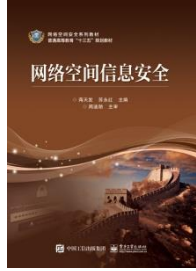
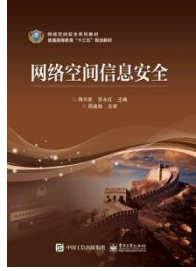


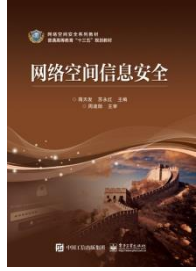
网络空间信息安全

第7章 无线网络安全机制



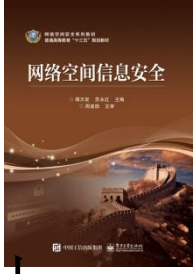
本章主要内容

- 7.1 无线网络
- 7.2 短程无线通信
- 7.3 无线移动通信技术
- 7.4 无线网络结构及实现
- 7.5 无线网络的安全性



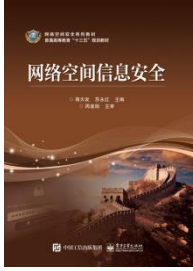
7.1 无线网络

- 通常计算机组网的传输媒介是铜缆和光缆，但有线网络在某些场合中会受到布线的限制：布线、改线工程量大；线路容易损坏；网中的各结点不可移动。特别是当要把相距较远的结点联系起来时，铺设专用通信线路的布线施工难度大、费用高、耗时长，和正在迅速扩大的联网需求形成了严重的矛盾。



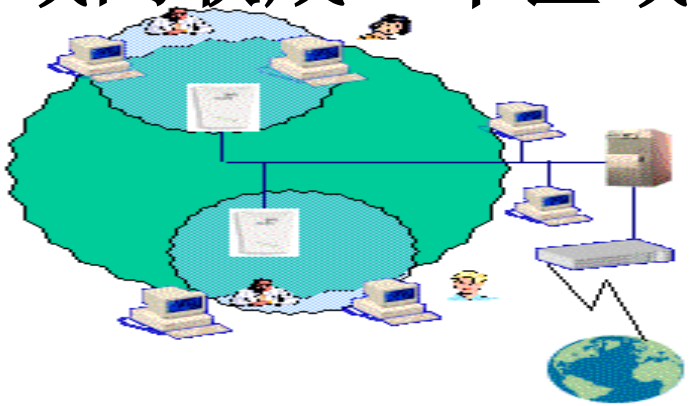
7.1 无线网络

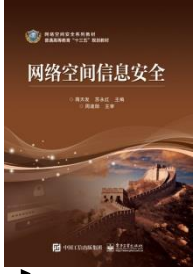
- 解决这一难题迅速和有效的方法是采用新型计算机无线通信和无线计算机网络系统。无线局域网是指以无线信号作为传输媒介的计算机局域网。
- 计算机无线通信和计算机无线联网不是一个概念，其功能和实现技术有相当大的差异。计算机无线通信只要求两台计算机之间能传输数据即可。而计算机无线联网则进一步要求以无线方式相连的计算机之间实现资源共享，具有现有网络操作系统所支持的各种服务功能。



7.1 无线网络

- 计算机无线联网常见的形式是把一个（远程）计算机以无线方式联入一个计算机网络中，作为网络中的一个结点。如图7.1所示，使之具有网上工作站所应该具有的功能，获得网络上所有服务；或把数个（有线或无线）局域网联成一个区域网。

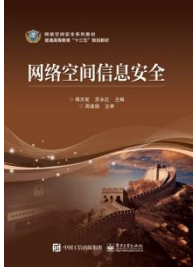




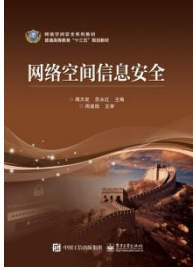
7.1 无线网络

- 整套的计算机无线网络产品是遵照IEEE 802.3以太网协议开发的，它采用以微波频段为媒介的直序扩展频谱或跳频方式发射的传输技术，并将此技术应用于发射、接收机
- 其通信方面的主要技术特点是：用900MHz、2.45GHz或5.85GHz微波作传输媒介，以先进的直序扩展频谱（DSSS）或跳频（FH）方式发射信号。其射频带宽为26MHz。与传统的无线电窄带调制发射方式不同，它采用的是宽带调制发射。故它具有传输速率高（可达11Mbps），发射功率小（只有60-250mw），保密性好，抗干扰能力很强，不会与其他无线电设备及用户发生互相干扰的特点。

7.1.2无线网络的分类

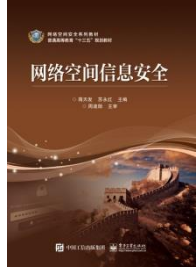


- （1）无线个人网（WPAN）：主要用于个人用户工作空间，典型距离覆盖几米，可以与计算机同步传输文件，访问本地外围设备，如打印机等。无线个域网的通信技术有很多，如蓝牙、红外、HomeRF等。
- （2）低速率无线个域网(LR-WPAN)
- 最重要的技术标准是IEEE 802.15.4协议，它是为了满足低功耗、低成本的无线传感器网络要求而专门开发的低速率WPAN标准。ZigBee协议就是基于这个标准而设立的，它的应用目标主要是：工业控制(如自动控制设备、无线传感器网络)、医护(如监视和传感)、家庭智能控制(如照明、水电气计量及报警)、消费类电子设备的遥控装置、PC外设的无线连接等领域。
- 其他的低速率无线个域网通信技术还有Z-Wave, Insteon, HomePlug等。。



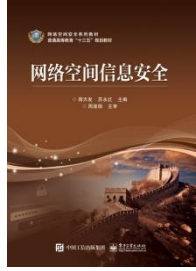
7.1 无线网络

- （3）无线局域网（WLAN）：主要用于宽带家庭、大楼内部以及园区内部，典型距离覆盖几十米至上百米。目前主要技术标准为802.11系列。无线局域网利用射频（Radio Frequency；RF）的技术，允许在局域网络环境中使用可以不必授权的ISM频段中的2.4GHz或5GHz射频波段，使用电磁波在空中进行通信连接，是非常便利的数据传输系统。WLAN的实现协议有很多，其中最为著名也是应用最为广泛的是无线保真技术--Wi-Fi。



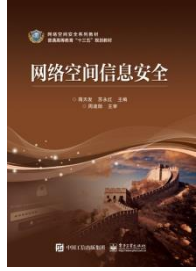
7.1 无线网络

- （4）无线LAN-to-LAN网桥：也即无线网络的桥接，从通信意义上来说包括电路型网桥和数据型网桥。主要用于大楼之间的联网通信，无线网桥功率大，传输距离远（最大可达约50km），抗干扰能力强，常采用802.11b或802.11g、802.11a和802.11n标准。



7.1 无线网络

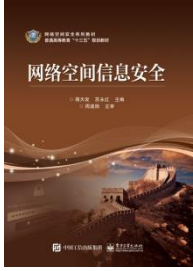
- （5）无线城域网：IEEE1999年设立了了IEEE 802.16工作组，其主要工作是建立和推进全球统一的无线城域网技术标准。2001年成立了WiMAX(Worldwide Interoperability for Microwave Access，全球微波接入互通)论坛组织），相关的无线城域网技术在市场上又被称为“WiMAX技术”。WiMAX利用无线发射塔或天线，能提供面向互联网的高速连接。其接入速率最高达75 Mbps，最大距离可达50km，覆盖半径达1.6km，它可以替代现有的有线和DSL连接方式，来提供最后1km的无线宽带接入。



7.1 无线网络

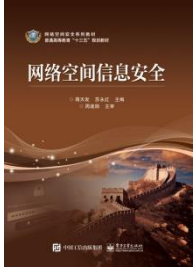
- (6)无线域域网，主要是为了满足超出一个城市范围的信息交流和网际接入需求，一般要用到GSM、GPRS、GPS、CDMA和3G等通信技术。3G推荐的主流技术标准有三种，WCDMA、CDMA2000及中国提出来的TD-SCDMA，这三种系统所使用的无线电核心频段都在2000Hz左右。

7.2 短程无线通信



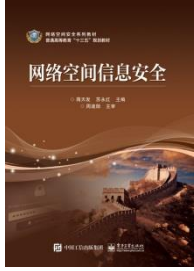
- 短距离低功耗无线通信是指传输距离在数十米或数百米之内，适用较低发射功率（小于100mW）的无线通信技术。目前使用较广泛的短距离、低功耗无线通信技术包括蓝牙（Bluetooth）、无线局域网Wi-Fi(IEEE802.11)、ZigBee（IEEE 802.15.4）、超宽频（UWB，Ultra Wide Band）、近场通信（NFC）、射频识别(RFID)、红外数据传输（IrDA）等。
- 以下主要介绍蓝牙、ZigBee、RFID、Wi-Fi、射频识别等无线网络技术：

7.2.1 蓝牙技术



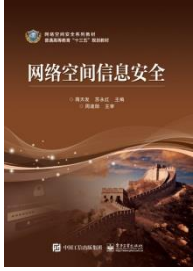
- 蓝牙技术是由移动通信公司与移动计算公司联合起来开发的传输范围约为6m左右的短距离无线通信技术，设计用来在便携式计算机、移动电话以及其他的移动设备之间建立起一种小型、经济、短距离的无线链路。使得包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间能够进行无线信息交换。目前IEEE将蓝牙列为IEEE802.15.1标准但不做限制。工作在2.4GHz-2.485 频带，带宽为1Mb/s。
-

7.2.1 蓝牙技术



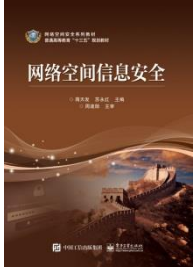
- 蓝牙使用跳频技术，将传输的数据分割成数据包，通过79个指定的蓝牙频道分别传输数据包。每个频道的频宽为1 MHz。蓝牙4.0使用2 MHz 间距，可容纳40个频道。第一个频道始于2402 MHz，每1 MHz一个频道，至2480 MHz。有适配跳频（Adaptive Frequency-Hopping，简称AFH）功能，通常每秒跳1600次。

7.2.1 蓝牙技术

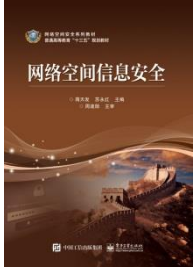


- 蓝牙是基于数据包、有着主从架构的协议。一个主设备至多可和同一微微网中的七个从设备通讯。所有设备共享主设备的时钟。
- 蓝牙已经经过8个版本的更新，分别为1.1、1.2、2.0、2.1、3.0、4.0、4.1、4.2。
- 2014年12月4日，蓝牙4.2标准颁布，改善了数据传输速度和隐私保护程度，并接入了该设备将可直接通过IPv6和6LoWPAN接入互联网。在新的标准下蓝牙信号想要连接或者追踪用户设备必须经过用户许可，否则蓝牙信号将无法连接和追踪用户设备。。

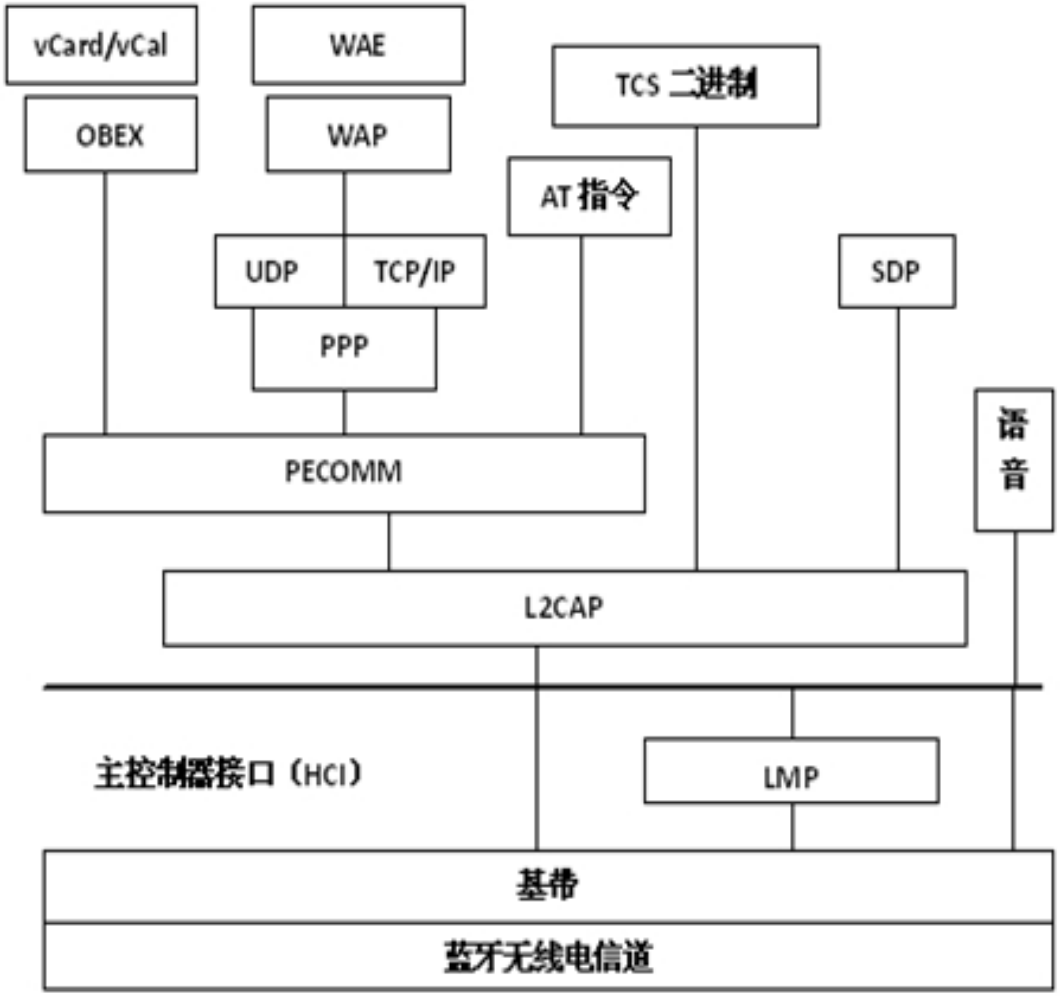
7.2.1 蓝牙技术



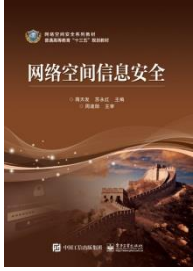
- 2016年6月，蓝牙技术联盟执行董事马克·鲍威尔透露，蓝牙技术联盟近期将在伦敦正式发布蓝牙5.0标准，该标准将实现颠覆性技术提升，支持室内定位，传输速率大幅提高。现在使用的蓝牙4.x设备理论覆盖范围可达100米，无线传输速率可达1兆比特。而“蓝牙5”的覆盖范围增加一倍，传输速率可提升至原来的4倍。“蓝牙5”还拥有室内定位和导航功能。


网络空间信息安全

完整的蓝牙协议栈

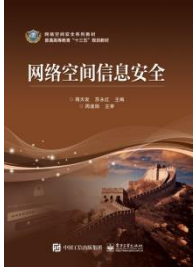

vCard/vCal
WAE
TCS 二进制
OBEX
WAP
AT 指令
UDP
TCP/IP
SDP
PPP
语音
PECOMM
L2CAP
主控制器接口（HCI）
LMP
基带
蓝牙无线电信道

7.2.1 蓝牙技术

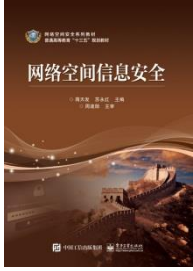


- 蓝牙核心协议蓝牙的核心协议由基带,链路管理,逻辑链路控制与适应协议和服务搜索协议等4部分组成.
- （1）基带协议基带协议确保各个蓝牙设备之间的射频连接，以形成微微网络。
- （2）链路管理协议
- 链路管理协议（LMP）负责蓝牙各设备间连接的建立和设置。LMP通过连接的发起，交换和核实进行身份验证和加密，通过协商确定基带数据分组大小；还控制无线设备的节能模式和工作周期，以及微微网络内设备单元的连接状态。

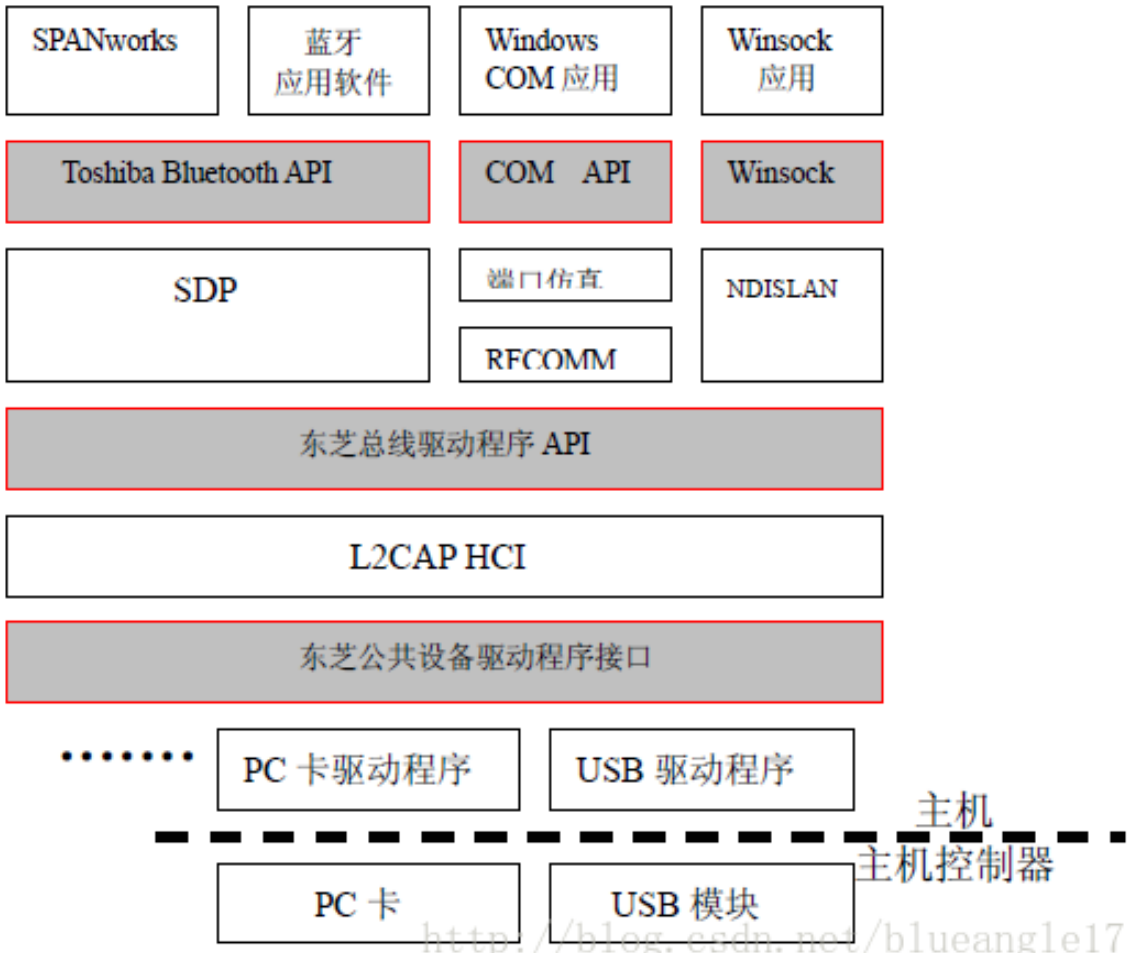
7.2.1 蓝牙技术



- （3）逻辑链路控制和适配协议
- 逻辑链路控制和适配协议（L2CAP）是基带的上层协议，可以认为L2CAP与LMP并行工作。L2CAP与LMP的区别在于当业务数据不经过LMP时，L2CAP为上层提供服务。
- （4）服务搜索协议
- 使用服务搜索协议（SDP），可以查询到设,备信息和服务类型，从而在蓝牙设备间建立相应的连接。

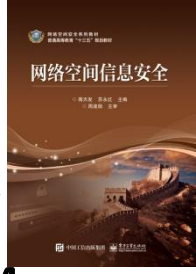


东芝蓝牙协议栈



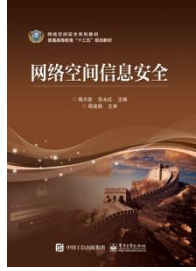
http://blog.csdn.net/blueangle17

7.2.1 蓝牙技术



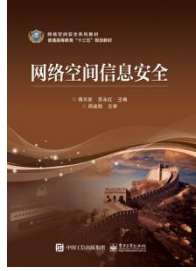
- 东芝蓝牙协议栈产品BluetoothTM Utility软件栈是由主机控制接口以上的蓝牙协议栈（L2CAP、RFCOMM、SDP）、硬件驱动程序（USB和PC卡）、应用程序接口（API）和支持蓝牙剖面的用户应用模块组成。它与蓝牙的1.0b板一致。
- 该软件栈能够实现通用访问应用规范GAP（Generic Access Profile）特性和业务发现应用规范SDAP（Service Discovery Application Profile）特性，它包括了蓝牙服务中心、蓝牙监视和蓝牙的LocalCOM三个方面的应用。
- 其中，蓝牙服务中心主要是指用户接口UI（User Interface）方面的应用，它为蓝牙最终用户提供了发现远端的设备、查询在远端设备提供的服务、与远端设备进行连接、以及列表管理等多种蓝牙服务；

7.2.1 蓝牙技术



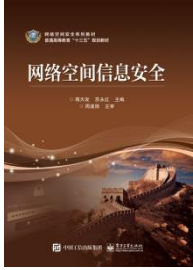
- 蓝牙监视是在当系统加电后，用户就可以使用该应用来控制蓝牙设备的供电状态并能够指示蓝牙设备的连接模式、状态、standby模式和断电模式；
- 蓝牙的LocalCOM主要是一个向导应用，用户可以用它来与自己选择的远端设备生成虚拟的COM、服务和连接。该软件栈中的L2CAP和RFCOMM是作为驱动程序模块来实现的，而SDP协议是作为用户模式应用来实现的。

7.2.1 蓝牙技术

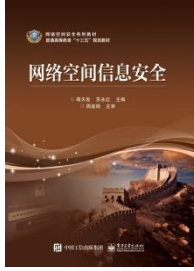


- 对蓝牙用户支持的剖面特性还使用了一些Windows COM应用和电话应用，这些应用使用应用程序接口（API）与蓝牙协议栈进行通信。如图 7.3 中的蓝牙ad hoc网络应用软件SPANworks就是通过API与其它包含蓝牙技术的设备进行数据交换的。

7.2.1 蓝牙技术

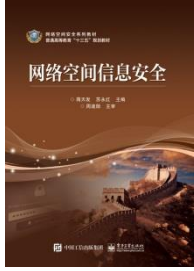


- 从蓝牙4.0版本开始引入BLE技术。蓝牙低能耗(BLE)技术是低成本、短距离、可互操作的鲁棒性无线技术，工作在免许可的2.4GHz ISM射频频段。它从一开始就设计为超低功耗(ULP)无线技术，利用许多智能手段最大限度地降低功耗。
- 蓝牙低能耗技术采用可变连接时间间隔，这个间隔根据具体应用可以设置为几毫秒到几秒不等。BLE技术采用非常快速的连接方式，平时可以处于“非连接”状态(节省能源)，此时链路两端相互间只是知晓对方，只有在必要时才开启链路，从而在尽可能短的时间内关闭链路。



7.2.1 蓝牙技术

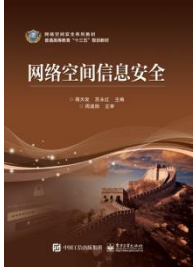
- BLE技术的工作模式非常适合用于从微型无线传感器(每半秒交换一次数据)或使用完全异步通信的遥控器等其它外设传送数据。这些设备发送的数据量非常少(通常几个字节)，而且发送次数也很少(例如每秒几次到每分钟一次，甚至更少)。
- 蓝牙低能耗技术的三大特性——最大化的待机时间、快速连接和低峰值的发送/接收功耗成就了ULP（超低功耗）性能。



7.2.1 蓝牙技术

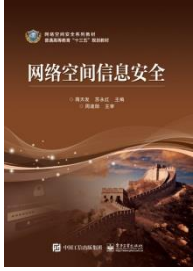
- 蓝牙低能耗技术用来最小化无线开启时间：仅用3个“广告”信道搜索其它设备或向寻求建立连接的设备宣告自身存在。相比之下，标准蓝牙技术使用了32个信道。换句话说，蓝牙低能耗技术扫描其它设备只需“开启”0.6至1.2ms时间，而标准蓝牙技术需要22.5ms时间来扫描它的32个信道。蓝牙低能耗技术定位其它无线设备所需的功耗要比标准蓝牙技术低10至20倍。

Frequency (MHz)	Bluetooth low energy Advertising channel	Bluetooth low energy Data channel	Wi-Fi Channel
2480	39		
2478		36	
2476		35	
2474		34	
2472		33	11
2470		32	11
2468		31	11
2466		30	11
2464		29	11
2462		28	11
2460		27	11
2458		26	11
2456		25	11
2454		24	11
2452		23	11
2450		22	
2448		21	6
2446		20	6
2444		19	6
2442		18	6
2440		17	6
2438		16	6
2436		15	6
2434		14	6
2432		13	6
2430		12	6
2428		11	6
2426	38		
2424		10	
2422		9	1
2420		8	1
2418		7	1
2416		6	1
2414		5	1
2412		4	1
2410		3	1
2408		2	1
2406		1	1
2404		0	1
2402	37		1



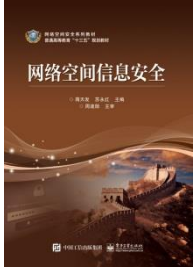
该规范的设计师选择的广告信道不会与Wi-Fi默认信道发生冲突

7.2.1 蓝牙技术



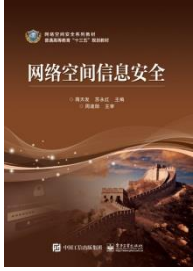
- 一旦连接成功后，蓝牙低能耗技术就会切换到37个数据信道之一。在短暂的数据传送期间，无线信号将使用标准蓝牙技术倡导的自适应跳频(AFH)技术以伪随机的方式在信道间切换(虽然标准蓝牙技术使用79个数据信道)。
- 要求蓝牙低能耗技术无线开启时间最短的另一个原因是它具有1Mbps的原始数据带宽——更大的带宽允许在更短的时间内发送更多的信息。举例来说，具有250kbps带宽的另一种无线技术发送相同信息需要开启的时间要长8倍。

7.2.1 蓝牙技术



- 蓝牙低能耗技术“完成”一次连接(即扫描其它设备、建立链路、发送数据、认证和适当地结束)只需3ms。而标准蓝牙技术完成相同的连接周期需要数百毫秒。无线开启时间越长，消耗的电池能量就越多。
- 蓝牙低能耗技术还能通过两种其它方式限制峰值功耗：采用更加“宽松的”射频参数以及发送很短的数据包。两种技术都使用高斯频移键控(GFSK)调制，但蓝牙低能耗技术使用的调制指数是0.5，而标准蓝牙技术是0.35。0.5的指数接近高斯最小频移键控(GMSK)方案，可以降低无线设备的功耗要求(这方面的原因比较复杂，本文暂不赘述)。更低调制指数还有两个好处，即提高覆盖范围和增强鲁棒性。

7.2.1 蓝牙技术

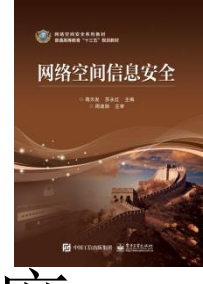


- 现阶段的智能硬件大多采用蓝牙4.0 BLE，这个版本相对蓝牙2.1标准有质的飞跃。从2011年苹果iPhone 4S发布开始，“蓝牙”派智能硬件几年间已经发展成业内公认的智能硬件和物联网连接标准之一。各种炫酷的新硬件如运动手环、智能手表、智能秤、防丢贴片等通常以手机作为控制终端，安装App连接蓝牙来操作。Google迟到了两年，在2013年才推出支持蓝牙4.0 BLE特性的Android 4.3。

7.2.1 蓝牙技术

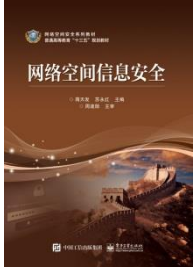
- 苹果利用技术BLE实现了Apple TV的自动化设置。只要用一款运行iOS 7的设备轻轻触碰第三代Apple TV，就能让它自动设置Wi-Fi网络、地区设置和Apple Store账户。这使得设备不需要在同一Wi-Fi下，甚至不需要和目标设备配对，就能实现复杂的交互。要实现这一功能，你需要把iPhone 4S、iPad 3、iPad Mini、iPod touch 5或更新款的设备中的蓝牙打开。然后在第三代Apple TV的设置界，把iOS设备轻触上去。设备会进行配对，提示你在iOS设备上输入苹果ID。之后你可以选择是否记住账户信息，让Apple TV可购买内容。

7.2.1 蓝牙技术

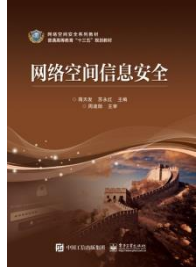


- 蓝牙4.0 BLE的缺点在于Android手机终端支持度极差。原因有两个方面：一是虽然Google在Android 4.3开始支持BLE，但这款系统普及率不高，尤其在中国；二是标准不统一，Google和现有存量机型对BLE的诠释不同。假设一款智能硬件支持连接蓝牙 4.0 BLE的Android手机，那么它需要既兼容博通蓝牙芯片及蓝牙BLE SDK（主要是HTC、小米两家采用），也要兼容三星的蓝牙BLE SDK，Android原生BLE SDK支持当然也不能少。如果不做兼容适配，这款硬件蓝牙连接三星、HTC等手机就会出问题

7.2.1 蓝牙技术



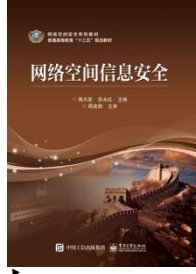
- 蓝牙在应用层和链路层上都采取了保密措施以保证通信的安全性，所有蓝牙设备都采用相同的认证和加密方式。在链路层，使用 4 个参数来加强通信的安全性，即蓝牙设备地址BD_ADDR、认证私钥、加密私钥和随机码RAND。
- 蓝牙设备地址是一个48位的IEEE地址，它唯一地识别蓝牙设备，对所有蓝牙设备都是公开的；认证私钥在设备初始化期间生成，其长度为128比特；加密私钥通常在认证期间由认证私钥生成，其长度根据算法要求选择8~128比特之间的数（ 8 的整数倍），对于目前的绝大多数应用，采用64比特的加密私钥就可保证其安全性；随机码由蓝牙设备的伪随机过程产生，其长度为128比特



7.2.2 ZigBee技术

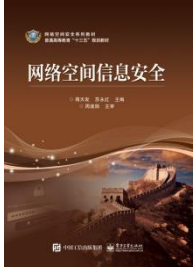
- ZigBee来源于 ZigZag，是一种蜜蜂的肢体语言。当蜜蜂新发现一片花丛后会用特殊「舞蹈」来告知同伴发现的食物种类及位置等信息，是蜜蜂群体间一种简单、高效的传递信息方式，因此 ZigBee 也被成为「紫蜂协议」。

7.2.2 ZigBee技术



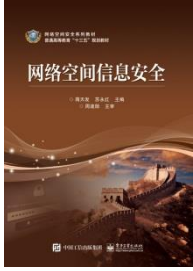
- ZigBee协议从下到上分别为物理层(PHY)、媒体访问控制层(MAC)、传输层(TL)、网络层(NWK)、应用层(APL)等。其中物理层和媒体访问控制层遵循IEEE 802.15.4标准的规定。它是一种低速短距离传输的无线网络协议。ZigBee协议在2003年正式问世。它使用了在它之前所研究过的面向家庭网络的通信协议Home RF Lite。ZigBee在数千个微小的传感器之间相互协调实现通信，需要的能量很少，以接力的方式通过无线电波将数据从一个网络节点传到另一个节点。

7.2.2 ZigBee技术



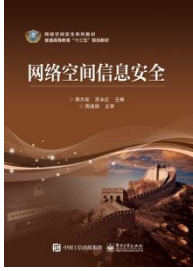
- ZigBee具有低功耗、低成本、低速率、近距离、短时延等优点。
- 在低耗电待机模式下，2节5号干电池可支持1个节点工作6～24个月，甚至更长。它工作在20～250kbps的速率，每块芯片的价格大约为2美元。传输范围一般介于10～100m之间，在增加发射功率后，亦可增加到1～3km。
- ZigBee的响应速度较快，一般从睡眠转入工作状态只需15ms，节点连接进入网络只需30ms，进一步节省了电能。相比较，蓝牙需要3～10s、WiFi 需要3 s。ZigBee网络主要是为工业现场自动化控制数据传输而建立，每个ZigBee“基站”却不到1000元人民币。

7.2.2 ZigBee技术

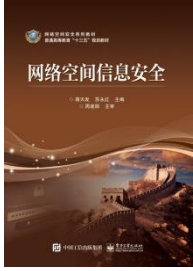


- 因为ZigBee协议的低速率(工作在 20～250 kbps 较低速率上)，优秀的自组网能力（与蓝牙的点对点传输方式相比，最多支持 65000 个设备组网)，较高的安全性(至今全球尚未出现一起破解先例)，可以很方便的应用于智能家居上。

小米智能家居多媒体网关

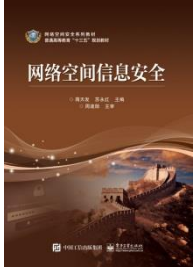


- 选择ZigBee协议的原因之一：低功耗。在小米智能家庭套装中，除了多功能网关（图7.5），其他三个产品都是靠内置电池供电的，可以持续使用 2 年以上。如此长的续航时间，离不开低功耗的传感器和传输协议。
- 选择ZigBee协议的原因之二：物联网设备体积小、安装位置不固定，要想获得长久的续航时间，需要ZigBee协议的加入。
- 选择ZigBee协议的原因之三：安全性较高。
- 选择ZigBee协议的原因之四: 良好的自组网能力。小米致力构建智能家居生态链（**大量智能设备同时工作**），当然不能使用蓝牙（最多连7个设备）。



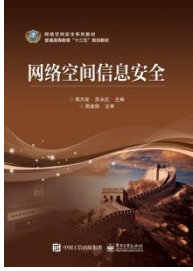
小米智能家居多媒体网关

多功能网关存在的意义：ZigBee 协议也存在一些不足，它虽然可以方便地组网但不能接入互联网，在 ZigBee 网络中必须有一个类似路由器的角色。就像小米智能家庭套装中的多功能网关承担了这个角色，它是一个能够接入 WiFi 的控制中心，通过这种方式来打通物联网和互联网的世界。



ZigBee协议栈体系结构安全

- ZigBee协议栈由物理层、数据链路层、网络层和应用层组成。
- 物理层负责基本的无线通信，由调制、传输、数据加密和接收构成。链路层提供设备之间单跳通信，可靠传输和通信安全。网络层主要提供通用的网络层功能（如拓扑结构的搭建和维护、寻址和安全路由）。应用层包括应用支持子层、ZigBee设备对象和各种应用对象。应用支持子层提供安全和映射管理服务，ZDO负责设备管理，包括安全策略和安全配置的管理，应用层提供对ZDO和ZigBee应用的服务。

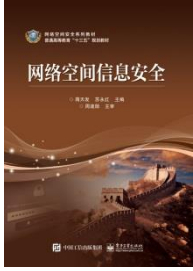


ZigBee协议栈体系结构安全

- **数据链路层安全**
- 数据链路层通过建立有效的机制保护信息安全。
- MAC层有 4 种类型的帧，分别是命令帧、信标帧、确认帧和数据帧。安全帧格式如下图：

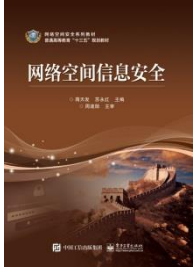
SYNC	PHY Header	MAC Header	Auxiliary Header	Encrypted MAC Payload	MIC

图 7.7　数据链路层安全帧格式



ZigBee协议栈体系结构安全

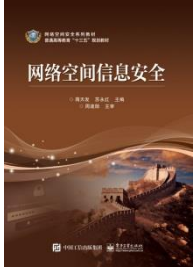
- 其中，Auxiliary　Header是携带的安全信息，MIC提供数据完整性检查，有０、３２、６４、１２８位可供选择。对于数据帧，MAC层只能保证单挑通信安全，为了提供多条通信的安全保证，必须依靠上层提供的安全服务。在MAC层上使用的是AES加密算法，根据上层提供的密钥的级别，可以保障不同水平的安全性。



ZigBee协议栈体系结构安全

- IEEE８０２.１５.４标准MAC层使用的是CCM模式，CCM是一种通用的认证和加密模式，被定义使用在类似于AES的１２８位大小的数据库上，它由CTR模式和CBC—MAC模式组成。CCM主要包括认证和加密解密，认证使用CBC－MAC模式，而加密解密适用的是CTR模式。ＺｉｇＢｅｅ适用一种改进的模式对数据进行保护：CMM*模式，它是通过执行AES－１２８加密算法对数据保密。

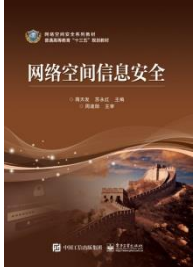
ZigBee协议栈体系结构安全



- **网络层安全**
- 网络层对帧采取的保护机制同上面一样，为了保证帧能正确传输，帧格式中也还有Auxiliary Header和MIC。网络层的安全帧格式如图

SYNC	PHY Header	MAC Header	NWK Header	Auxiliary Header	Encrypted MAC Payload	MIC

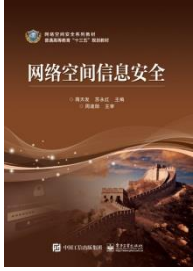
图7.8 网络层安全帧格式



ZigBee协议栈体系结构安全

- 网络层的主要思想是首先广播路由信息，接着处理接收到的路由信息，例如判断数据帧来源，然后根据数据帧中的目的地址采取相应机制将数据帧传送出去。
- 在传送的过程中一般是利用链接密钥对数据进行加密处理，如果链接密钥不可用网络层将利用网络密钥进行保护，由于网络密钥在多个设备中使用，可能带来内部攻击，但是它的存储开销代价更小。网络层对安全管理有责任，但其上一层控制着安全管理。

ZigBee协议栈体系结构安全

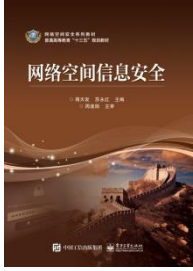


- 应用层安全
- 应用层安全通过APS子层提供，根据不同的应用需求采用不同的密钥，主要使用的是链接密钥和网络密钥。应用层的安全帧格式如图

SYNC	PHY Header	MAC Header	NWK Header	APS Header	Auxiliary Header	Encrypted MAC Payload	MIC

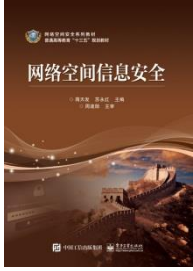
图7.9　应用层安全帧格式

应用层安全



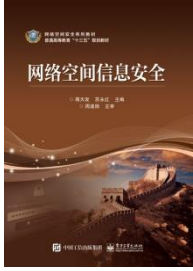
- APS提供的安全服务由密钥建立、密钥传输和设备服务管理。
- 密钥建立是在两个设备间进行，包括四个步骤：交换暂时数据，生成共享密钥，获得链接密钥，确认链接密钥。
- 密钥传输服务在设备间安全传输密钥。设备服务管理包括更新设备和移除设备，更新设备服务提供一种安全的方式通知其他设备有第三方设备需要更新，移除设备则是通知有设备不满足安全需要，要被删除。

ZigBee协议栈体系结构安全

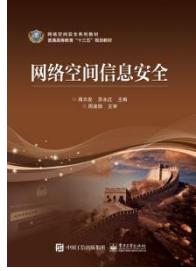


- 值得注意的是，系统的整体安全性是在模板级定义的，这意味着模板应该定义某一特定网络中应该实现何种类型的安全。
- 每一层(MAC、网络或应用层)都能被保护，为了降低存储要求，它们可以分享安全钥匙。SSP是通过ZDO进行初始化和配置的，要求实现高级加密标准(AES)。ZigBee规范定义了信任中心的用途。信任中心是在网络中分配安全钥匙的一种令人信任的设备。

ZigBee协议栈体系结构安全



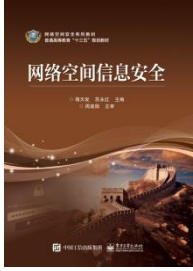
- ZigBee采用3种基本密钥，网络密钥，链接密钥，主密钥。
- 网络密钥可以在数据链路层、网络层和应用层中应用，主密钥和链接密钥则使用在应用层及子层。
- 网络密钥可以在设备制造时安装，也可以在密钥传输中得到。主密钥可以在信任中心设置或者在制造是安装，还可以是基于用户访问的数据:个人识别码（PIN）、密码和口令等。



ZigBee协议栈体系结构安全

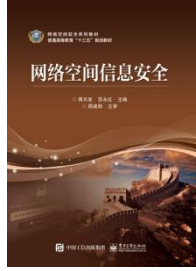
- 为了保证传输过程中主密钥不被窃听，需要确保主密钥的保密性和正确性。
- 链接密钥是在两个端设备通信时共享，可以由主密钥建立，也可以在设备制造时安装。链接密钥和网络密钥要不断更新。当两个设备同时拥有两种密钥时，采用链接密钥来通信。尽管存储网络密钥开销小，但是降低了系统安全。

ZigBee协议栈体系结构安全

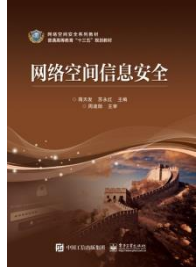


- 为了满足安全性需要，商业模式下，ＺｉｇＢｅｅ标准提供不同的方法来确保安全:
- （１）加密技术。ＺｉｇＢｅｅ适用AES—１２８加密算法。网络层加密是通过网络密钥来完成，设备层是通过唯一链接密钥在两端设备同时完成加密。加密技术的有无不影响帧序更新、完整性和鉴权。
- (２)鉴权技术。鉴权可以保证信息的原始性，使得信息不被第三方攻击。鉴权有网络层和设备层两种，网络层鉴权可以组织外部攻击，但增加了内存开销，它通过共享网络密钥完成。设备层鉴权通过设备间唯一链接密钥完成。

ZigBee协议栈体系结构安全

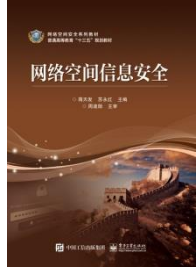


- （３）完整性保护。对信息的完整性可选择四种：０、３２、６４、１２８位，默认采用６４位。
- (４)帧序更新。通过使用设置计数器来保证数据更新，通过使用一个有序编号来避免帧重发攻击。在接收到一个数据帧以后，将新的编号和最后一个编号比较，如果新的编号更新，校验通过，编号更新，反之校验失败。



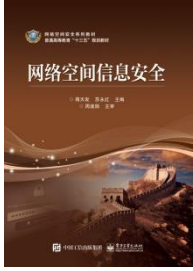
7.2.3 RFID技术

- RFID是Radio Frequency Identification的缩写，即射频识别。常称为感应式电子芯片或近接卡、感应卡、非接触卡、电子卷标、电子条形码等等。可通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触。

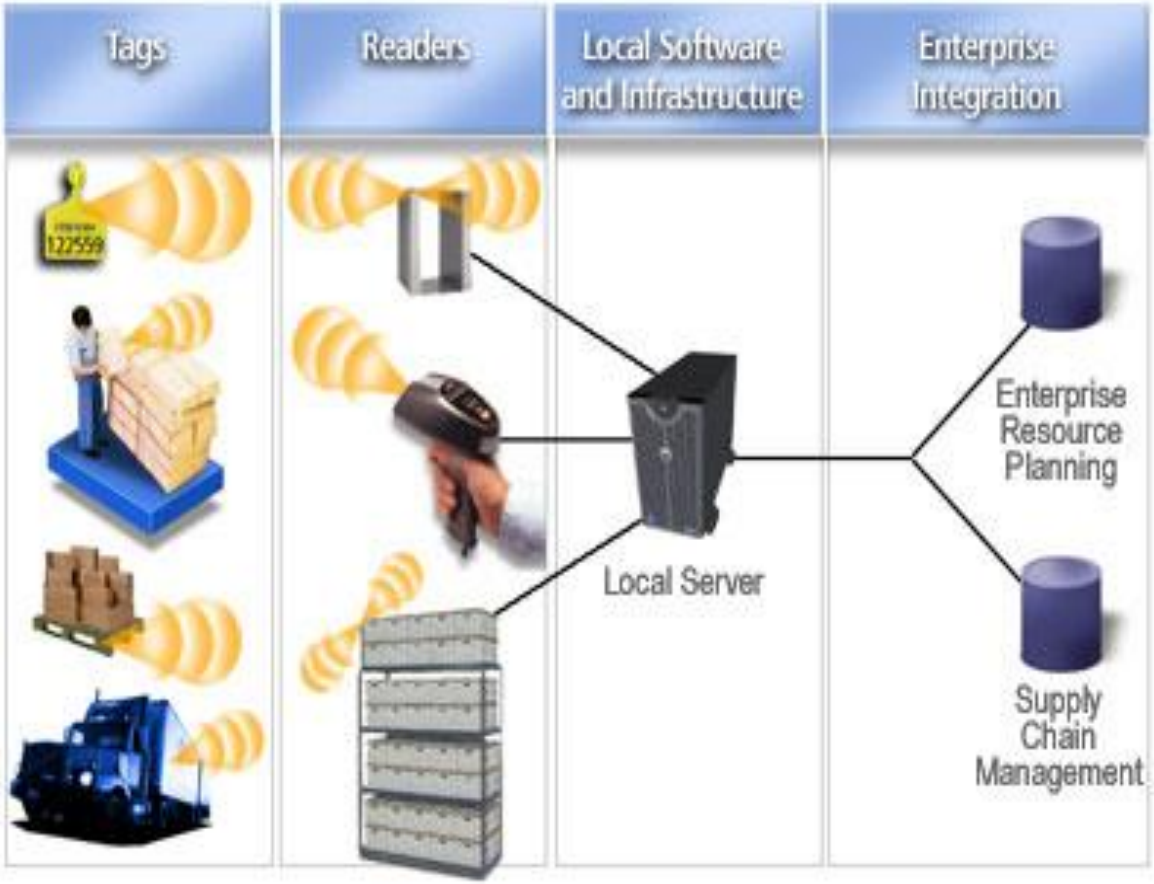


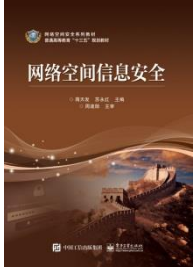
7.2.3 RFID技术

- 最基本的RFID系统由三部分组成：
- **应答器：**由天线，耦合元件及芯片组成，一般来说都是用标签作为应答器，每个标签具有唯一的电子编码，附着在物体上标识目标对象。
- **阅读器：**由天线，耦合元件，芯片组成，读取（有时还可以写入）标签信息的设备，可设计为手持式rfid读写器（如：C5000W）或固定式读写器。
- **应用软件系统：**是应用层软件，主要是把收集的数据进一步处理，并为人们所使用。


网络空间信息安全

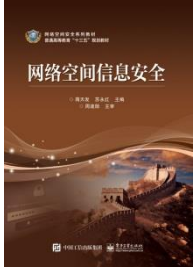
射频识别技术


Tags
Readers
Local Software and Infrastructure
Enterprise Integration
122559
Local Server
Enterprise Resource Planning
Supply Chain Management



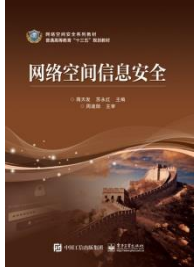
7.2.3 RFID技术

- RFID技术中所衍生的产品大概有三大类：无源RFID产品、有源RFID产品、半有源RFID产品。
- 1、无源RFID产品。比如，公交卡、食堂餐卡、银行卡、宾馆门禁卡、二代身份证等，属于近距离接触式识别类。其产品的主要工作频率有低频125KHZ、高频13.56MHZ、超高频433MHZ，超高频915MHZ。
- 2、有源RFID产品。其远距离自动识别的特性，决定了其巨大的应用空间和市场潜质。在远距离自动识别领域，如智能监狱，智能医院，智能停车场，智能交通，智慧城市，智慧地球及物联网等领域有重大应用。产品主要工作频率有超高频433MHZ，微波2.45GHZ和5.8GMHZ。



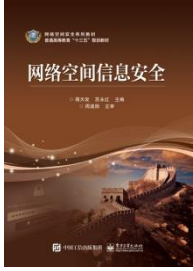
7.2.3 RFID技术

- 3、半有源RFID产品，结合有源RFID产品及无源RFID产品的优势，在低频125KHZ频率的触发下，让微波2.45G发挥优势。半有源RFID技术，也可以叫做低频激活触发技术，利用低频近距离精确定位，微波远距离识别和上传数据，来解决单纯的有源RFID和无源RFID没有办法实现的功能。简单的说，就是近距离激活定位，远距离识别及上传数据。



7.2.3 RFID技术

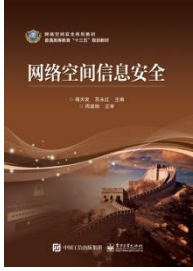
- 半有源RFID是一项易于操控、简单实用且特别适合用于自动化控制的灵活性应用技术，识别工作无须人工干预，它既可支持只读工作模式也可支持读写工作模式，且无需接触或瞄准；可在各种恶劣环境下自由工作，短距离射频产品不怕油渍、灰尘污染等恶劣的环境，可以替代条码，例如用在工厂的流水线上跟踪物体；长距射频产品多用于交通上，识别距离可达几十米，如自动收费或识别车辆身份等。



7.2.3 RFID技术

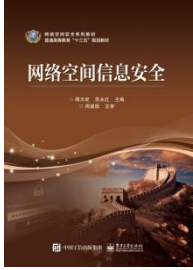
- RFID的优势表现在：
- 1）读取方便快捷：数据的读取无需光源，甚至可以透过外包装来进行。有效识别距离更大，采用自带电池的主动标签时，有效识别距离可达到30米以上；
- 2）识别速度快：标签一进入磁场，解读器就可以即时读取其中的信息，而且能够同时处理多个标签，实现批量识别；
- 3）数据容量大：数据容量最大的二维条形码(PDF417)，最多也只能存储2725个数字；若包含字母，存储量则会更少；RFID标签则可以根据用户的需要扩充到数十K；

7.2.3 RFID技术

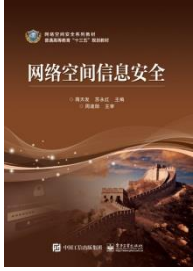


- 4）使用寿命长，应用范围广：其无线电通信方式，使其可以应用于粉尘、油污等高污染环境和放射性环境，而且其封闭式包装使得其寿命大大超过印刷的条形码；
- 5）标签数据可动态更改：利用编程器可以向其写入数据，从而赋予RFID标签交互式便携数据文件的功能，而且写入时间相比打印条形码更少；
- 6）更好的安全性：不仅可以嵌入或附着在不同形状、类型的产品上，而且可以为标签数据的读写设置密码保护，从而具有更高的安全性；

7.2.3 RFID技术

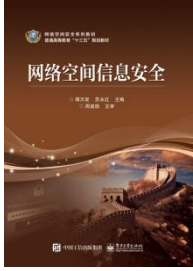


- 7）动态实时通信：标签以与每秒50～100次的频率与解读器进行通信，所以只要RFID标签所附着的物体出现在解读器的有效识别范围内，就可以对其位置进行动态的追踪和监控。
- RFID技术的基本工作原理并不复杂：标签进入磁场后，接收解读器发出的射频信号，凭借感应电流所获得的能量发送出存储在芯片中的产品信息（*Passive Tag*，无源标签或被动标签），或者由标签主动发送某一频率的信号（*Active Tag*，有源标签或主动标签），解读器读取信息并解码后，送至中央信息系统进行有关数据处理。



7.2.3 RFID技术

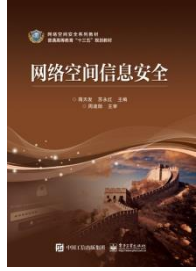
- RFID的安全性方面，我们可以从以下几个方面进行防御：
- 1.采用更强加密算法的芯片卡，比如CPU卡；
- 2.敏感数据应进行加密处理；
- 3.读卡器与后端主机数据库实行线上作业，采用即时连线的方式进行系统核查；
- 4.结合uid进行加密，并设置uid白名单；
- 5.对全扇区采用非默认密码加密。



7.2.3 RFID技术

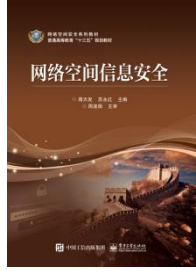
- RFID应用前景广阔，据前瞻网《2013-2017年中国RFID行业市场前瞻与投资战略规划分析报告》调查数据显示，到2010年，全球RFID标签的生产数量将达到330亿，是2005年13亿产量的25倍以上，RFID在未来几年的应用会随着产业不同而有很大差异。从1991年至今，已经有超过15000万台汽车在使用RFID标签。而根据分析师的预测，未来RFID将主要应用在供应链管理等物流领域。

7.2.4 Wi-Fi技术



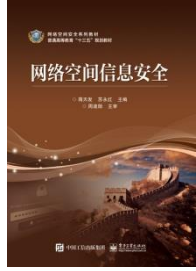
- 2015年9月，Skyhook与Mapbox两家公司收录的wifi信号数据表示，全球wifi信号多达9亿。使用IEEE 802.11系列协议的局域网就称为Wi-Fi。它是一种能够将个人电脑、手持设备（如Pad、手机）等终端以无线方式互相连接的技术。Wi-Fi是一个无线网路通信技术的品牌，由Wi-Fi联盟(Wi-Fi Alliance)所持有。

7.2.4 Wi-Fi技术



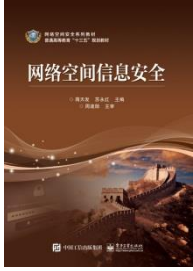
- Wi-Fi其实并不存在英文全称，Wireless Fidelity是错误的解读，无线网络在无线局域网的范畴是指“无线相容性认证”.通过无线电波来连网；常见的就是一个无线路由器，在这个无线路由器的电波覆盖的有效范围都可以采用无线保真连接方式进行联网，如果无线路由器连接了一条ADSL线路或者别的上网线路，则又被称为热点。

7.2.4 Wi-Fi技术



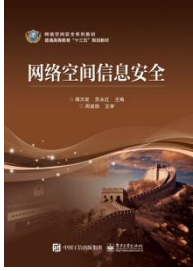
- 1996年，美国网络通讯设备大厂朗讯（Lucent）率先发起成立无线以太兼容性联盟（Wireless Ethernet Compatibility Alliance，WECA），着手创立无线网络协议（WLAN），1999年，WECA更名为Wi-Fi联盟，再度架构一套认证标准，提出通行业界的无线网络技术--802.11一系列规格，包括802.11.b、802.11.a、802.11.g等。

7.2.4 Wi-Fi技术



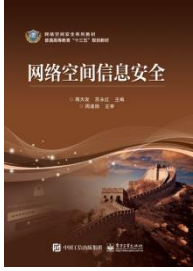
- **IEEE 802.11标准**
- 1997年6月26日，IEEE 802.11标准制定完成，1997年11月26日正式发布。IEEE 802.11无线局域网标准的制定是无线网络技术发展的一个里程碑。802.11规范了无线局域网络的媒体访问控制（Medium Access Control，MAC）层及物理层，使得各种不同厂商的无线产品得以互联。IEEE 802.11标准的颁布，使得无线局域网在各种有移动要求的环境中被广泛接受。我们耳熟能详的IEEE 802.11a/b/g,主要以PHY层的不同作为区分，区别直接表现在工作频段及数据传输率、最大传输距离这些指标上。

7.2.4 Wi-Fi技术



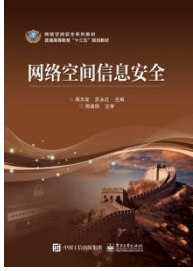
- 2000年8月，IEEE 802.11标准得到了进一步的完善和修订，并成为IEEE/ANSI和ISO/IEC 的一个联合标准，ISO/IEC将该标准定为ISO 8802.11。这次IEEE 802.11标准的修订内容包括用一个基于SNMP的MIB来取代原来基于OSI协议的MIB。另外，还增加了两项新内容：

7.2.4 Wi-Fi技术



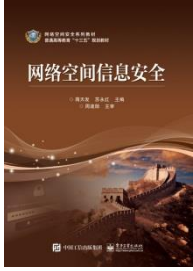
- 1）IEEE 802.11a——它扩充了标准的物理层，规定该层使用5GHz的频带。该标准采用正交频分调制数据，传输速率范围为6M～54Mbps。这样的速率既能满足室内的应用，也能满足室外的应用。
- 2）IEEE 802.11b——它是IEEE 802.11标准的另一个扩充，它规定采用2.4GHz频带，调制方法采用补偿码键控(CKK)。CKK来源于直序扩频技术，多速率机制的介质访问控制(MAC)确保当工作站之间的距离过长或干扰太大、信噪比低于某个门限值时，传输速率能够从11Mbps自动降到5.5Mbps，或者根据直序扩频技术调整到2Mbps和1Mbps。

7.2.4 Wi-Fi技术



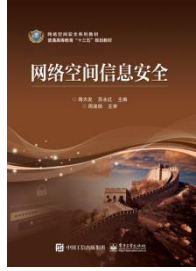
- IEEE 802.11b对无线局域网通信的最大贡献是可以支持两种速率——5.5Mbps和11Mbps。要做到这一点，就需要选择DSSS作为该标准的惟一物理层技术，因为，目前在不违反FCC规定的前提下，采用跳频技术无法支持更高的速率。这意味着IEEE 802.11b系统可以与速率为1Mbps和2Mbps的IEEE 802.11DSSS系统交互操作，但是无法与1Mbps 和2Mbps的IEEE 802.11的FHSS系统交互操作。

7.2.4 Wi-Fi技术



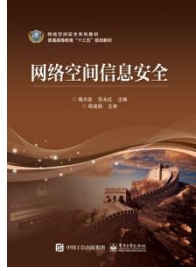
- 2003年完成草案的IEEE802.11g是作为使用2.4GHz频带无线电波的IEEE802.11b的高速版而制定的标准。
- 但是为了实现54Mbps的传输速度，11g采用了与11b不同的OFDM（正交频分复用）调制方式。因此，为了兼容802.11b，802.11g除本身特有的调制方式以外，还具备使用与802.11b相同的调制方式进行通信的功能，可以根据不同的通信对象切换调制方式。
- 在802.11g和802.11b终端混用的场合，802.11g接入点可以为每个数据包根据不同的对象单独切换不同的调制方式。也就是说以802.11g调制方式与802.11g终端通信，以802.11b调制方式与802.11b终端通信。

7.2.4 Wi-Fi技术



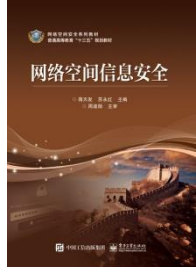
- **IEEE802.11a标准**
- 1999年，IEEE 802.11a标准制定完成，该标准规定无线局域网工作频段在5.15～5.825GHz，数据传输速率达到54Mbps/72Mbps(Turbo)，传输距离控制在6～60米。802.11a采用提高频率信道利用率的正交频分复用（OFDM）的独特扩频技术；可提供25Mbps的无线ATM接口和6Mbps的以太网无线帧结构接口，以及TDD/TDMA的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

7.2.4 Wi-Fi技术



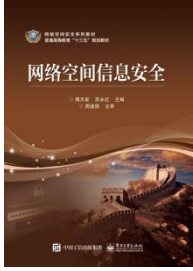
- 直到2001年12月市场上才出现第一款兼容802.11a的产品。802.11a标准最高可以提供54Mbps的数据传输速率和8个不重叠的频率通道,从而可以增加网络容量，提高可扩展性，并能够在不干扰相邻单元的情况下创建微型单元式结构。
- 802.11a工作在不需申请的5GHz频段，因为不会受到来自与工作在2.4GHz频段的设备的干扰，例如微波炉、无绳电话和蓝牙设备。

7.2.4 Wi-Fi技术



- 但是，802.11a标准并不能与现有的支持802.11b的设备兼容。已经采用了802.11b设备，并希望获得802.11a技术所提供的更高通道数和网络速度的企业必须安装一整套全新的802.11a基础设施，以及802.11a接入点和客户端适配器。需要指出的是，2.4GHz和5GHz设备可以在互不干扰的情况下在同一个物理环境下工作。

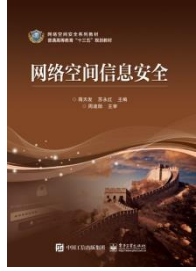
7.2.4 Wi-Fi技术



- 到目前为止，802.11a还未在欧洲获得批准；但是，IEEE和欧洲通信标准委员会（ETSI）目前正在设法通过IEEE 802.11h任务小组达成一项协议，解决802.11a的电源问题和通道设置问题。

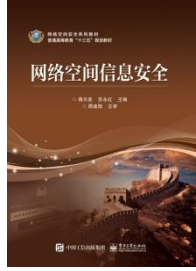
  推广802.11a的另外一个障碍是缺乏对互操作性的认证。目前，各个厂商的产品之间的互操作性还没有保障。WECA将为802.11a产品提供互操作性测试，并致力于进一步推广该技术。但是，只有在两家芯片厂商开始制造相应的芯片，并至少有三家厂商在这些芯片的基础上制造产品以后，WECA才会开始进行这样的测试。

7.2.4 Wi-Fi技术



- **IEEE 802.11b 标准**
- 1999年9月IEEE 802.11b被正式批准，该标准规定无线局域网工作频段在2.4～2.4835GHz，数据传输速率达到11Mbps，比两年前刚批准的IEEE 802.11标准快5倍，扩大了无线局域网的应用领域。
- 该标准是对IEEE 802.11的一个补充，采用点对点模式和基本模式两种运作模式，在数据传输速率方面可以根据实际情况在11Mbps、5.5Mbps、2Mbps、1Mbps的不同速率间自动切换，而且在2Mbps、1Mbps速率时与802.11兼容。

7.2.4 Wi-Fi技术



- 802.11b使用直接序列（Direct Sequence）DSSS作为协议。802.11b和工作在5GHz频率上的802.11a标准不兼容。由于价格低廉，IEEE 802.11b的优点参见表7.1。802.11b产品已经被广泛地投入市场，并在许多实际工作场所运行。

7.2.4 Wi-Fi技术

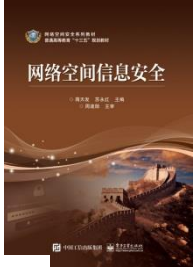
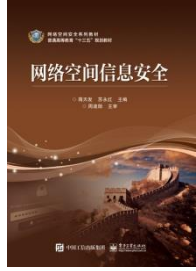


表 7.1　IEEE　802.11b 的优点

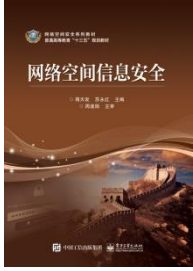
功能	优点
速度	2.4GHz 直接序列扩频，提供最大为 11Mbps 的数据传输速率，无须直线传播
动态速率转换	当射频情况变差时，降低数据传输速率为 5.5Mbps、2Mbps 或 1Mbps
使用范围	IEEE 802.11b 支持以百米为单位的范围（在室外为 300m，在办公环境中最长为 60m）
可靠性	与以太网类似的连接协议，为数据包确认提供可靠的数据传送和网络带宽的有效使用
互用性	与以前标准不同的是，802.11b 只允许一种标准的信号发送技术。WECA 将认证产品的兼容性
电源管理	网络接口卡可转到休眠模式，访问点将信息缓冲到客户，延长了笔记本电脑的电池寿命
漫游支持	允许在访问点之间进行无缝连接
加载平衡	信号拥塞或信号质量差时，无线网卡可更改与之连接的访问点，以提高性能
可伸缩性	最多 3 个访问点可以同时定位于有效使用范围中，以支持上百个用户
安全性	内置式鉴定和加密

7.2.4 Wi-Fi技术



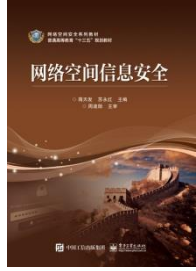
- 802.11b运作模式基本分为两种：点对点模式（ad-hoc mode）和基本模式 (infrastructure mode)，这跟无线局域网的两种拓扑结构相对应。
- 点对点模式是指无线网卡和无线网卡之间的通信方式。只要PC插上无线网卡即可与另一具有无线网卡的PC连接，对于小型的无线网络来说，是一种方便的连接方式，最多可连接256台PC机。而基本模式是指无线网络规模扩充或无线和有线网络并存的通信方式，这是802.11b最常用的方式。此时，插上无线网卡的PC需要由接入点与另一台PC连接。

7.2.4 Wi-Fi技术



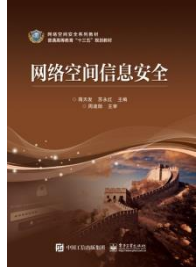
- 接入点负责频段管理及漫游等指挥工作，一个接入点最多可连接624台PC机（无线网卡）。当无线网络节点扩增时，网络存取速度会随着范围扩大和节点的增加而变慢，此时添加接入点可以有效控制和管理频宽与频段。无线网络需要与有线网络互连，或无线网络节点需要连接和存取有线网络的资源和服务器时，接入点可以作为无线网和有线网之间的桥梁。

7.2.4 Wi-Fi技术



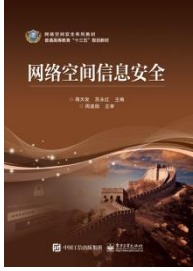
- **IEEE 802.11g标准**
- IEEE的802.11g标准是对流行的IEEE 802.11b（即Wi-Fi标准）的提速（速度从IEEE 802.11b的11Mb/s提高到54Mb/s）。
- IEEE802.11g接入点支持IEEE 802.11b和IEEE802.11g客户设备。同样，采用IEEE802.11g网卡的笔记本电脑也能访问现有的IEEE 802.11b接入点和新的IEEE802.11g接入点。

7.2.4 Wi-Fi技术



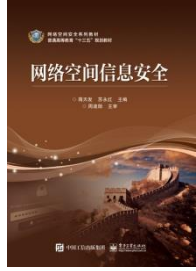
- 不过，基于IEEE802.11g标准的产品目前还不多见。如果需要高速度，已经推出的IEEE802.11a产品可以提供54Mb/s的最高速度。IEEE802.11a的主要缺点是不能和IEEE 802.11b设备互操作，而且与IEEE 802.11b相比，IEEE802.11a网卡和接入点较贵。

7.2.4 Wi-Fi技术



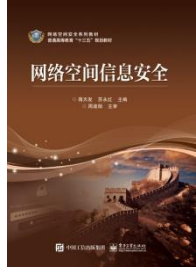
- IEEE802.11g可以提供与IEEE802.11a相同的54Mbps数据传输速率，还可以对IEEEIEEE802.11b设备向后兼容。这意味着IEEE 802.11b客户端卡可以与IEEE802.11g接入点配合使用，而IEEE802.11g客户端卡也可以与IEEE 802.11b接入点配合使用。
- 因为IEEE802.11g和IEEE 802.11b都工作在不需许可的2.4GHz频段，所以对于那些已经采用了IEEE 802.11b无线基础设施的企业来说，移植IEEE到IEEE802.11g将是一种合理的选择。

7.2.4 Wi-Fi技术



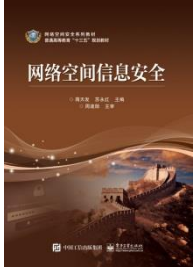
- 需要指出的是，IEEE 802.11b产品无法"软件升级"到IEEE802.11g，这是因为IEEE802.11g无线收发装置采用了一种与IEEE 802.11b不同的芯片组，以提供更高的数据传输速率。但是，就像以太网和快速以太网的关系一样，IEEE802.11g产品可以在同一个网络中与IEEE 802.11b产品结合使用。由于IEEE802.11g与IEEE 802.11b工作在同一个无需申请的频段，所以它需要共享三个相同的频段，这将会限制无线容量和可扩展性。

7.2.4 Wi-Fi技术



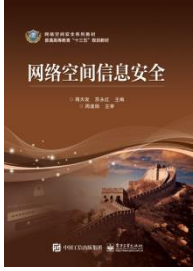
- **IEEE 802.11n 标准**
- 在802.11g和802.11a之上发展起来的一项技术，与之前的技术标准相比，具有以下特点：
- 1）速率更高，最高可达600Mbps
- 2）采用智能天线技术，通过多组独立天线组成的天线阵列，可以动态调整波束，保证信号的稳定性，同时可以减少其它信号的干扰。
- 3）覆盖范围可以扩大到好几平方公里，移动性极大提高。
- 4）采用软件无线电技术，兼容性大大增强。

7.2.4 Wi-Fi技术

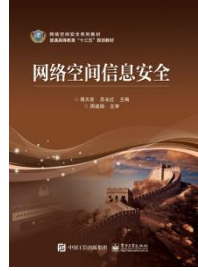


- 5）传输速率从之前的54Mbps,可增强到300Mbps~600Mbps.
- 6)设计更精密，物理层涉及的主要技术有MIMO、MIMO-OFDM、40MHz、Short GI等。802.11n对MAC采用了Block确认、帧聚合等技术，大大提高了MAC层的效率
- 7）**功耗**更低。802.11n在功耗和管理方面进行了重大创新，不仅能够延长Wi-Fi智能手机的电池寿命，还可以嵌入到其它设备中，如医疗监控设备，楼宇控制系统，实时定位跟踪标签和消费电子产品。可以不断地监测和收集数据，可基于用户的身份和位置进行个性化。

IEEE802.11a .11b .11g的对比



- **IEEE802.11a .11b .11g的对比**
- IEEE 802.11b和IEEE802.11a的提出是WLAN发展的一个里程碑，它们分别为2.4GHz和5GHz频段做定义，IEEE 802.11b物理层最大数据率为11Mbps，而IEEE802.11a更可达到54Mbps，这样的速率对于无线网络而言无疑是相当有吸引力的。虽然IEEE802.11a具有明显的速率优势，但成本问题成为制约其发展的绊脚石，因为想要在目前的市场上占据主导地位就必须具有价格优势。从表7.2可见，技术更成熟的是IEEE 802.11b。

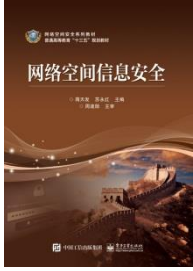


IEEE802.11a .11b .11g的对比

表 7.2　IEEE802.11a, .11b, .11g 的对比

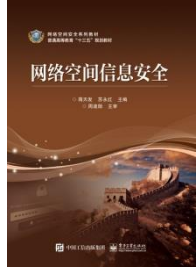
无线标准	802.11b	802.11a	802.11g	802.11n
工作频段	2.4GHz	5GHz	2.4GHz	2.4GHz 和 5GHz.
最大数据率	11Mbps	54Mbps	54Mbps	600Mbps
调制技术	DSSS/CCK	OFDM	OFDM	OFDM
覆盖范围	较大	较大	较小	较大

7.2.4 Wi-Fi技术

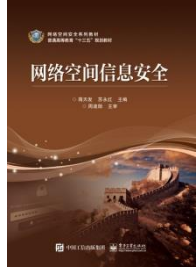


- Wi-Fi目前的验证有WEP、WPA/WPA2、WPS等。但是无线网络存在巨大的安全隐患。
- 1）Wi-Fi钓鱼陷阱
- 许多商家为招揽客户，会提供Wi-Fi接入服务，客人发现Wi-Fi热点，一般会找服务员索要连接密码。黑客就提供一个名称与商家类似的免费Wi-Fi接入点，吸引网民接入。一旦连接到黑客设定的Wi-Fi热点，上网的所有数据包都会经过黑客设备转发，这些信息都可以被截留下来分析，一些没有加密的通信可以直接被查看。

7.2.4 Wi-Fi技术

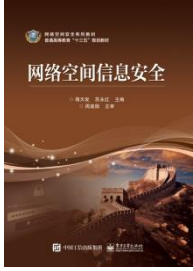


- 2）Wi-Fi接入点被“偷梁换柱”
- 除了伪装一个和正常Wi-Fi接入点雷同的Wi-Fi陷阱之外，攻击者还可以创建一个和正常WiFi名称完全一样的接入点。如果无线路由器信号覆盖不够稳定，手机会自动连接到攻击者创建的WiFi热点。在完全没有察觉的情况下，会又一次掉落陷阱。



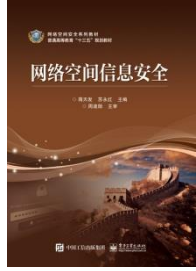
7.2.4 Wi-Fi技术

- 3）黑客主动攻击
- 黑客可以使用黑客工具，攻击正在提供服务的无线路由器，干扰连接，家用型路由器抗攻击的能力较弱，网络连接就这样断线了，继而连接到黑客设置的无线接入点。



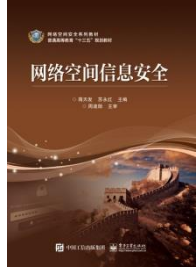
7.2.4 Wi-Fi技术

- 4）攻击家用路由器
- 攻击者首先会使用各种黑客工具破解家用无线路由器的连接密码，如果破解成功，黑客就会成功连接家用路由器，共享一个局域网。攻击者并不甘心免费享用网络带宽，有些人还会进行下一步，尝试登录无线路由器管理后台。由于市面上存在安全隐患的无线路由器相当常见，黑客很可能破解用户的家用路由器登录密码。



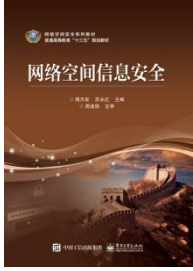
7.2.4 Wi-Fi技术

- 5）劫机风险
- 一名黑客可以使用飞机上的Wi-Fi信号或机上娱乐系统来侵入其航空电子设备，以破坏或修改卫星通信，从而干扰飞机的导航和安全系统。因此，利用飞机Wi-Fi来劫机在理论上是有可能发生的。



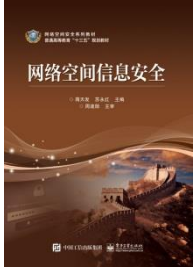
7.2.4 Wi-Fi技术

- 金山毒霸安全工程师为此提供了五大安全使用建议。
- 第一，谨慎使用公共场合的Wi-Fi热点。官方机构提供的而且有验证机制的Wi-Fi，可以找工作人员确认后连接使用。其他可以直接连接且不需要验证或密码的公共Wi-Fi风险较高，背后有可能是钓鱼陷阱，尽量不使用。



7.2.4 Wi-Fi技术

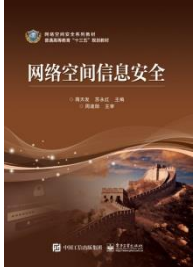
- 第二，使用公共场合的Wi-Fi热点时，尽量不要进行网络购物和网银的操作，避免重要的个人敏感信息遭到泄露，甚至被黑客银行进行转账。
- 第三，养成良好的Wi-Fi使用习惯。进入公共区域后，尽量不要打开Wi-Fi开关，或者把Wi-Fi调成锁屏后不再自动连接，避免在自己不知道的情况下连接上恶意Wi-Fi。



7.2.4 Wi-Fi技术

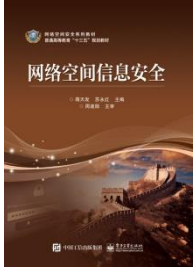
- 第四，家用路由器管理后台的登录账户、密码，不要使用默认的admin，可改为字母加数字的高强度密码；设置的Wi-Fi密码选择WPA2加密验证方式，相对复杂的密码可大大提高黑客破解的难度。
- 第五，不管在手机端还是PC端都应安装安全软件。对于黑客常用的钓鱼网站等攻击手法，安全软件可以及时拦截提醒。

7.3 无线移动通讯技术LTE



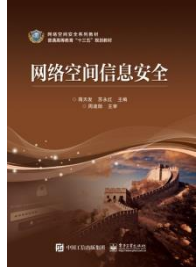
- LTE（Long Term Evolution，长期演进)是由3GPP（The 3rd Generation Partnership Project，第三代合作伙伴计划）组织制定的UMTS（Universal Mobile Telecommunications System，通用移动通信系统）技术标准的长期演进，于2004年12月在3GPP多伦多会议上正式立项并启动。

7.3 无线移动通讯技术LTE



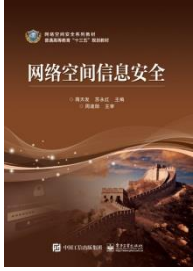
- 目前4G的标准只有两个，分别为LTE Advanced与WiMAX-Advanced。其中，LTE-Advanced就是LTE技术的升级版，在特性方面，LTE-Advanced可以后向兼容技术，并完全兼容LTE，其原理类似HSPA升级至WCDMA这样的关系。
- 而WiMAX-Advanced(全球互通微波存取升级版)：即IEEE 802.16m，是WiMAX的升级版，由美国Intel所主导，接收下行与上行最高速率可达到300Mbps，在静止定点接收可高达1Gbps/s。也是电信联盟承认的4G标准。

7.3 无线移动通讯技术LTE



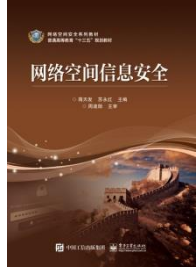
- 实际来说，我们目前接触的LTE并非4G网络，虽然上百兆的速度远超3G网络，但与ITU提出的1Gbps/s的4G技术要求还有很大距离，因此，目前的LTE也经常被称为3.9G。但就目前来说，现在的4G网络其实指的的就是LTE网络。

7.3 无线移动通讯技术LTE



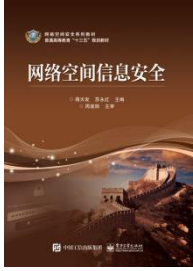
- 从移动通信技术的发展来看:
- 1G网络：使用蜂窝组网，采用模拟技术和频分多址（FDMA）等技术。
- 2G网络：目前使用最为广泛的通信系统，主要使用技术是时分多址(TDMA)技术，如GSM网络
- 3G网络:国际标准有WCDMA、CDMA2000、TD-SCDMA。 技术指标：室内速率2Mbps，室外384kbps，行车速率144kbps。能够实现语音业务、高速传输及无线接入Internet等服务
- LTE网络：采用OFDM及MIMO技术，在20MHz的系统带宽下，下行峰值速率100Mbps，上行50Mbps(现有UE能力支持)，提供VoIP及IMS等高速数据传输服务。

7.3 无线移动通讯技术LTE



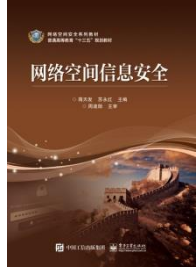
- LTE系统引入了OFDM（Orthogonal Frequency Division Multiplexing，正交频分复用）和MIMO（Multi-Input & Multi-Output，多输入多输出）等关键技术，根据实际组网以及终端能力限制，一般认为下行峰值速率为100Mbps，上行为50Mbps。它支持多种带宽分配：1.4MHz，3MHz，5MHz，10MHz，15MHz和20MHz等，且支持全球主流2G/3G频段和一些新增频段，因而频谱分配更加灵活，系统容量和覆盖也显著提升。LTE系统支持与其他3GPP系统互操作。

7.3 无线移动通讯技术LTE



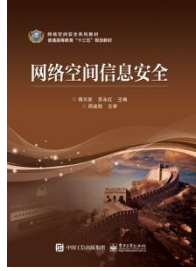
- LTE网络由用户设备（UE）、接入网及核心网组成。其针对空中接口和核心网络的演进技术分别被称为演进的通用陆地无线接入网（Evolved Universal Terrestrial Radio
- Access Network，E-UTRAN）和演进的分组核心系统。（Evolved Packet Core,EPC）.因此LTE网络有时也被称为演进的分组系统（Evolved Packet System, EPS）.

7.3 无线移动通讯技术LTE



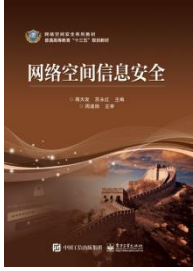
- 根据双工方式不同LTE系统分为FDD-LTE（Frequency Division Duplexing）和TDD-LTE (Time Division Duplexing)，二者技术的主要区别在于空口的物理层上（像帧结构、时分设计、同步等）。而中国移动采用的TD-LTE就是LTE-TDD版本，同时也是由中国主导研制推广的版本。TD-LTE与TD-SCDMA实际上没有关系，TD-SCDMA是CDMA(码分多址)技术，TD-LTE是OFDM(正交频分复用)技术。两者从编解码、帧格式、空口、信令，到网络架构，都不一样。
- **TD-LTE的工作频段**在R8中，TDD可用的频段从33到40号，有8个。其中B38：2.57~2.62GHz，可全球漫游；B39：1.88~1.92GHz，这是国内TD-SCDMA的频段；B40：2.3~2.4GHz，可全球漫游。B是Band的缩写，代表频段的意思。

7.3 无线移动通讯技术LTE



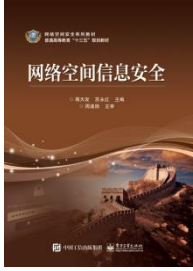
- 这些频段中，中国移动采用B38以及B39来实施室外覆盖，B40来实施室内覆盖。B38、B39、B40在中国移动分别又有绰号：D频段、F频段和E频段。
- 到了R10，3GPP又引入了新的TDD频段，其中B41为2500~2690MHz，非常重要。因为中国政府已经宣布，将B41的全部频段用于TD-LTE。

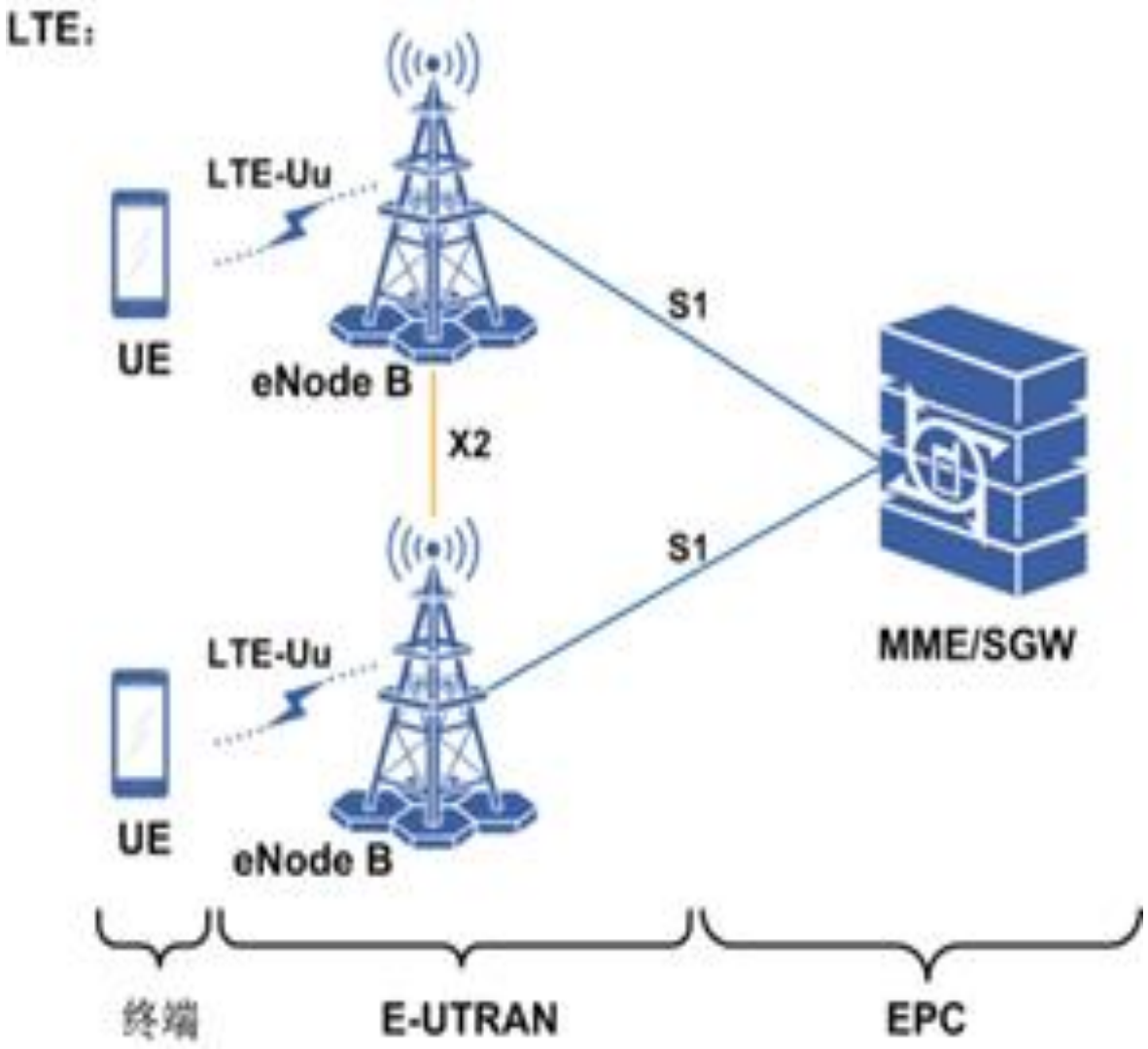
7.3.2 LTE 网络架构



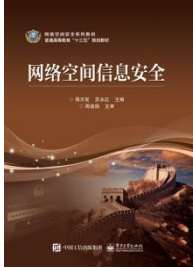
- LTE系统只存在分组域。分为两个网元，EPC（Evolved Packet Core，演进分组核心网）和eNode B（Evolved Node B，演进Node B）。EPC负责核心网部分，信令处理部分为MME（Mobility Management Entity，移动管理实体），数据处理部分为S-GW（Serving Gateway，服务网管）。eNode B负责接入网部分，也称E-UTRAN（Evolved UTRAN，演进的UTRAN），如图

7.3.2 LTE 网络架构


网络空间信息安全

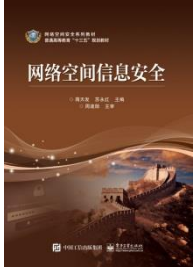

LTE:
LTE-Uu
UE
eNode B
X2
S1
S1
MME/SGW
LTE-Uu
UE
eNode B
终端
E-UTRAN
EPC

7.3.2 LTE 网络架构

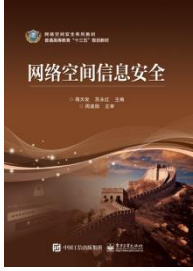


- eNode B与EPC通过S1接口连接；eNode B之间通过X2接口连接；eNode B与UE之间通过Uu接口连接。
- MME的功能主要包括：寻呼消息发送；安全控制；Idle状态的移动性管理；SAE承载管理；以及NAS信令的加密与完整性保护等。
- SGW的功能主要包括：数据的路由和传输，以及用户数据的加密。

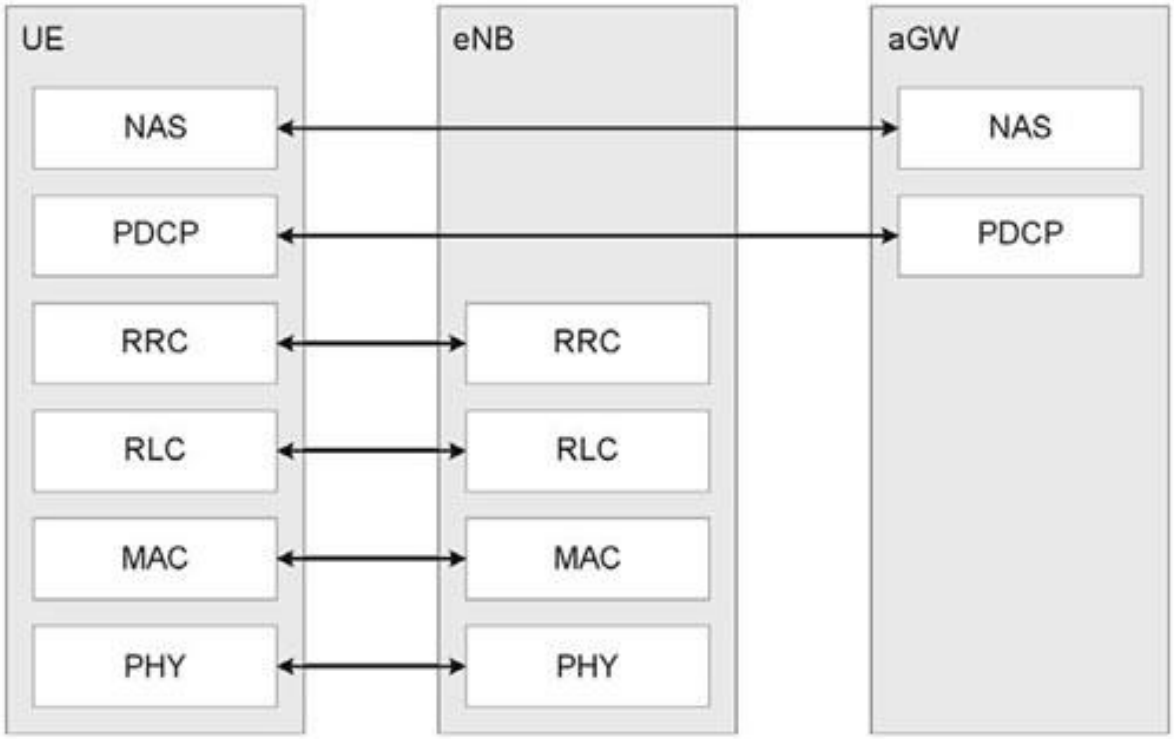
7.3.3 LTE无线接口协议



- 空中接口是指终端和接入网之间的接口，简称Uu口通常也称之为无线接口。无线接口协议主要是用来建立、重配置和释放各种无线承载业务。无线接口协议栈根据用途分为用户平面协议栈和控制平面协议栈。

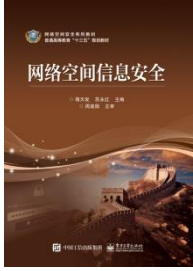


控制平面协议

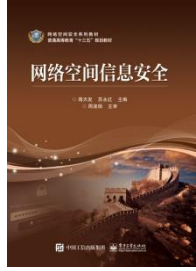


控制平面负责用户无线资源的管理，无线连接的建立，业务的QoS保证和最终的资源释放

7.3.3 LTE无线接口协议

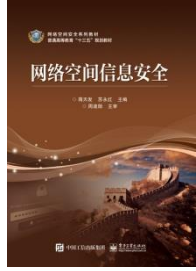


- 控制平面协议栈主要包括非接入层（Non-Access Stratum，NAS）、无线资源控制子层（Radio Resource Control，RRC）、分组数据汇聚子层（Packet Date Convergence Protocol，PDCP）、无线链路控制子层（Radio Link Control，RLC）及媒体接入控制子层（Media Access Control，MAC）。
- 控制平面的主要功能由上层的RRC层和非接入子层（NAS）实现。
- NAS控制协议实体位于终端UE和移动管理实体MME内，主要负责非接入层的管理和控制。实现的功能包括：EPC承载管理，鉴权，产生LTE-IDLE状态下的寻呼消息，移动性管理，安全控制等。



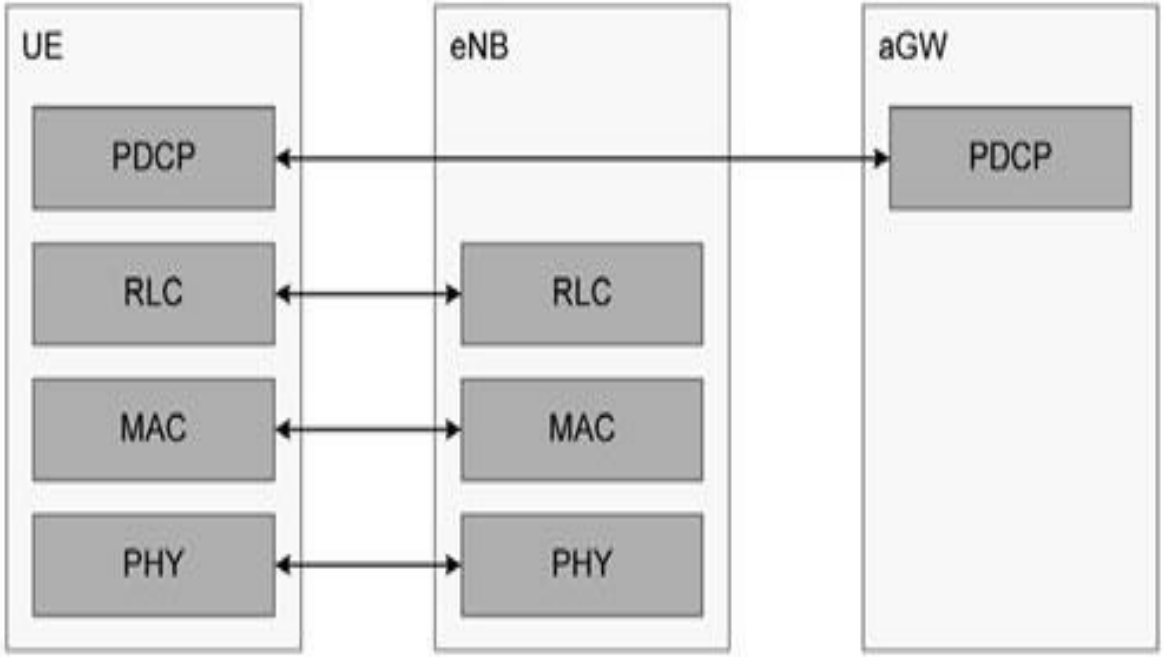
7.3.3 LTE无线接口协议

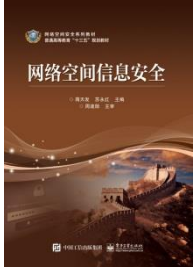
- RRC协议实体位于UE和eNode B网络实体内，主要负责接入层的管理和控制，实现的功能包括：系统消息广播，寻呼建立、管理、释放，RRC连接管理，无线承载（Radio Bearer，RB）管理，移动性功能，终端的测量和测量上报控制。
- PDCP、MAC和RLC的功能和在用户平面协议实现的功能相同



用户平面协议

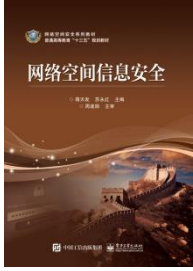
用户平面用于执行无线接入承载业务，主要负责用户发送和接收的所有信息的处理





7.3.3 LTE无线接口协议

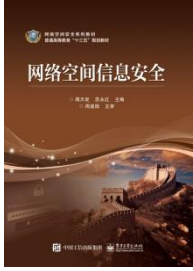
- 用户平面协议栈主要由MAC，RLC，PDCP三个子层构成。
- PDCP主要任务是头压缩，用户数据加密。
- MAC子层实现与数据处理相关的功能，包括信道管理与映射、数据包的封装与解封装，HARQ功能，数据调度，逻辑信道的优先级管理等。
- RLC实现的功能包括数据包的封装和解封装，ARQ过程，数据的重排序和重复检测，协议错误检测和恢复等。
- 另外，LTE还有S1接口协议和X2接口协议。



7.3.4 LTE关键技术OFDM和MIMO

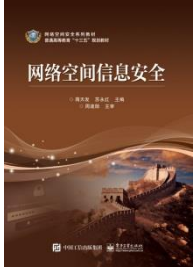
- 以公示C = B x V为例，C表示为速率，B是带宽，V是每Hz的速率，通过公式我们可以发现，想提高网络的速度有2个方法，一个是增加带宽，一个是增加频带利用率。LTE提高网路速度也是用这2个方法。

7.3.4 LTE关键技术OFDM和MIMO



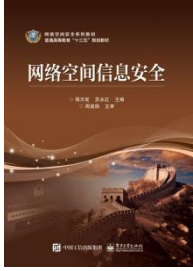
- 首先讲讲增加带宽，这个技术直接导致CDMA技术在4G被pass的原因之一。如果将一个通信技术的频谱从 1.25MHz扩展到20MHz，要面临很多的问题，第一个是多载波的聚合，举个例子，你原来只需要管理个单车道，现在突然给你个100车道，一个是协调问题，要保证不乱，其次调度问题，要保证高效，所以复杂程度大大的增加。第二个是频谱特性问题，如果你真的用一个20Mhz的载波，跨度那么大，频率特性就很难兼顾，包括传播特性，扩频效率等，另外包太大的话调度的精度也受影响，因此LTE选择含正交子载波技术的OFDM技术来实现多增加带宽。

7.3.4 LTE关键技术OFDM和MIMO

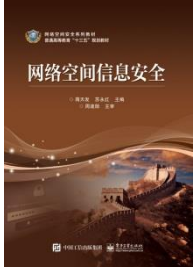


- 其次就是增加频带利用率，信源要最终发射必须要经过编码和调制，编码的作用是将前后的信息位建立联系并最终保证纠错，相当于一种冗余，而调制的方式则是通过相位来区别更多的符号，相当于一种压缩，那么高效的编码和高阶的调制无疑会增加频谱利用率，LTE支持MIMO也是一种增加频谱利用率的方式。

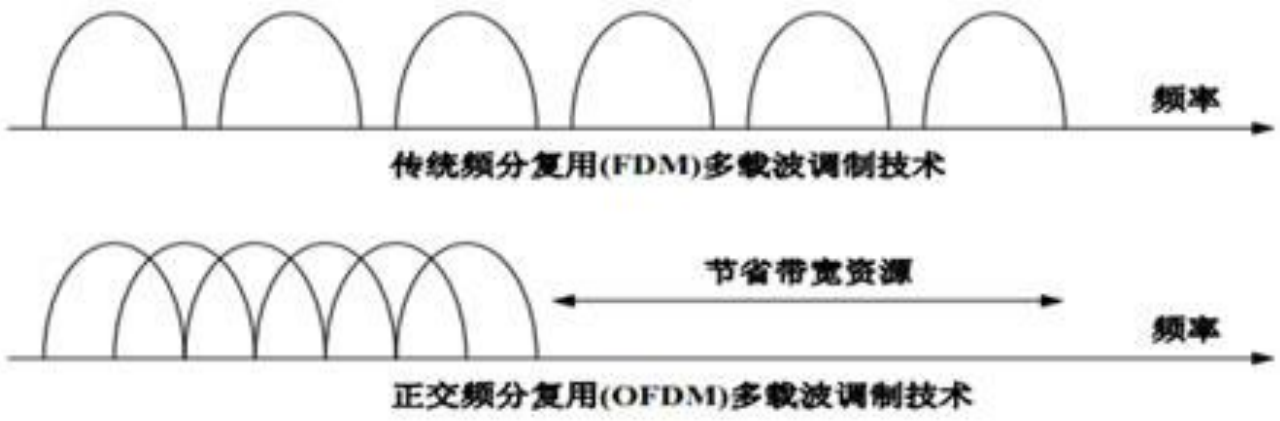
7.3.4 LTE关键技术OFDM和MIMO



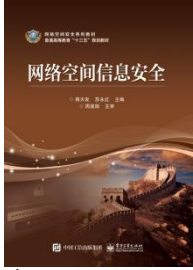
- **OFDM（orthogonal frequently division multiplexing）正交频分复用。**
- OFDM原理就是将大的频谱分为若干小的子载波，各相邻子载波相互重叠，相邻子载波互相正交（通过傅里叶变换实现），从而使其重叠但不干扰。之后将串行数据映射到子载波上传输，实现统一调度，见图


网络空间信息安全

OFDM技术

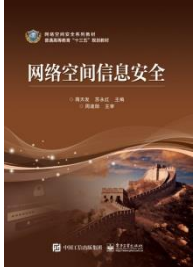

频率
传统频分复用(FDM)多载波调制技术
节省带宽资源
频率
正交频分复用(OFDM)多载波调制技术

7.3.4 LTE关键技术OFDM和MIMO



- 和传统的FDM多载波调制技术的区别:传统的多载波是分开的，载波之间要有保护间隔，OFDM则是重叠在一起的，最大的一个好处就是节省了带宽。同时OFDM是统一调度，而传统的FDM是子载波分别调度，效率是不一样的。
- OFDM的子载波也不同于传统的载波，他非常小，小于信道相干带宽，这样的好处是可以克服频率选择性衰落，举个例子，1hz和1.1hz之间的无线特性几乎一样，而1hz和101hz之间的无线特性就差别大了，带宽越小，衰落越一致，同理一个OFDM符号的时间也是很小的，小于相干时间可以克服时间选择性衰落，等效为一个线性时不变系统。

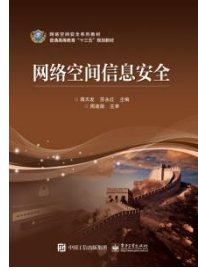
7.3.4 LTE关键技术OFDM和MIMO



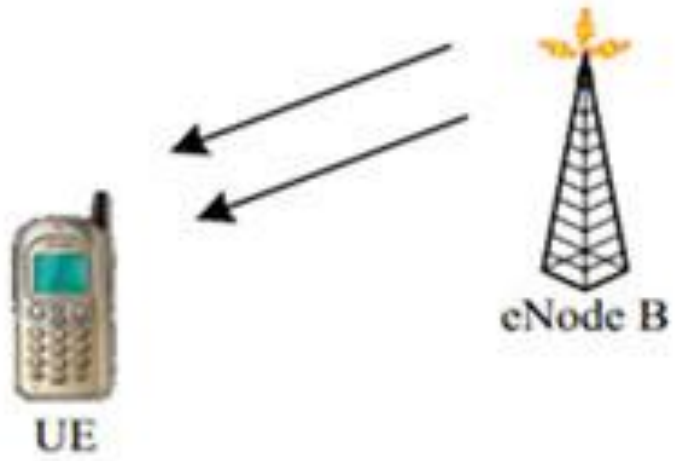
- 而对于OFDM来说，最难的还是在于如何保证各个子载波间的正交，其重要的一点就是利用了快速傅里叶变换，还有就是近代芯片运算能力的增加。
- OFDM有很多优点，但是也有其不可克服的缺点，如由于一个OFDM符号时间和频率都很小所以对频偏比较敏感，还有由于信号重叠厉害就会需要克服较大的峰均比PARA。

MIMO(Multiple-Input Multiple-Out-put)

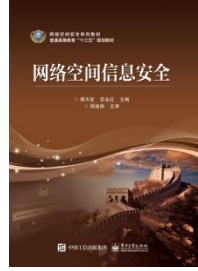
- MIMO技术可以说是4G必备的技术，无论哪种4G制式都会用，原理是通过收发端的多天线技术来实现多路数据的传输，从而增加速率。
- MIMO大致可以分为3类，空间分集，空间复用和波束赋形。有的资料加了一个多用户MIMO，其实就是单用户的一个引申。
- 1、空间分集（发射分集、传输分集）
- 利用较大间距的天线阵元之间或赋形波束之间的不相关性，发射或接收一个数据流，避免单个信道衰落对整个链路的影响。其实很简单，看图



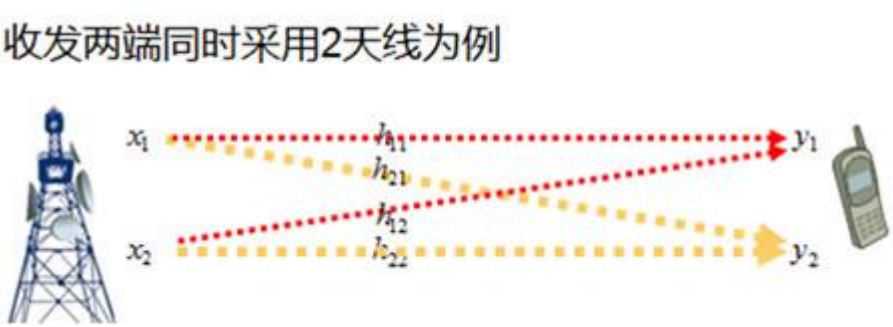
空间分集

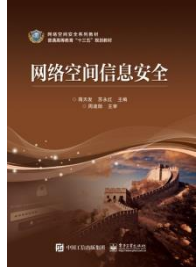


- SU-MIMO: 发射分集
- 只传给UE一个数据流



- 其实说白了，就是2根天线传输同一个数据，但是2个天线上的数据互为共轭，一个数据传2遍，有分集增益，保证数据能够准确传输。
- 2、空间复用（空分复用）
- 利用较大间距的天线阵元之间或赋形波束之间的不相关性，向一个终端/基站并行发射多个数据流，以提高链路容量（峰值速率），见上图





- 如果上一个技术是增加可靠性，这个技术就是增加峰值速率，2个天线传输2个不同的数据流，相当于速率增加了一倍，当然，必须要在无线环境好的情况下才行。
- 另外注意一点，采用空间复用并不是天线多了就行，还要保证天线之间相关性低才行，否则会导致无法解出2路数据可以通过数学公式来阐明。假设收发双方是MIMO2*2，如图

MIMO(Multiple-Input Multiple-Out-put)

- 那么UE侧的计算公式是

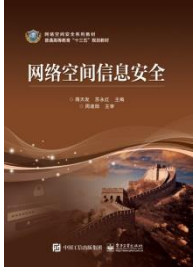
$$y_1 = h_{11}x_1 + h_{12}x_2 + n_1$$
$$y_2 = h_{21}x_1 + h_{22}x_2 + n_2$$

- 由于是UE接收，所以y1和y2都知道，h和n是天线的相关特性也都知道，求x。假如天线的相关性较高，h11和h21相等，h12和h22相等，或者等比例，那么这个公式就无解。
-

$$3 = 2x_1 + 5x_2 + 1$$

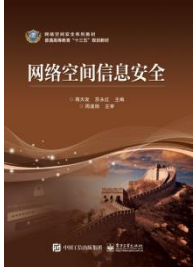
$$6 = 4x_1 + 10x_2 + 2$$

MIMO(Multiple-Input Multiple-Out-put)

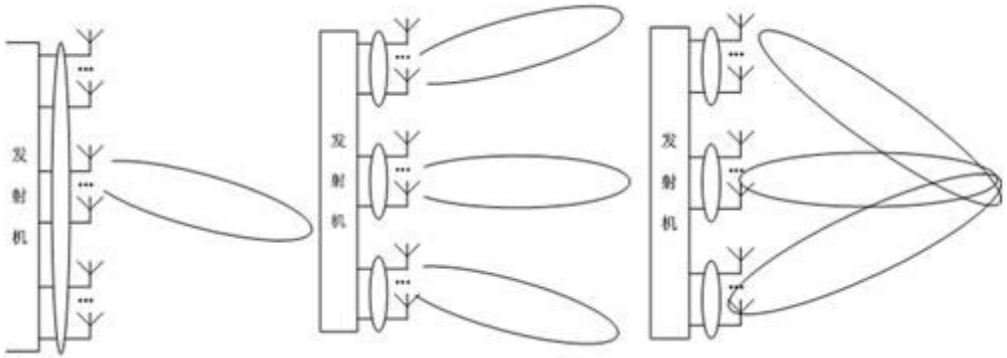


- 是一个二元一次方程，由于上下两个方程成比例，所以无法解出x1和x2的。也就无法使用空间复用，因为这两根天线相关性太高了，如果想解决的话，可以增加天线的间隔从而使h不成比例，一般建议大于4倍波长，具体要看天线说明。

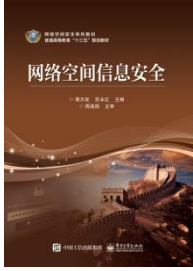
MIMO(Multiple-Input Multiple-Out-put)



- 利用较小间距的天线阵元之间的相关性，通过阵元发射的波之间形成干涉，集中能量于某个（或某些）特定方向上，形成波束，从而实现更大的覆盖和干扰抑制效果，见图７.１６：

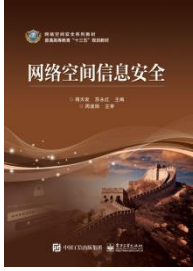


MIMO(Multiple-Input Multiple-Out-put)



- 上面是单播波束赋形，波束赋形多址和多播波束赋形，通过判断UE位置进行定向发射，提高传输可靠性。这个在TD-SCDMA上已经得到了很好的应用。
- 而 至于多用户MU-MIMO，实际上是将两个UE认为是一个逻辑终端的不同天线，其原理和单用户的差不多，但是采用MU-MIMO有个很重要的限制条件，就 是这2个UE信道必须正交，否则解不出来。这个在用户较多的场景还行，用户少了的话很难找到。（也有种说法只要相关性弱就行）

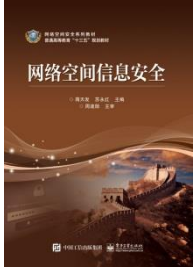
MIMO(Multiple-Input Multiple-Out-put)



- 目前的R8版本主要分了7类MIMO，具体现网中使用哪种需要网管人员结合实际情况去设置相关的门限和条件。下面列出这7类分别讲解下原理和适用场景

MIMO(Multiple-Input Multiple-Out-put)

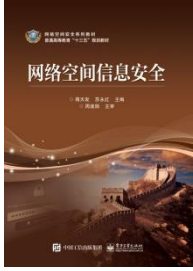
- （1）单天线传输，也是基础模式，兼容单天线ue。
- （2）不同模式在不同天线上传输同一个数据，适用于覆盖边缘。
- （3）开环空分复用，无需用户反馈，不同天线传输不同的数据，相当于速率增加一倍，适用于覆盖较好区域
- （4）同上，只不过增加了用户反馈，对无线环境的变化更敏感



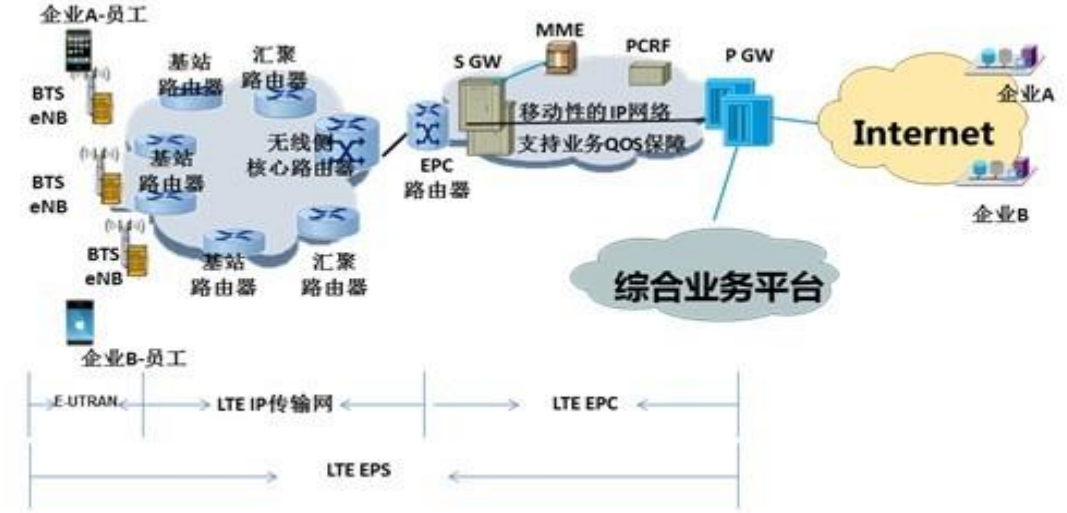
MIMO(Multiple-Input Multiple-Out-put)

- （5）多个天线传输给多个用户，如果用户较多且每个用户数据量不大的话可以采用，增加小区吞吐量。
- （6）闭环波束赋形一种，基于码本的（预先设置好），预编码矩阵是在接收端终端获得，并反馈PMI，由于有反馈所以可以形成闭环。
- （7）无需码本的波束赋形，适用于TDD，由于TDD上下行是在同一频点，所以可以根据上行推断出下行，无需码本和反馈，FDD由于上下行不同频点所以不能使用。

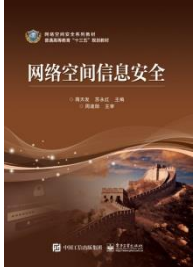
7.3.5 LTE架构安全



- LTE的网络从空口无线侧开始就是IP网络，同时智能终端只要开启电源就会附着IP地址，因而智能终端、LTE无线接入侧、传输网侧和EPC(核心网)都面临着原来IP网络固有的安全威胁，图

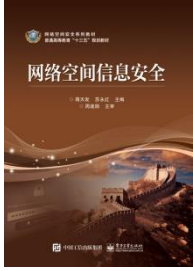


7.3.5 LTE架构安全



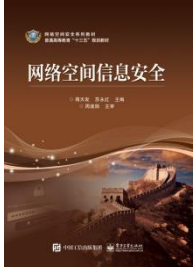
- 这些安全威胁如下：
  1）无线侧智能终端面临僵木蠕、恶意代码等攻击；
  2）无线智能侧终端成为DDoS攻击源，进而对整个LTE EPS网络发起DDoS 攻击；
  3）EPC核心网元面临信令风暴问题；
  4）智能终端通过LTE EPC、Internet等非信任网络时进行明文传输敏感数据时，面临泄露数据的问题；(例如企业A-员工 利用智能终端APP通过LTE EPS访问互联网的企业A 内部的关键数据库时，通过的开放的Internet网络时面临敏感数据给窃听的问题)

7.3.5 LTE架构安全



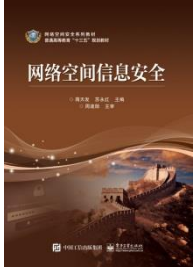
- 5)LTE EPS综合业务平台面临攻击的威胁；
  6)EPC Pi口(P GW<->Internet)面临来自Internet攻击的威胁；
  7）前IPv4地址早已分配完，如何在4G 移动互联网中应对持续发展的数据业务；
  8）合业务平台如何更好地进行流量经营、如何构建有价值的管道；
- 通过在不同的位置部署不同功能的网络设备可以从网络层面有效解决LTE EPS上述的网络安全及业务问题。

7.3.5 LTE架构安全



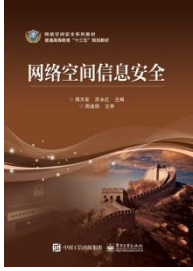
- 针对第一个问题，可通过在EPC中部署手机恶意代码检测及分析系统，类似在3G网络中应对该问题一样，但在4G网络中，由于带宽的大幅提升，因而该检测分析系统必须有足够性能及容量来应对4G网络中恶意代码检测的要求。
- 针对流量攻击及信令风暴的问题，可通过在传输接入侧部署流量采集分析设备，结合运营商本身的网络安全管理平台来进行基于流量、信令等安全事件的分析，及时发现和防范该类型的攻击，保障移动网的正常运营。

7.3.5 LTE架构安全



- 针对第四个面临的安全问题，根据不同的应用场景来部署不同的IPSec 网关来解决。
- 如果传输回送网络对移动运营商来说是非自建网络（例如移动运营商可以向固网运营商租用相关的传输网络进行数据业务的传输）的情况下，为了保障客户关键敏感的数据及语音在非信任的第三方网络上进行安全传输则可以在EPC网络中加入大容量IPsec网关，针对不同eNodeB与该IPSec 网关启用 IPSec隧道进行数据加密传输；而传输网和EPC为运营商自建的网络情况下，为保障客户关键敏感的数据在非信任的Internet 上进行传输，则可在P-GW处侧挂高性能IPSec网关，与对端企业机构互联网出口的IPSec网关进行加密传输，为客户提供数据加密传输的安全服务。

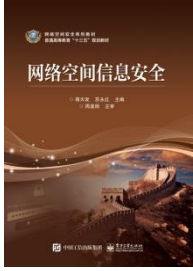
7.3.5 LTE架构安全



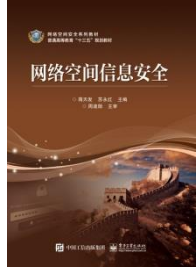
- 针对5-8的问题，可在P-GW侧挂高性能设备来解决网络安全及数据业务问题。在Pi口部署安全智能设备能将Internet与EPC间、Internet与业务平台间进行安全隔离，对EPC网元进行安全保护，该设备具备相应的CGN及智能分流功能，能对IPv4地址进行高效复用，在IPv6未成熟正式商用前能应对运营商数据业务的急速发展，同时该设备针对数据流的应用层做深度分析及后续引流、重定向的功能，对向往运营商非流量经营平台的流量进行直接转发到Internet上，节省流量经营平台的压力，提升客户上网的体验。由于Pi口部署的设备具备解决上述问题的能力，因而该设备不单纯是个安全设备或者应用交付设备或DPI，而是一个高性能的综合承载网元设备

LTE　EPS 安全及业务实施逻辑图

7.4 无线网络结构及实现



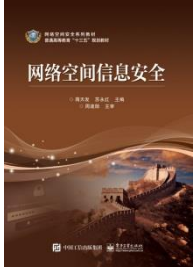
- 无线局域网可以在普通局域网基础上通过无线Hub、无线接入站（Access Point，AP,亦称网络桥接器）、无线网桥、无线Modem及无线网卡等来实现，以无线网卡最为普遍，使用最多。与有线网络一样，无线局域网同样也需要传送介质。但它不是使用双绞线或者光纤，而是使用红外（IR）或者射频（RF）波段,无线局域网一般普遍采用扩频微波技术。
- 一般来讲，无线局域网有两种拓扑结构：有中心拓扑和无中心拓扑。一般来讲，无中心拓扑也称为没有基础设施的无线局域网，有中心拓扑也称为有基础设施的无线局域网。细分来看，主要包括以下几种结构：



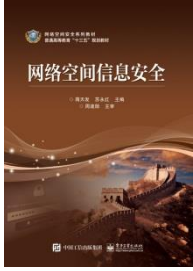
7.4 无线网络结构及实现

- 点对点模式；
- 基础结构模式；
- 多AP模式；
- 中继模式；
- Mesh结构；

7.4 无线网络结构及实现

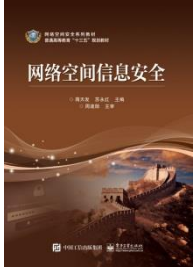


- （1）点对点模式，无中心拓扑或者无基础设施的无线局域网的典型组网方式为点对点模式Ad-hoc，也叫做对等结构模式或者称为自组织网络/移动自组网。
- 它覆盖的服务区被称为独立基本服务区。对等网络用于一台无线工作站与另一台或多台其他无线工作站直接通信，该网络无法接入有线网络中，只能独立使用。对等网络中的一个节点必需能同时“看”到网络中的其他节点，否则就认为网络中断。因此对等网络只能用于少数用户的组网环境，比如4至8个用户，并且他们离得足够近。
- 这种拓扑的网络无法接入到有线网络中，只能独立使用，无需AP，安全等功能由各个客户端自行维护。



7.4 无线网络结构及实现

- 移动自组网采用非集中式的MAC协议。
- 基本服务区由一个无线访问点以及与其关联（Associate）的无线工作站构成，在任何时候，任何无线工作站都与该无线访问点关联。换句话说，一个无线访问点所覆盖的微蜂窝区域就是基本服务区。无线工作站与无线访问点关联采用AP的基本服务区标示符（BSSID），在802.11中，BSSID是AP的MAC地址。图7.2 0 为对等网络拓扑结构：



7.4 无线网络结构及实现

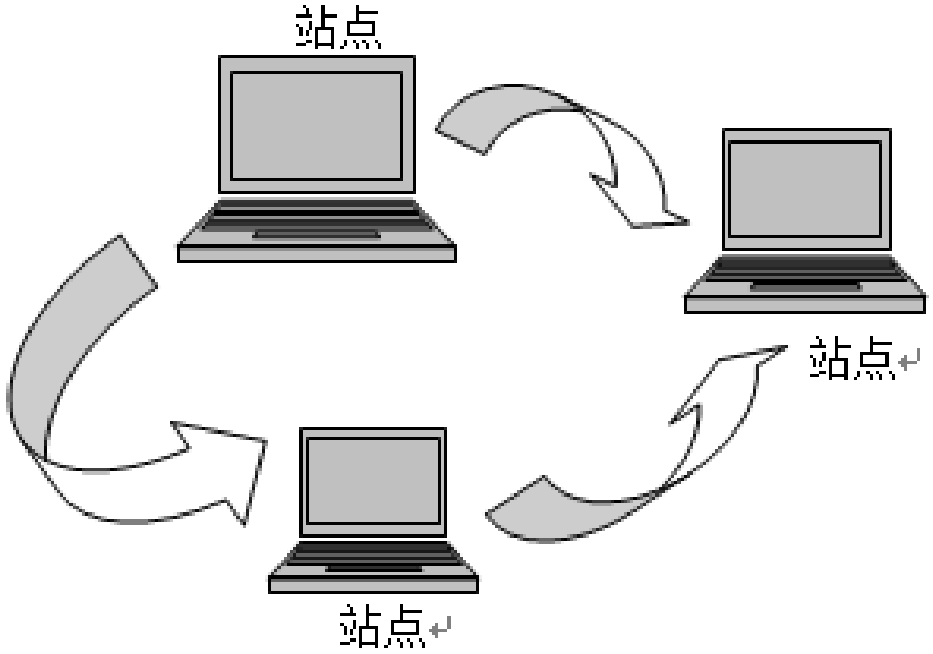
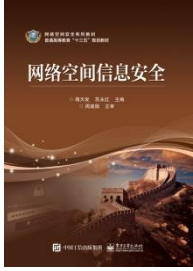


图 7.20 对等网络拓扑结构

7.4 无线网络结构及实现



- 对等网络拓扑结构的优点是建网容易、费用低、可移动性强。缺点主要有三个：一是用户数过多也就是站点过多容易引起信道竞争。二是用户数增加时路由信息也会增加，严重时会占据有效通信。三是站点布局受环境和覆盖范围限制。
- （2）基础结构模式。由无线访问点（AP）、无线工作站（STA）以及分布式系统（DSS）构成，覆盖的区域分为基本服务区（BSS）和扩展服务区（ESS）。无线访问点也称无线Hub，用于在无线STA和有线网络之间接收、缓存和转发数据。无线访问点能够覆盖几十至几百用户，覆盖半径达上百米。基础结构模式的拓扑结构如图7.2 1 所示：

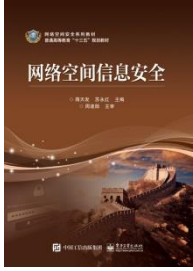
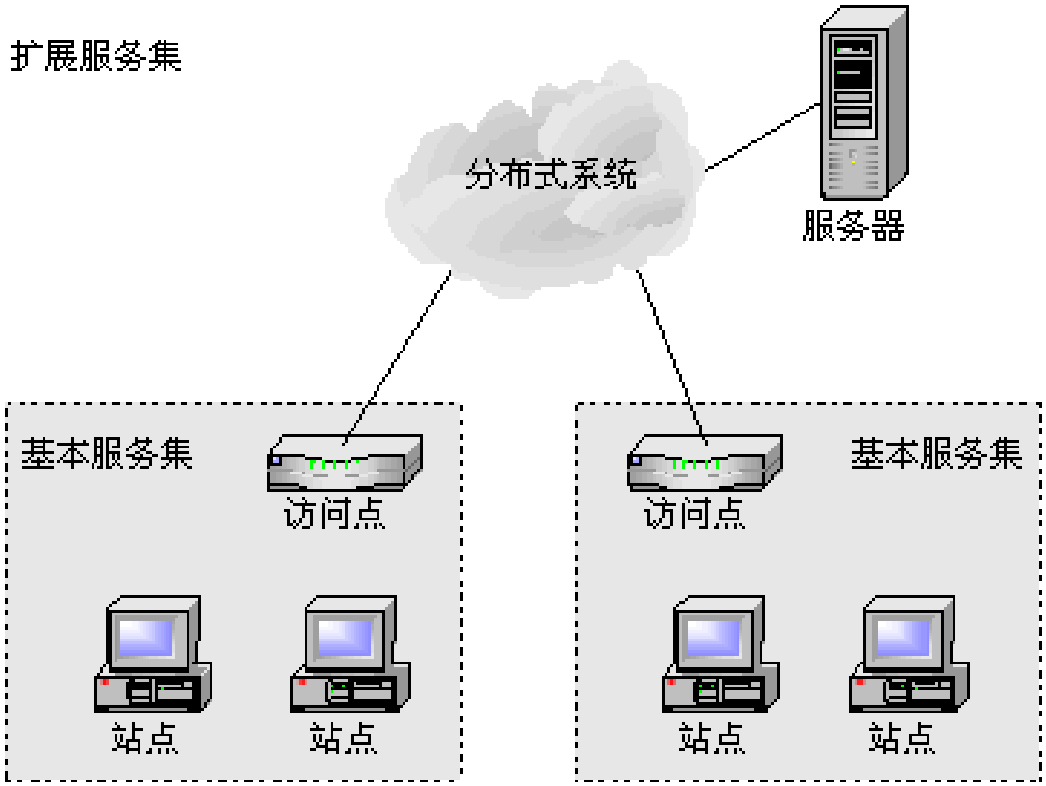
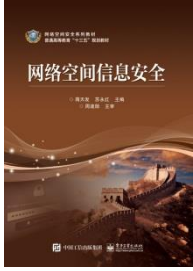


图7.2 1 基础结构模式

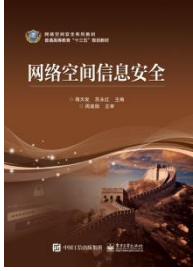


7.4 无线网络结构及实现



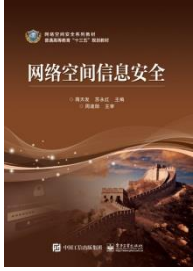
- 扩展服务区是指由多个AP以及连接它们的分布式系统组成的结构化网络，所有AP必需共享同一个扩展服务区标示符（ESSID），也可以说扩展服务区ESS中包含多个BSS。分布式系统在IEEE 802.11标准中并没有定义，但是目前大都是指以太网。扩展服务区是一个Layer 2网络结构，对于高层协议比如IP来说，它是一个子网。
- 从应用角度出发，绝大多数无线局域网都属于有中心网络拓扑结构。
- 基础结构网络也使用非集中式MAC协议。但有中心网络拓扑的抗摧毁性差，AP 的故障容易导致整个网络瘫痪。

7.4 无线网络结构及实现



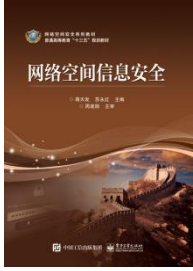
- （3）多AP模式
- 多AP模式指由多个AP以及连接它们的分布式系统DSS组成的基础结构模式。
- 每个AP是一个独立的BSS，多个BSS组成一个扩展服务集ESS（extended service set）。ESS内所有AP共享同一个扩展服务器标示符ESSID（extended service set identifier）。
- DSS在802.11中并没有定义，目前多指以太网。相同ESSID之间可以漫游，不同ESSID的无线网络形成不同的逻辑子网。

7.4 无线网络结构及实现

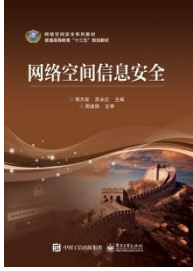


- 多AP模式也称为“多蜂窝结构”。各个蜂窝之间建议由15%的重叠范围，便于无线工作站的漫游。漫游时必须进行不同AP接入点之间的切换。切换可以通过交换机以集中的方式控制，也可以通过移动节点、监测节点的信号强度来控制（非集中控制方式）。
- 在有线不能到达的环境，可以采用多蜂窝无线中继结构。但这种结构中要求蜂窝之间要有50%的信号重叠。同时客户端的使用效率会下降50%。

7.4 无线网络结构及实现

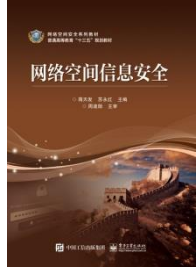


- （4）无线网桥模式
- 利用一对无线网桥连接两个有线或者无线局域网网段。使用放大器和定向天线可以覆盖距离增大到50Km。
- （5）AP client客户端模式
- 将部分AP设置为AP client模式，远端AP作为终端访问中心AP。
- 应用在室外，相当于点对多点的连接方式。区别在于：中心接入点把远端局域网看成像一个无线终端的接入，不限制接入远端AP client模式的无线接入点连接的局域网络数量和网络连接方式。



7.4 无线网络结构及实现

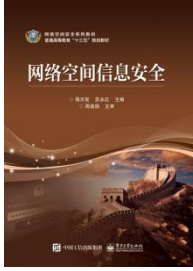
- (6) Mesh结构
- IEEE802.16—2004标准定义了两种网络拓扑：一种是点到多点（point to Multi-Point,PMP）的蜂窝网结构；另一种是Mesh结构。
- Mesh结构也叫无线网状网。网络中的每个节点都可以发送和接收信号。无线Mesh网络也称为“多跳（Multi-hop）”网络。
- 由一组呈网状分布的无线AP构成，AP之间均采用点对点方式通过无线中继链路互联，将传统的无线“热点”扩展为真正大面积覆盖的无线“热区”。



7.4 无线网络结构及实现

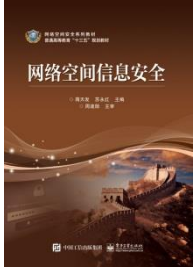
- Mesh网络中的AP之间通过无线方式“直达”，无需有线中转。且具有宽带无线汇聚连接功能，有效的路由和故障发现特性。因此更适合与大规模的无线网络配置。
- 与传统的交换式网络相比，Mesh网络没有布线的需求，但仍具备分布式网络提供的冗余机制和重新路由能力。

7.4 无线网络结构及实现

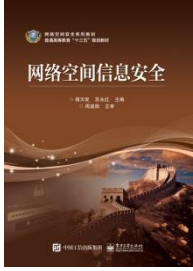


- 它的优点：
- （1）快速部署和易于安装。因为不需要进行布线，所以设备安装非常快速简单。而设备的配置和其他网络管理功能与传统WLAN相同。因此可以大大降低总拥有成本（TCO）和安装时间。
- （2）非视距传输（NLOS）。AP之间的无线互联，有效的路由发现特性和“多跳”网络的本质使具有直接视距的用户实际上为没有直接视距的邻近用户提供了无线宽带访问能力。
- （3）健壮性。Mesh结构网络中，由于每个站点都有一条或者几条传输数据的路径，某个节点出现故障或者被干扰，数据将自动路由到备用链路。

7.4 无线网络结构及实现



- （4）结构灵活。多跳网络中，设备可以通过不同的节点同时连接到网络，因此不会降低系统性能。
- （5）更大的冗余机制和通信负载平衡功能。每个设备都有多个传输路径可用，网络可以根据每个节点的负载动态分配路由，避免节点拥塞。
- （6）高带宽。节点之间中继，使相邻节点之间的通信距离变短，对于无线通信来讲，带宽就越高。
- （7）功能消耗小。因为相邻节点之间的距离短，因此所需的信号功率也小。相应的，节点之间的无线信号干扰也较小。



7.4 无线网络结构及实现

- Ｍｅｓｈ结构的缺点在于：
- （1）兼容性问题。当前的Mesh网络产品没有统一的技术标准，用户选择产品时必须考虑兼容性问题。
- （2）通信延迟。由于网络数据传输的多跳特性，较远距离的通信数据传输延迟较大。
- （3）数据安全问题。网络的多跳特性使数据过多的暴露在公共环境，对于数据的安全提出了更过的要求。

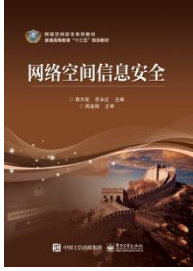
7.4 无线网络结构及实现

- 对于不同局域网的应用环境与需求，无线局域网可采取以下不同的网络结构来实现互连。
- （1）网桥连接型：不同的局域网之间互连时，由于物理上的原因，若采取有线方式不方便，则可利用无线网桥的方式实现二者的点对点连接，无线网桥不仅提供二者之间的物理与数据链路层的连接，还为两个网的用户提供较高层的路由与协议转换。
- （2）基站接入型：当采用移动蜂窝通信网接入方式组建无线局域网时，各个站点之间的通信是通过基站接入、数据交换方式来实现互连的。各移动站不仅可以通过交换中心站点自行组网，还可以通过广域网与远地站点组建自己的工作网络。

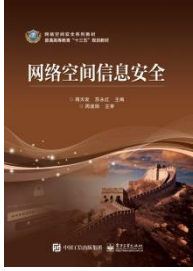
7.4 无线网络结构及实现

- （3）Hub接入型：利用无线Hub可以组建星型结构的无线局域网，具有与有线Hub组网方式相类似的优点。在该结构基础上的无线局域网，可采用类似于交换型以太网的工作方式，要求Hub具有简单的网内交换功能。
- （4）无中心结构：网中任意两个站点可直接通信。此结构一般使用公用广播信道，MAC层采用CSMA类型的多址接入协议。

7.5 无线网络的安全性



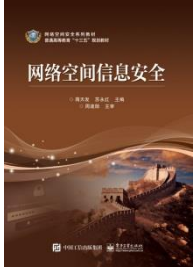
- 对无线网络进行入侵首先可以采用射频干扰的方法在信号级切断信息传播的通道。不管是有意还是无意，只要噪声的功率大于信号功率，在接收端信噪比差到一定程度，就会出现误码，甚至无线传输链路彻底中断。黑客入侵无线网络的以下手法如下：
- 方法一：利用现在的开放网络。
- 黑客扫瞄所有开放型的无线接入点(无线路由器和无线AP)，其中，部分网络的确是专供大众使用，但多数则是因为使用者没有做好安全设置，门户大开。入侵者的企图是免费上网、透过网络攻击第三方或探索其它人的网络。

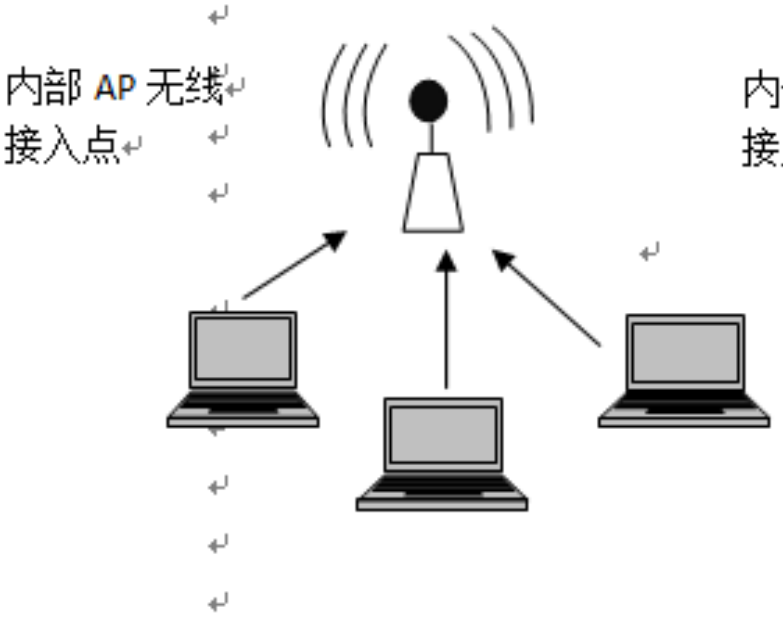


7.5 无线网络的安全性

- 方法二：无线伪装
- 伪造AP基站的攻击主要有以下目的：
- (1)伪装成正常的工作基站，使得合法客户端连接到此基站，达到转发客户端网络连接请求，以便截获其中内容的目的。
- (2)恶意创建大量虚假AP基站，干扰正常无线通信。
- (3)由间谍或被收买的内部成员在内部有线网络设备上偷偷搭建非法AP，从外部可以轻松渗透高强度安全环境，如采用内外网隔离的机构。
- 攻击者会通过搭建非法AP基站的途径来进行无线网络攻击，如图7.22所示：

7.5 无线网络的安全性





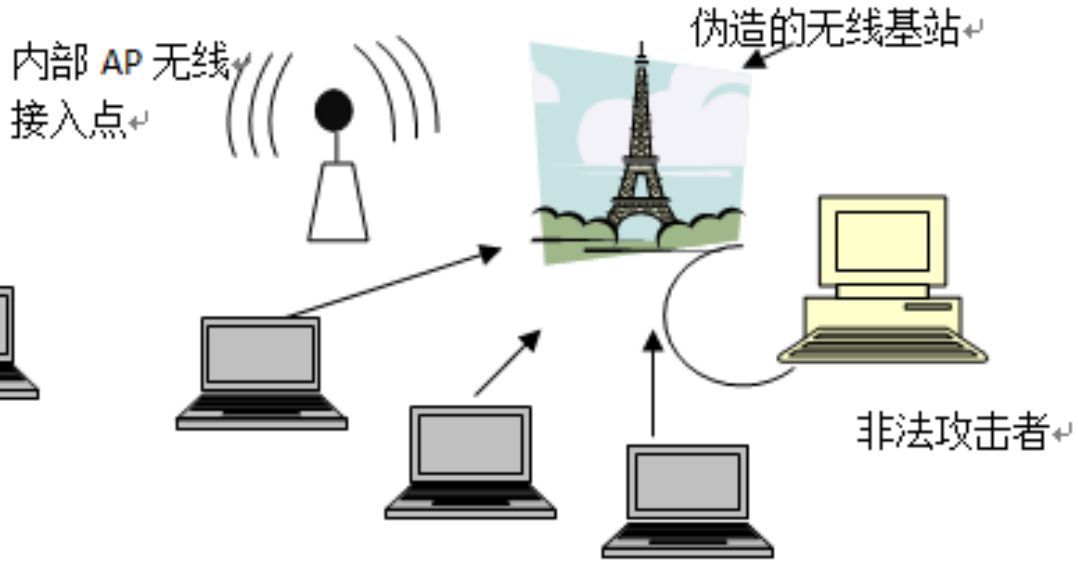
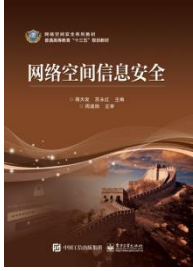
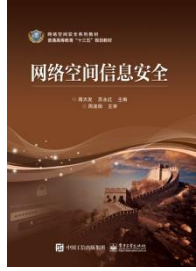


图 7.22 伪造 AP 示意图



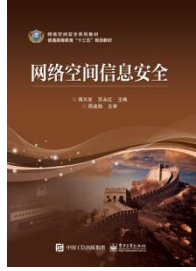
7.5 无线网络的安全性

- 方法三：加密破解。
- （1）WEP破解
- 过程：黑客侦测WEP安全协议漏洞，破解无线存取设备与客户之间的通讯。若黑客只是采取监视方式的被动式攻击，可能得花上好几天的时间才能破解，但有些主动式的攻击手法只需数小时便可破解。入侵者的企图是非法侦测入侵、盗取密码或身份，取得网络权限。



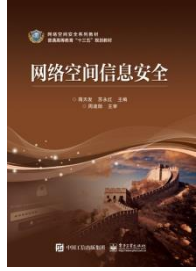
7.5 无线网络的安全性

- BackTrack是一套专业的计算机安全检测软件，简称BT。目前最新版本是BT5，可以用来破解WEP，也可破解WPA/WPA2加密的无线网络，当然前提是需要求足够强大的密码字典软件。BT5在以往版本工具的基础上又加入了基于GPU的破解工具oclhashcat,分别为oclhashcat+(ATI),oclhashcat+(Nvidia)破解速度理论上可以达到CPU破解的百倍。
- 在VMware中成功安装BackTrack5系统后，在BT5系统中通过ifconfig命令可以连接无线网卡。



7.5 无线网络的安全性

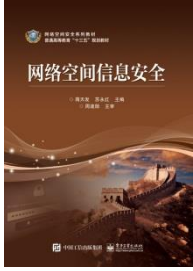
- (2)WPA破解
- 由于WEP的不安全性，在IEEE802.11i协议完善前，采用WPA为 用户提供一个临时的解决方案。WPA的数据加密采用TKIP协议，认证模式有两种：一是利用802.11x协议，二是PSK（Pre-Shared Key）模式。802.11x认证服务器散布不同的要是给哥哥客户，PSK模式让每个用户都要用同一个密码，有些不太保险。WPA的资料是用一把128位元的要是和一个48位元初向量(IV)的RC4流密码来加密。TKIP加上更长的初向量，可以击败对WEP的金钥匙攻击。



7.5 无线网络的安全性

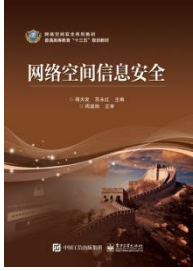
- WPA 在认证上也有改进，采用MIC（信息完整性检查，采用Michael算法），这是一种更安全的信息认证码，它包含了帧计数器，以避免WEP回访攻击（Replay Attack）.
- 在WPA2中，Michael算法由CCMP信息认证码取代，RC4由AES取代。WPA2符合802.11i标准。

7.5 无线网络的安全性



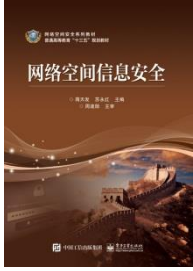
- 然而，WPA技术可以被以下工具破解：
- DIY暴力破解专用字典，如易优超级字典生成器。
- Fern工具，接上外置无线网卡后，打开fern-wifi-craker进行设置，破解密码。
- Gerix工具，打开gerix-wifi-craker-ng软件，进行操作破解密码。
- 使用wifite工具进行破解，接上外置无线网卡后，打开wifite工具，进行破解。
- 使用Aircrack-ng工具包及相关命令进行WPA/WPA2 deauth攻击破解WPA/WPA2网络。

7.5 无线网络的安全性



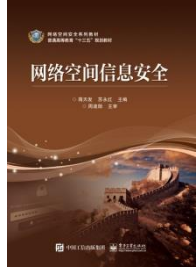
- 方法四：无线DoS攻击
- DoS(Deny of Service,拒绝服务供给)通过故意攻击网络协议的缺陷或通过某种手段耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使得目标系统服务停止响应甚至崩溃。这些服务资源包括网络宽带、系统堆栈、开放的进程、允许的连接等。无线DoSe攻击既是把DoS攻击延伸到无线网络上。
- Charon(亡灵摆渡人)是MDK3的图形化版本，可以发动无线DoS攻击。
- MDK3是Linux Shell下运行的无线DoS工具，它的功能非常强大，支持Auth Flood,De-auth Flood、Associate Flood、De-associate Flood等多种主流攻击。

7.5 无线网络的安全性



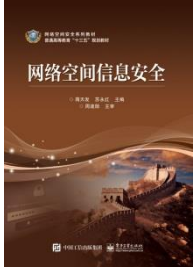
- 方法五：WEP注入攻击
- Aircrack -ng是一款用于破解无线802.11WEP及WPA-PSK加密的工具。有两种方式进行WEP破解。
- 一种是FMS攻击，利用了RC4的密钥排列算法和IV适用上的弱点。弱IV值会泄露密钥流的第一个字节中的密钥信息。因为相同的密钥与不同的IV被反复使用，如果收集到了足够多的具有弱IV的数据包，且密钥流的第一个字节是已知的，就可以确定密钥。802.11b进行数据包封装时，第一个字节是SNAP（Sub Network Access Protocol）头，它几乎总是0xAA。可以通过用0xAA 与密文中第一个加密字节进行异或，就会轻松的得到密钥流的第一个字节。

7.5 无线网络的安全性



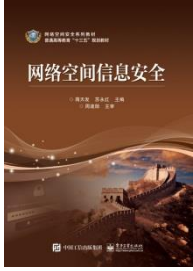
- 有一种是KoreK攻击。这种效率远远高于FMS攻击。KoreK Attack用了更多的弱IV，在计算中用到了密钥流的第一个字节和第二个字节，发现总结了额外的16种RC4密钥前i个字节，中间生产的密钥流的前两个字节和下一个密钥K[i]之间的关系。这样使得捕获包的利用率被大大提高了，攻击效率大大提高。
- Aircrack –ng工具破解WEP的思路是通过监听抓包，生成IVS文件，对IVS文件进行分析破解。

7.5 无线网络的安全性



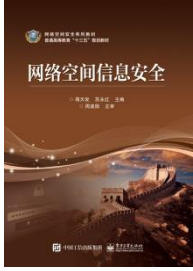
- 方法六、WEP ARP注入攻击
- 这种攻击模式是一种抓包后分析重发的过程。即可以利用合法客户端，也可以利用虚拟连接的伪装客户端。如果有合法客户端那一般需要等几分钟，让合法客户端和AP之间通信，少量数据就可产生有效ARP request,才可利用交互模式注入成功。如果长时间没有ARP Request，可以尝试利用冲突模式攻击。如果没有合法客户端，则可以利用建立虚拟连接的伪装客户端，连接过程中获得验证数据包，从而产生有效ARP request，再通过交互模式注入。

7.5 无线网络的安全性



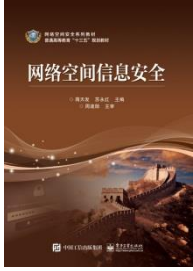
- 方法七：WEP高级攻击
- chop chop攻击，主要是获得一个可利用包含密钥数据的XOR文件，不能用来解密数据包，用它来产生一个新的数据包以便进行注入。
- fragmentation 攻击实现：fragmentation碎片包攻击模式主要是获得一个可利用PRGA，这里的PRGA并不是WEP密码数据，不能用来解密数据包。也是用它来产生一个新的数据包以便进行注入。其工作原理就是使得目标AP重新广播包，但AP重广播时，一个新的IVS产生。
-

7.5 无线网络的安全性

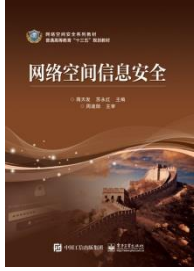


- 很多用户都没有开启安全功能，把自己主动暴露在黑客的面前，这是十分危险的。其实用户只要通过改变用户的路由器缺省管理员密码、禁止SSID广播、设置使用WEP和WPA等各种加密，同时使用MAC地址过滤，就能够获得相对安全的无线网络环境。不论在咖啡店这样的公共场所，还是在公司或家里，我们应该将无线安全设置变成一种日常的行为规范，养成良好的习惯，这样才能最大限度的保护无线网络安全。

7.5.4防范无线网络入侵的安全措施



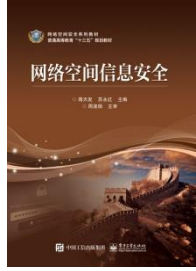
- 防止无线网络受到黑客入侵的十项措施:
- （1）正确放置网络的接入点设备。在网络配置中，要确保无线接入点放置在防火墙范围之外。
- （2）利用MAC阻止黑客入侵。利用基于MAC地址的ACL（访问控制列表）确保只有经过注册的设备才能进入网络。MAC过滤技术就如同给系统的门前再加一把锁，设置的障碍越多，越会使得黑客知难而退，不得不转而寻求去入侵其他低安全的网络。
- （3）有效管理无线网络的ID。所有无线局域网都有一个缺省SSID或网络名。立即更改这个名字，用文字和数字符号来表示。如果企业具有网络管理功能，应该定期更改SSID，更要取消SSID自动播放功能。



7.5.4防范无线网络入侵的安全措施

- （4）保证WEP协议的重要性。WEP是802.11b无线局域网的标准网络安全协议。在传输信息时，WEP可以通过加密无线传输数据来提供类似有线传输的保护。在简便的安装和启动之后，应立即更改WEP密钥的缺省值。最理想的方式是WEP的密码能够在用户登陆后进行动态改变，这样，黑客要想获得无线网络的数据就需要不断跟踪这种变化。基于会话和用户的WEP密码管理技术能够实现最优保护，为网络增加另外一层防范。

7.5.4防范无线网络入侵的安全措施



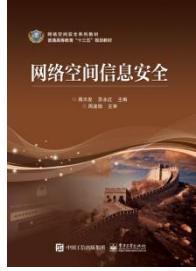
- （5）要清楚地认识到WEP协议不是万能的。不能将加密保障都寄希望于WEP协议。WEP只是多层网络安全措施中的一层，虽然这项技术在数据加密中具有相当重要的作用，但整个网络的安全不应该只依赖这一层的安全性能。

7.5.4防范无线网络入侵的安全措施

- （6）采用VPN技术。 VPN是最好的网络技术之一，如果每一项安全措施都是阻挡黑客进入网络前门的门锁，那么，VPN则是保护网络后门安全的关键。VPN具有比WEP协议更高层的网络安全性（第三层），能够支持用户和网络间端到端的安全隧道连接。
- （7）提高已有的RADIUS服务能力。大公司的远程用户常常通过RADIUS（远程用户拨号认证服务）实现网络认证登录。企业的IT网络管理员能够将无线局域网集成到已经存在的RADIUS架构来简化对用户的管理。这样不仅能实现无线网络的认证，而且还能保证无线用户与远程用户使用同样的认证方法和帐号。

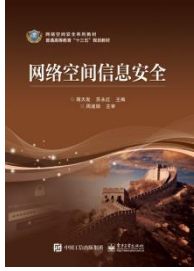
7.5.4防范无线网络入侵的安全措施

- （8）简化网络安全管理，集成无线和有线网络安全策略。无线网络安全不是单独的网络架构，它需要各种不同的程序和协议。制定结合有线和无线网络安全的策略能够提高管理水平，降低管理成本。例如，不论用户是通过有线还是无线方式进入网络时，都采用集成化的单一用户ID和密码。



7.5.4防范无线网络入侵的安全措施

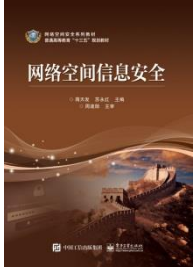
- 9）认识到WLAN设备不全都一样。尽管802.11b是一个标准协议，所有获得Wi-Fi标志认证的设备都可以进行基本功能的通信，但不是所有这样的无线设备都完全对等。虽然Wi-Fi认证保证了设备间的互操作能力，但许多生产商的设备都不包括增强的网络安全功能。



7.5.4防范无线网络入侵的安全措施

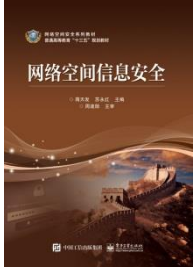
- （10）不能让非专业人员构建无线网络。尽管现在的无线局域网的构建已经相当方便，非专业人员可以在自己的办公室安装无线路由器和接入点设备，但是，他们在安装过程很少考虑到网络的安全性，只要通过网络探测工具扫描网络就能够给黑客留下入侵的后门。因而，在没有专业系统管理员同意和参与的情况下，要限制无线网络的构建，这样才能够保证无线网络的安全。

7.5.5攻击无线网的工具及防范措施



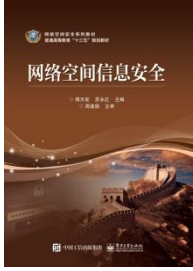
- 1. 寻找无线网络的工具
- 找到无线网络是攻击的第一步，有两种寻找无线网络的工具：
- （1）Network Stumbler a.k.a NetStumbler。这个基于Windows的工具可以非常容易地发现一定范围内广播出来的无线信号，还可以判断哪些信号或噪音信息可以用来做站点测量。
- （2）Kismet。NetStumbler缺乏的一个关键功能就是显示那些没有广播SSID的无线网络。访问点（Access Points）会常规性地广播这个信息。Kismet会发现并显示没有被广播的那些SSID，而这些信息对于发现无线网络是非常关键的。

7.5.5攻击无线网的工具及防范措施



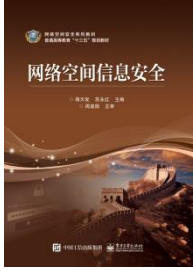
- 2. 连接无线网络的工具
- 发现了一个无线网络后，下一步就是连上它。如果该网络没有采用任何认证或加密安全措施，可以很轻松地连上它的SSID。如果SSID没有被广播，可以用这个SSID的名称创建一个文件。如果无线网络采用了认证和/或加密措施，需要以下工具中的某一个的工具来连接。

7.5.5攻击无线网的工具及防范措施

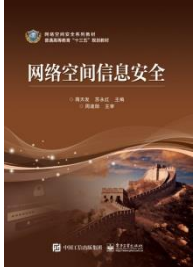


- （1）Airsnort。这个工具非常好用，可以用来嗅探并破解WEP密钥。很多人都用WEP，当然比什么都不用要好。在用这个工具时就会发现它捕获大量抓来的数据包，来破解WEP密钥。还有其他的工具和方法，可以用来强制无线网络上产生的流量去缩短破解密钥所需时间，不过Airsnort并不具有这个功能。
- （2）CowPatty。这个工具被用做暴力破解WPA-PSK，因为家庭无线网络很少用WEP。这个程序非常简单地尝试一个文章中各种不同的选项，来看是否某一个刚好和预共享的密钥相符。

7.5.5攻击无线网的工具及防范措施



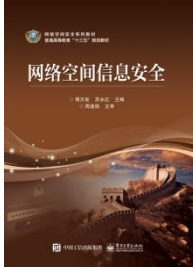
- （3）ASLeap。如果某无线网络用的是LEAP，这个工具可以搜集通过网络传输的认证信息，并且这些抓取的认证信息可能会被破解。LEAP不对认证信息提供保护，这也正是LEAP可以被攻击的主要原因。



7.5.5攻击无线网的工具及防范措施

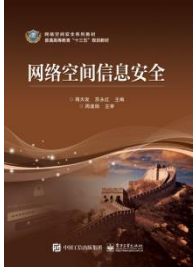
- 3. 抓取无线网上信息的工具
- 不管是不是直接连到了无线网络，只要所在的范围内有无线网络存在，就会有信息传递。要看到这些信息，需要一个工具。这就是Ethereal，这个工具非常有价值，毫无疑问。Ethereal可以扫描无线网和以太网信息，还具备非常强的过滤能力。它还可以嗅探出802.11管理信息，也可被用作嗅探非广播SSID。
- 前面提出的工具，都是无线网络安全工具包中所必须的。熟悉这些工具最简单的办法就是在一个可控的实验环境下使用他们。这些工具都可以在因特网上免费下载到。

7.5.5攻击无线网的工具及防范措施



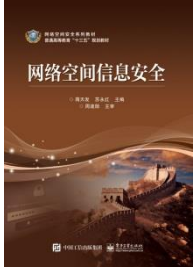
- 4. 对工具的防范措施
- 知道怎样使用上述工具是非常重要的，不过，知道怎样防范这些工具、保护自己的无线网络安全更为重要。
- 防范NetStumbler：不要广播自己的SSID，保证自己的WLAN受高级认证和加密措施的保护。
- 防范Kismet：没有办法让Kismet找不到自己的WLAN，所以一定要保证有高级认证和加密措施。
- 防范Airsnort：使用128比特的，而不是40比特的WEP加密密钥，这样可以使破解需要更长时间。如果自己的设备支持的话，使用WPA或WPA2，不要使用WEP。

7.5.5攻击无线网的工具及防范措施

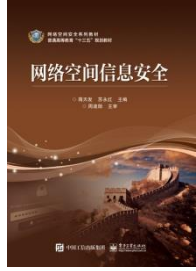


- 防范Cowpatty：选用一个长的复杂的WPA共享密钥。密钥的类型要不太可能存在于黑客归纳的文件列表中，这样破坏者猜测用户的密钥就需要更长的时间。如果是在交互场合，不要用共享密钥使用WPA，用一个好的EAP类型保护认证，限制账号退出之前不正确猜测的数目。
- 防范ASLeap：使用长的复杂的认证，或者转向EAP-FAST或另外的EAP类型。

7.5.5攻击无线网的工具及防范措施



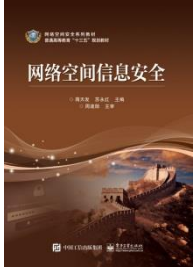
- 防范Ethereal：使用加密，这样任何被嗅探出的信息就很难或几乎不可能被破解。WPA2，使用AES算法，普通黑客是不可能破解的。WEP也会加密数据。在一般不提供加密的公共无线网络区域，使用应用层的加密，像Simplite，来加密IM会话，或使用SSL。对于需要交互的用户，使用IPSec VPN，并关闭分隧道功能。这就强制所有的流量都必须通过加密隧道，并通过DES、3DES或AES加密。



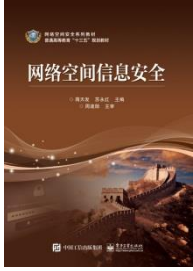
7.5.5攻击无线网的工具及防范措施

- （1）无线网技术的安全性级别定义。
- 第一级，扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据。
- 第二级，采取网络隔离及网络认证措施。
- 第三级，设置严密的用户口令及认证措施，防止非法用户入侵。
- 第四级，设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容

7.5.5攻击无线网的工具及防范措施



- 常见的无线网络的安全加密措施
- 在这里我们介绍几种常用的加密技术：WEP、WPA、WPA2、VPN、硬件安全交换机、ESSID。并指出了在日常生活中配置Wi-fi时需要注意的事项。
- 第一，连线对等保密(WEP)。采用rsa数据安全性公司开发的rc4 prng算法, WEP的全称是Wired Equivalent Privacy，中文意为有线对等保密。在链路层采用RC4对称加密技术，所有客户端与无线接入点的数据都会以一个共享的密钥进行加密，密钥长40~256位，从而防止非授权用户的监听以及非法用户的访问，密钥长度越长，破解时间也就越长。用户的加密钥匙必须与AP的钥匙相同，并且一个服务区内的所有用户都共享同一把钥匙。WEP加密过程如下：



WEP加密过程

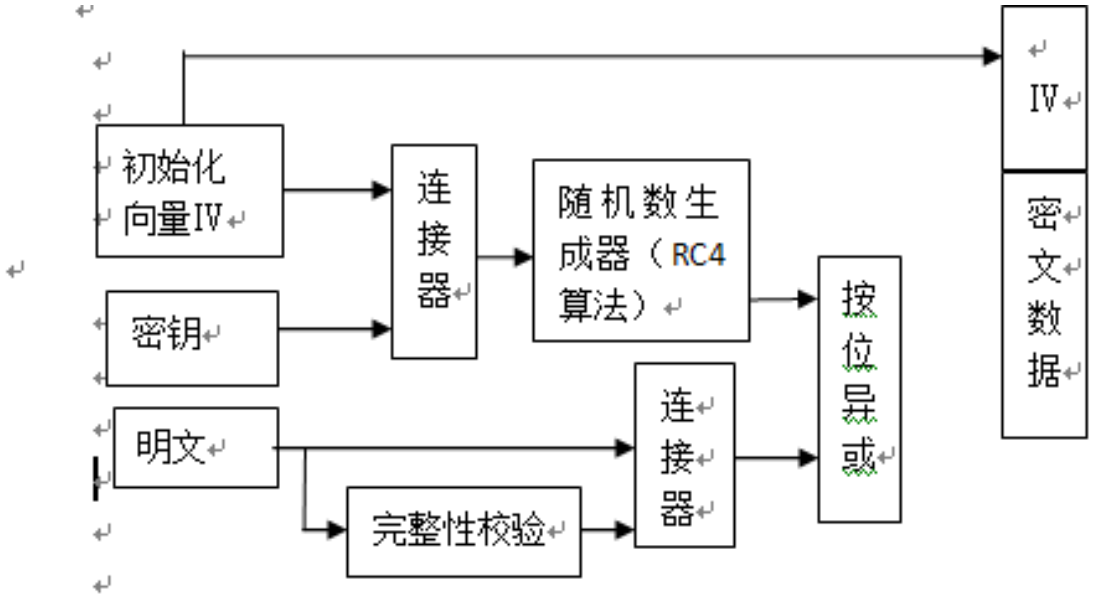
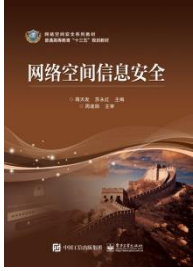
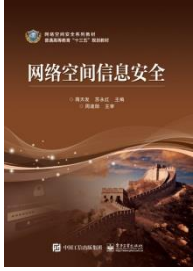


图 7-22 WEP加密过程



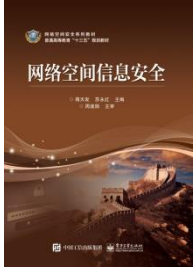
WEP加密过程

- (1)WEP协议工作在MAC层，从上层获得需要传输的明文数据后，首先利用CRC循环冗余校验序列进行计算，利用CRC算法将生成32位的ICV完整性校验值，将明文和ICV结合作为将要被加密的数据。
- (2)WEP协议利用RC4的算法产生伪随机序列流，用伪随机序列流和要传输的明文进行异或运算，产生密文。RC4加密密钥分成两部分，一部分是24位的初始化向量IV，另一部分就是用户密钥。不同的IV可以确保生成的伪随机序列流不同，从而可用于加密不同的选哦被传输的帧。



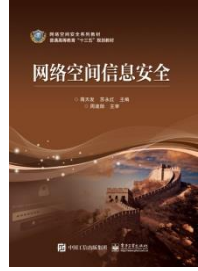
WEP加密过程

- (3)逐字节生成的伪随机序列流和被加密内容进行异或运算，生成密文，将初始向量IV和密文一起传输给接收方。
- (4)先进行帧的完整性效验，然后从中取出IV和使用的密码编号，将IV和对应的密钥组合成解密密钥流，再通过RC4计算出伪随机序列流，进行异或运算，计算出载荷以及ICV内容。对解密处的内容再用步骤（1）的方法生成ICV’，比较ICV’和ICV，如果相同则为正确。WEP协议解密的过程如图7.23所示：



WEP加密过程

- WEP使用RC4串流加密技术大道机密性，并使用CRC-32校验和达到资料正确性。标准的64位WEP使用40位的钥匙街上24位的初向量（Initialization Vector,IV）成为RC4用的钥匙。
- WEP有两种认证方式：开放式系统认证（Open System Authentication）和共有键认证（Shared Key Authentication）.



WEP解密过程

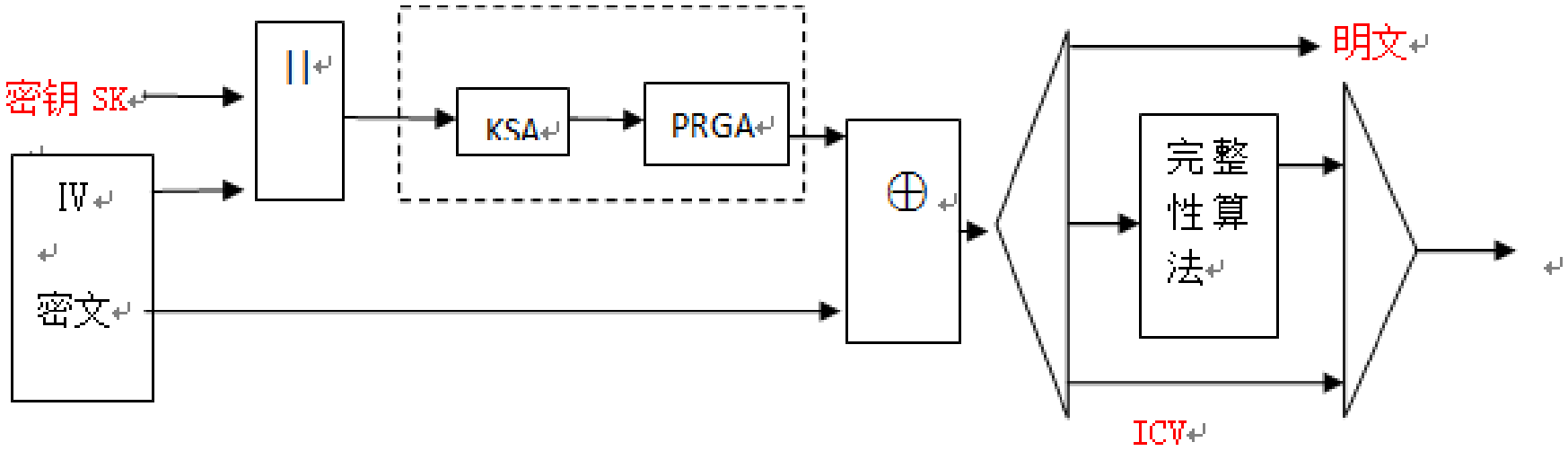
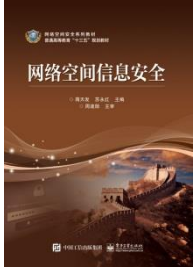
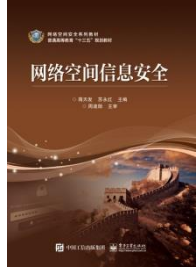


图 7.23 WEP 解密过程



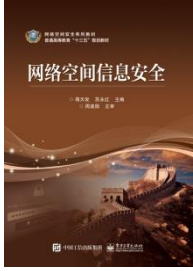
WEP解密过程

- WEP的破解其实就是利用加密体制缺陷，通过收集足够的IV数据包，使用分析密钥算法还原出密码。而WPA目前没有加密体制的缺陷可被利用，破解它的方法是常规的字典攻击法。
- 第二， Wi-fi网络安全接入（WPA）。WPA即Wi-Fi Protected Access，实现了 IEEE 802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案。WPA包括两种模式：WPA-PSK共享密钥模式和WPA-Radius证书模式。



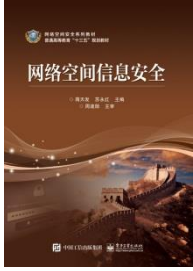
WEP解密过程

- 针对这两种模式的WPA的认证也有两种：一种是WPA-PSK采用静态的共享密钥为认证方式，这种方式相对来说较易破解。另一种是通过Radius服务器进行可扩展性认证的802.1x+EAP认证。WPA的采用的加密方式是TKIP，也即Temporal Key Integrity Protocol（临时密钥完整性协议），这种加密模式只针对于WPA-Radius模式，而且必须是在Enterprise模式下，对WPA-PSK无用。TKIP的密钥头长度有48位，但是加密方式仍然是RC4，存在破解的威胁。IT168网上曾报导：研究员ErikTews将在东京的PacSec大会上，演示他是如何在15分钟内破解WPA加密技术的。之前的无线加密技术WEP只需使用当今的笔记本即可在几分钟内破解。



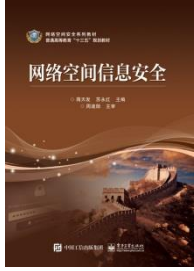
WEP解密过程

- 第三，WPA2. Wi-Fi 联盟在 2002 年 10 月发表了率先采用 IEEE 802.11i 功能的 WPA，在04年的6月，推出了WPA2，除了支持TKIP加密方式外，还支持“AES”加密方式。截止到 2006 年 03 月，WPA2 已经成为一种强制性的标准。WPA采用的加密算法是TKIP，并用MIC算法来计算校验和。在WPA2中， AES取代了WPA的TKIP，WCCMP取代了WPA的MIC，加密算法更为安全。WPA2解决了WPA存在的一些弊端：初始向量太短、不能保证数据完整性、使用主密钥而非派生密钥、不重新生成密钥、无重播保护等。目前有黑客通过字典及PIN码来破解WPA2，所以WPA2不存在100%的安全。给出的应对策略是设置复杂的密码，关闭WPS/QSS。



WEP解密过程

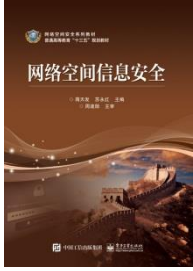
- 第四，虚拟专用网VPN。当无线局域网中的用户使用VPN通道的时候，在到达VPN网关之前，通讯数据是经过加密的，是一种点到点的一种安全措施。在企业网络核心中，VPN加密从计算机到VPN网关的整个链路，在计算机到无线访问点之间的无线网络部分也是被加密的。VPN可防止入侵者重入截取网络通讯数据。



WEP解密过程

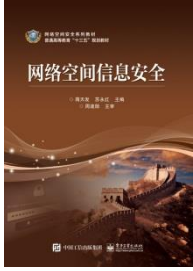
- 第五，硬件交换机。CNVD（国家信息安全漏洞共享平台）收录与基础电信企业软硬件资产相关的漏洞825个，其中与路由器、交换机等网络设备相关的漏洞占比达66.2%，主要包括内置后门、远程代码执行等类型[3]。如果我们将原先的企业级AP诸如安全、QoS、接入控制和负载均衡等功能集成到交换机中，原先的企业级AP只充当天线的功能，把AP中存放的IP地址、密码、安全认证、ACL、QoS等集成到交换机中，在一定程度上可解决无线安全设置问题。

WEP解密过程



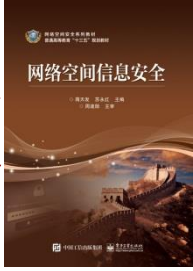
- 第六、ESSID。有了32位字符的SSID和3位字符的跳频序列，想要通过推断出确切的SSID和跳频序列经由局域网的无线网段进入局域网变的变得困难。
- 在保障无线网络安全方面，我们需要注意一下几点：
- 第一、注意SSID，SSID是一个无线网络的标识，在可能的情况下不应使用设备缺省的SSID。设置为封闭的Wi-Fi网络不响应那些将SSID设置为Any的无线设备，而且不在无线网络内进行SSID广播。

WEP解密过程



- 第二、禁用DHCP服务器。原因是在无线网络中的计算机，不仅需要一个SSID号码，还需要分配一个IP地址才能连入无线网络。
- 第三、设置网络密钥：设置尽可能高强度的密钥。
- 第四、定期更换密钥：考虑至少每个季度更换一次密钥。
- 第五、过滤计算机：启用MAC和IP地址过滤，尽量保证只有得到授权的计算机才能访问无线网络。

7.5.5攻击无线网的工具及防范措施

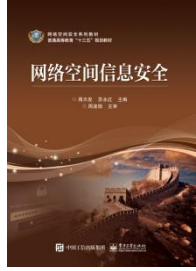


- 保证WLAN的安全，我们可以从以下几点做到：
- （1）访客级。如果打算提供非正式或者无监管的Internet接入，则可能会受到不受控制的访问及AP直接连接到Internet。这类WLAN可能不需要实施WEP链路安全措施或者访问加密/签名，并且允许所有不同厂商的WLAN卡能够互操作。使用这种服务的公司会使来宾非常愉快，但要承担雇员对它进行滥用、使企业暴露在Internet上的风险。

7.5.5攻击无线网的工具及防范措施

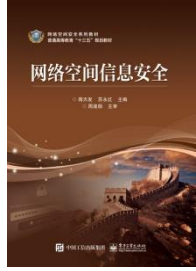
- （2）进行访问登记。这是为Internet接入提供基本服务的一个折中。其使用WEP安全措施和简单的口令认证。这样就可以为Internet接入有选择地使用AP，并且可以防止未经许可的访客偶然进入，当然对蓄意闯入的黑客起不了作用。

  （3）私有的intranet访问。在这种保守的解决方法中，AP使用RADIUS进行比较强的链路加密和签名。其安全性和保密性不错，但由于缺少强链路加密的标准，采用这种方法不能实现互操作。企业必须锁定一个厂商，以确保能够受到保护。



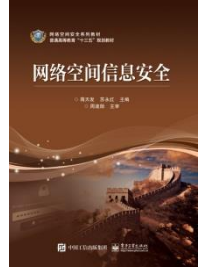
7.5.5攻击无线网的工具及防范措施

- （4）私有VPN接入。这是对创建私有接入合乎情理的折中。AP通过企业的VPN网关接到WLAN的入口，只有拥有合法的企业签名、运行适当的VPN的用户才能被允许通过AP接入。链路加密固然很重要，但合法的VPN会话保证也减少了窥探和攻击的危险。由于在AP上存在着对等攻击（peer attacks）的危险，采用这种方法的企业必须确保用户的PC装有同级别的抗病毒程序和个人防火墙，同时还要求用户都使用VPN。不能允许Split tunneling，因为以前已经证明这对VPN用户是一个严重的威胁，AP上的所有用户都有可能成为黑客的俘虏。



7.5.5攻击无线网的工具及防范措施

- （5）访问别人的公共WLAN服务。那些为移动用户提供无线网卡的企业和自己购买网卡的用户最终会发现他们能够获得公共的WLAN服务，但同时也冒着使自己公司的系统暴露的危险。任何允许移动用户使用无线网卡的企业必须确保用户安装了防病毒软件和个人防火墙。由于大多数公司都有合适的防病毒软件，个人防火墙也可以和无线网卡打包发给用户。



- 谢谢！