LoRa WAN 采用传统的网线或 3/4G 网络作为连接数据交互手段，这样的网络延迟和稳定性很差，数据交互经常需要上百毫秒。

4. LoRa 的标准及规范

本节针对 LoRa 应用的一些标准和规范进行介绍，其中，LoRa WAN 协议标准是重点部分。由于 LoRa WAN 协议在一些高速响应或结点间通信应用中仍然存在一些问题，因而出现了一些协议的更新和创新，其中包括中继 Relay 协议，阿里巴巴推广的 LoRa D2D 协议等。这些协议都是基于 LoRa WAN 协议的创新，都是在兼容原有 LoRa WAN 协议的前提下的协议创新。Yosmart 公司开发的 YoLink 协议是一个吸收了 LoRa WAN、Dash 7 等多种协议优点的智能家居协议，既具有 LoRa WAN 的网络优势，又具有智能家居的快速响

应的优势。

LoRa WAN协议分为基础类型Class A和可选功能类别Class B、Class C。

1) Class A(双向传输终端)

Class A的终端在每次上行后都会紧跟两个短暂的下行接收窗口,以此实现双向传输。终端基于自身通信需求来安排传输时隙,在随机时间的基础上具有较小的变化(属于随机多址ALOHA协议)。这种Class A操作为应用提供了最低功耗的终端系统,只要求应用在终端上行传输后的很短时间内进行服务器的下行传输。服务器在其他任何时间进行的下行传输都需要等待终端的下一次上行。通常用于低功耗的物联网设备,如水表、气表、烟感、门磁等多种传感器。

2) Class B(划定接收时隙的双向传输终端)

Class B的终端会有更多的接收时隙。除了Class A的随机接收窗口,Class B设备还会在指定时间打开另外的接收窗口。为了让终端可以在指定时间打开接收窗口,终端需要从网关接收时间同步的信标(Beacon)。这使得服务器可以知道终端何时处于监听状态。一般应用于下行控制且有低功耗需求的场景,如水闸、气闸、门锁等。

3) Class C(最大化接收时隙的双向传输终端)

Class C的终端一直打开着接收窗口,只在发送时短暂关闭。Class C的终端会比Class A和Class B更加耗电,但同时从服务器下发给终端的时延也是最短的。一般Class C用于长带电的场景,如电表、路灯等。

学习Class A/B/C的时候经常忘记其特征,这里的A代表英文单词“All”,意思就是所有的LoRa WAN终端都必须满足Class A的规定;B代表英文单词“Beacon”;C代表英文单词“Continuous”。

3.6 无线移动局域网安全技术

无线局域网与传统有线局域网相比优势不言而喻,它可实现移动办公,其架设与维护更容易,但在巨大的应用与市场面前,无线局域网络的安全问题就显得尤为重要。在传统的有线网络上,一个攻击者可以物理接入到有线网络内或设法突破边缘防火墙或路由器。对一个无线网络而言,所有潜在的无线攻击者只需要携带其可移动设备待在一个舒服的位置,用无线嗅探软件就可展开工作。

无线局域网面临的主要安全威胁包括:非授权用户、地址欺骗、会话欺骗和高级入侵等。

1. 非授权用户

由于无线局域网的开放式访问方式,在一个AP所覆盖的区域中,包括未授权的客户端都可以接收到此AP的电磁波信号。未授权用户非法获取SSID(Service Set Identifier),就可以接入无线局域网,从而未经授权而擅自使用网络资源,占用宝贵的无线信道资源,增加带宽费用,降低合法用户的服务质量。

2. 地址欺骗和会话拦截

在无线环境中,入侵者也可以首先通过窃听获取授权用户的MAC地址,然后篡改自己计算机的MAC地址而冒充合法终端。另外,由于IEEE 802.11没有对AP身份进行认证,非法用户很容易装扮成AP进入网络,并进一步获取合法用户的鉴别身份信息,通过会话拦

截实现网络入侵。

3. 高级入侵

一旦攻击者进入无线网络，它将成为进一步入侵其他系统的起点。多数企业部署的WLAN都在防火墙之后，这样WLAN的安全隐患就会成为整个安全系统的漏洞，只要攻破无线网络，就会使整个网络暴露在非法用户面前。

3.6.1 加密技术

加密技术的基础是密码学。密码学为系统、网络、应用安全提供密码机制，是诸多网络安全机制的基石。密码学旨在发现、认识、掌握和利用密码内在规律，由密码编码学(Cryptography)和密码分析学(Cryptanalysis)两部分组成。

根据密钥数量和工作原理的不同，现代密码系统通常可划分为对称密钥密码系统和公开密钥密码系统两类。

1. 对称密钥密码系统

对于对称密钥密码系统，加密密钥和解密密钥完全相同，这种密码系统也称为单钥密码系统或秘密密钥密码系统。

对称密钥密码系统对明文信息加密主要采用序列密码(Stream Cipher)和分组密码(Block Cipher)两种形式。

典型的对称密钥密码系统有：DES、AES和RC4。

数据加密标准(Data Encryption Standard，DES)是一种分组密码，对二进制数据加密，明文分组的长度为64位，相应产生的密文分组也是64位。DES加密流程可以划分为初始置换、子密钥生成、乘积变换、逆初始置换等步骤。DES的解密与加密使用的是相同算法，仅仅在子密钥的使用顺序上存在差别。在DES的基础上，研究人员提出了3DES算法，增加了密钥长度。3DES算法使用3个密钥，并执行3次DES运算，遵循“加密-解密-加密”的工作流程。

高级数据加密标准(Advanced Encryption Standard，AES)是分组大小为128b的分组密码，支持密钥长度为128b、192b和256b。AES算法又称Rijndael算法。AES算法采用替换/转换网络，每轮包含三层。线性混合层：通过列混合变换和行移位变换确保多轮密码变换之后密码的整体混乱和高度扩散。非线性层：字节替换，由16个S-盒并置而成，主要作用是字节内部混淆。轮密钥加层：简单地将轮(子)密钥矩阵按位异或到中间状态矩阵上。

RC4(Rivest Cipher 4)是一种流密码算法。RC4具有算法简单，运算速度快，软硬件实现十分容易等优点，使其在一些协议和标准里得到了广泛应用。如IEEE 802.11无线局域网安全协议WEP与WPA中均使用了RC4算法。

2. 公开密钥密码系统

典型的密钥密码系统：RSA密码体制、ElGamal公钥密码体制度、椭圆曲线密码体制、基于身份的密码体制，以及Diffie-Hellman密钥交换协议。

RSA公钥密码系统基于“大数分解”这一著名数论难题。将两个大素数相乘十分容易，但要将乘积结果分解为两个大素数因子却极端困难。

椭圆曲线密码(Elliptic Curve Cryptography，ECC)以椭圆曲线为基础，利用有限域上

椭圆曲线的点构成的Abel群离散对数难解性,实现加密、解密和数字签名,将椭圆曲线中的加法运算与离散对数中模乘运算相对应,就可以建立基于椭圆曲线的对应密码体质。ECC的主要优势是密钥小,算法实施方便,计算速度快,非常适用于无线应用环境,而且安全性也能与RSA相当。

3.6.2 认证技术

认证或鉴别(Authentication)是信息安全领域的一项重要技术,主要用于证实身份合法有效或者信息属性名副其实。身份认证是最常见的一种认证技术,可以确保只有合法用户才能进入系统。其次是消息认证,在网络通信过程中,黑客常常伪造身份发送信息,也可能对网络上传输的信息内容进行修改,或者将在网络中截获的信息重新发送。因此要验证信息的发送者是合法的,即信源的认证和识别;验证消息的完整性,即验证信息在传输和存储过程中是否被篡改;验证消息的顺序,即验证是否插入了新的消息、是否被重新排序、是否延时重放等。最后,在通信过程中,还需要解决通信双方互不信任的问题,如发送方否认消息是自己发送的,或接收方伪造一条消息谎称是发送方发送的,这就需要用到数字签名技术。

1. 身份认证

身份认证可以基于以下四种与用户有关的内容之一或它们的组合实现。

(1) 所知:个人所知道的或所掌握的知识或信息,如密码、口令。

(2) 所有:个人所具有的东西,如身份证、护照、信用卡、智能门卡等。

(3) 所在:个人所用的机器的IP地址、办公地址等。

(4) 用户特征:主要是个人生物特征,如指纹、笔迹、声纹、手形、脸形、视网膜、虹膜、DNA,还有个人的一些行为特征,如走路姿势、按键动作等。

目前,身份认证技术主要包括口令认证、信物认证、地址认证、用户特征认证和密码学认证。

2. 消息认证

消息认证也称为“消息认证”“消息鉴别”。以下介绍消息属性的主流认证方法。

1) 报文源的认证

报文源的认证是指认证发送方的身份,确定消息是否由所声称的发送方发送而来。

2) 报文宿的认证

报文宿的认证是对报文接收方的身份进行认证。具体来看,它指的是消息的接收方在接收到报文以后判断报文是否是发送给自己的。

3) 报文内容的认证

报文内容的认证是指接收方在接收到报文以后对报文进行检查,确保自己接收的报文与发送方发送的报文相同,即报文在传输过程中的完整性没有受到破坏也称为“完整性检测”。

4) 报文顺序的认证

报文的发送顺序在通信中具有重要的安全意义。重放攻击就是攻击者对报文顺序的一种攻击方式。对报文顺序进行认证,最重要的一点就是在通信中增加标识报文顺序的信息。报文顺序信息可以多种形式出现,如序列号、时间戳等。

3. 数字签名

前面介绍的报文认证可以保护信息交换双方不受第三方的攻击，但是它不能处理通信双方自己产生的攻击。在收发双方不能完全相互信任的情况下，就需要除报文认证之外的其他方法来解决问题。这就需要数字签名技术。可以使用RSA密码系统实现数字签名，可以使用ElGamal密码系统实现数字签名，也可以使用椭圆曲线密码实现数字签名。

3.6.3 密钥交换技术

对称加密算法解决了数据加密的问题。以AES加密为例，在现实世界中，用户A要向用户B发送一个加密文件，A可以先生成一个AES密钥，对文件进行加密，然后把加密文件发送给对方。因为对方要解密，就必须需要A生成的密钥。现在问题是：如何传递密钥？在不安全的信道上传递加密文件是没有问题的，因为黑客拿到加密文件没有用。但是，如何在不安全的信道上安全地传输密钥？要解决这个问题，密钥交换算法Diffie-Hellman应运而生。

Diffie-Hellman密钥交换算法（简称“DH算法”或“DH交换”）由Whitfield Diffie和Martin Hellman于1976年提出，是最早的密钥交换算法之一。它使得通信的双方能在非安全的信道中安全地交换密钥，用于加密后续的通信消息。DH算法解决了密钥在双方不直接传递密钥的情况下完成密钥交换，这个神奇的交换原理完全由数学理论支持。Diffie-Hellman算法的有效性依赖于计算离散对数的难度。

下面简要看一下DH算法交换密钥的步骤。假设甲乙双方需要传递密钥，他们之间可以这么做：甲首先选择一个素数 p，例如509；底数 g，任选，例如5；随机数 a，例如123，然后计算 $A=g^a \bmod p$，结果是215；然后，甲发送 $p=509$，$g=5$，$A=215$ 给乙；乙收到后，也选择一个随机数 b，例如456，然后计算 $B=g^b \bmod p$，结果是181，乙再同时计算 $s=A^b \bmod p$，结果是121；乙把计算的 $B=181$ 发给甲，甲计算 $s=B^a \bmod p$ 的余数，计算结果与乙算出的结果一样，都是121。所以最终双方协商出的密钥 s 是121。注意到这个密钥 s 并没有在网络上传输。而通过网络传输的 p，g，A 和 B 是无法推算出 s 的，因为实际算法选择的素数是非常大的。

所以，更确切地说，DH算法是一个密钥协商算法，双方最终协商出一个共同的密钥，而这个密钥不会通过网络传输。

3.6.4 安全体系

无线网络安全体系包含方方面面的技术，例如认证、加密、安全策略、无线入侵检测等。本节主要介绍一下安全策略和无线入侵检测。

网络安全防护是一种网络安全技术，指致力于解决诸如如何有效进行介入控制，以及如何保证数据传输的安全性的技术手段，主要包括物理安全分析技术，网络结构安全分析技术，系统安全分析技术，管理安全分析技术，及其他的安全服务和安全机制策略。

防护措施：①对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限等。②数据加密防护。加密是防护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。③网络隔离防护。网络隔离有两种方式，一种是采用隔离卡来实现

的,一种是采用网络安全隔离网闸实现的。④其他措施。包括信息过滤、容错、数据镜像、数据备份和审计等。

入侵检测系统(IDS)通过分析网络中的传输数据来判断破坏系统和入侵事件。如今,入侵检测系统已用于无线局域网,来监视分析用户的活动,判断入侵事件的类型,检测非法的网络行为,对异常的网络流量进行报警。

无线入侵检测系统同传统的入侵检测系统类似。但无线入侵检测系统加入了一些无线局域网的检测和对破坏系统反应的特性。

无线入侵检测系统有集中式和分散式两种。

集中式无线入侵检测系统通常用于连接单独的 sensors(探测器,俗称探头),搜集数据并转发到存储和处理数据的中央系统中。分散式无线入侵检测系统通常包括多种设备来完成 IDS 的处理和报告功能。分散式无线入侵检测系统比较适合较小规模的无线局域网,因为它价格便宜和易于管理。

无线局域网通常被配置在一个相对大的场所。像这种情况,为了更好地接收信号,需要配置多个无线基站(WAPs),在无线基站的位置上部署 sensors,这样会提高信号的覆盖范围。由于这种物理架构,大多数的黑客行为将被检测到。另外的优点就是加强了同无线基站(WAPs)的距离,能更好地定位黑客的详细地理位置。

3.6.5 典型安全协议

无线网络常见的安全协议有 WEP、TKIP 和 WPA 等。

1. WEP

WEP(Wired Equivalent Privacy,有线等效保密协议)是常见的资料加密措施。WEP 安全技术源自于名为 RC4 的 RSA 数据加密技术,以满足用户更高层次的网络安全需求。在链路层采用 RC4 对称加密技术,当用户的加密密钥与 AP 的密钥相同时才能获准存取网络的资源,从而防止非授权用户的监听以及非法用户的访问。

WEP 的目的是向无线局域网提供与有线网络相同级别的安全保护,它用于保障无线通信信号的安全,即保密性和完整性。当 WEP 提供 40 位长度的密钥机制时,它存在许多缺陷,非法用户往往能够在有限的几个小时内就能将加密信号破解掉。另外,由于同一个无线局域网中的所有用户往往都共享使用相同的一个密钥,只要其中一个用户丢失了密钥,那么整个无线局域网网络都将变得不安全。

2. WPA 保护访问

WEP 存在的缺陷不能满足市场的需要,而最新的 IEEE 802.11i 安全标准的批准被不断推迟,Wi-Fi 联盟适时推出了 WPA(Wi-Fi Protected Access)技术。WPA 使用的加密算法还是 WEP 中使用的加密算法 RC4,所以不需要修改原来无线设备的硬件,其原理为根据通用密钥,配合表示计算机 MAC 地址和分组信息顺序号的编号,分别为每个分组信息生成不同的密钥。然后与 WEP 一样将此密钥用 RC4 加密处理。通过这种处理,所有客户端的所有分组信息所交换的数据将由各不相同的密钥加密而成。WPA 还具有防止数据中途被篡改的功能和认证功能。

WPA 标准采用了 TKIP(Temporal Key Integrity Protocol,临时密钥完整性协议)、EAP(Extensible Authentication Protocol,扩展认证协议)和 802.1X 等技术,在保持 Wi-Fi

认证产品硬件可用性的基础上，解决 IEEE 802.11 在数据加密、接入认证和密钥管理等方面存在的缺陷。因此，WPA 在提高数据加密能力、增强网络安全性和接入控制能力方面具有重要意义。WPA 是一种比 WEP 更为强大的加密方法。作为 IEEE 802.11i 标准的子集，WPA 包含了认证、加密和数据完整性校验三个组成部分，是一个完整的安全性方案。Wi-Fi6 使用最新的 WPA3。

3. WLAN 验证与安全标准——IEEE 802.11i

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，IEEE 802.11 工作组于 2004 年 6 月正式批准了 IEEE 802.11i 安全标准，从长远角度考虑解决 IEEE 802.11 无线局域网的安全问题。IEEE 802.11i 标准主要包含的加密技术是 TKIP 和 AES(Advanced Encryption Standard)，以及认证协议 IEEE 802.1x。定义了强壮安全网络(Robust Security Network，RSN)的概念，并且针对 WEP 加密机制的各种缺陷做了多方面的改进。

IEEE 802.11i 规范了 802.1x 认证和密钥管理方式，在数据加密方面，定义了 TKIP、CCMP(Counter-Mode/CBC2 MAC Protocol)和 WRAP(Wireless Ro2bust Authenticated Protocol)三种加密机制。其中，TKIP 可以通过在现有的设备上升级固件和驱动程序的方法实现，达到提高 WLAN 安全的目的。CCMP 机制基于 AES 加密算法和 CCM 认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。AES 是一种对称的块加密技术，有 128/192/256 位不同加密位数，提供比 WEP/TKIP 中 RC4 算法更高的加密性能，但由于 AES 对硬件要求比较高，因此 CCMP 无法在现有设备的基础上进行升级实现。

小　　结

本章重点讨论了无线局域网和无线广域网的相关技术，主要包括 Wi-Fi、ZigBee、5G、NB-IoT 和 LoRa，以及无线安全技术。

Wi-Fi 是 IEEE 802.11 无线局域网的代名词，其物理层标准主要有 IEEE 802.11b/a/g/n。重点介绍了 Wi-Fi 的主要设备、接入方式、关键技术和 Wi-Fi6。

ZigBee 作为短距离无线技术，以 IEEE 802.15.4 为起点，重点介绍了 ZigBee 的标准、技术特点、协议框架和各层规范。

5G 以无线接入网侧 RAN 为主，重点介绍了 5G 网络的三大应用场景 eMBB、uRLLC 和 mMTC；独立组网(SA)和非独立组网(NSA)；新空口的三大物理层技术 F-OFDM、SCMA 和 Polar 码；以及 Massive MIMO、毫米波、同时同频全双工 CCFD 技术。

NB-IoT 是一种基于蜂窝的窄带物联网技术，也是低功耗广域物联网(LPWAN)通信技术之一。重点介绍了 NB-IoT 的特点和优势，网络体系结构以及端到端的组网。

LoRa 作为 LPWAN 通信技术之一，采用基于扩频调制技术的超远距离无线传输方案。重点介绍了 LoRa 的技术特点、网络系统、标准规范。

无线局域网安全技术是网络的重要安全保障，常见的技术包括加密技术、认证技术、密钥交换技术、安全体系和安全协议等。

习题与实践

1. 填空题

(1) Wi-Fi6 的协议标准是_____,Wi-Fi5 的协议标准是_____。

(2) ZigBee 协议栈包含 5 层,分别是_____,_____,_____,_____和_____。

(3) 5G 蜂窝网络的三大应用场景是_____,_____,_____。

(4) 常见的窄带物联网有_____,_____。

2. 简答题

(1) 简述 Wi-Fi5 和 Wi-Fi6 的主要区别。

(2) 简述 ZigBee 协议框架。

(3) 简述 5G 的新空口技术。

(4) 简述 NB-IoT 的组网方式。

(5) 简述 LoRa 的组网方式。

(6) 简述常见的无线安全协议。

3. 实践

(1) 使用 Wi-Fi6 网络设备,在办公室或寝室组建一个小型的 Wi-Fi 网络。

(2) 进一步了解 5G 移动通信网络的核心网和承载网。