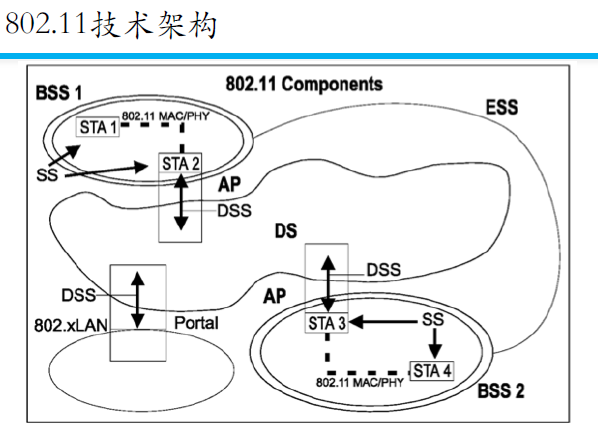
移动互联网安全

1. 无线网络安全基础
2. 无线网络通信协议中UWB和WiMax协议已经过时
3. ZigBee：个人短距离。ZigBee是基于IEEE802.15.4标准的低功耗局域网协议。根据国际标准规定，ZigBee技术是一种短距离、低功耗的无线通信技术。其特点是近距离、低复杂度、自组织、低功耗、低数据速率。主要适合用于自动控制和远程控制领域，可以嵌入各种设备。简而言之，ZigBee就是一种便宜的，低功耗的近距离无线组网通讯技术。ZigBee是一种低速短距离传输的无线网络协议。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。

3、



\*\*802.11体系结构的组成包括：无线站点STA（station），无线接入点AP（access point），独立基本服务组IBSS（independent basic service set），基本服务组BSS（basic service set），分布式系统DS（distribution system）和扩展服务组ESS（extended service set）。

STA：具备联网功能的设备。一个无线站点STA通常由一台PC机或笔记本计算机加上一块无线网卡构成

BSS：相对独立的无线网络，基本服务集（BSS）。基本服务集是802.11 LAN的基本组成模块。能互相进行无线通信的STA可以组成一个BSS（Basic Service Set） 。如果一个站移出BSS的覆盖范围，它将不能再与BSS的其它成员通信。对于个人PC来说，使用最多的所谓"无线Wi-Fi"指的就是BSS网络模式，我们通过AP(Access Point)接入点来接入网络

DS：链路层，相当于switch。连接BSS的组件称为分布式系统（Distribution System，DS）。ESS中的DS(分布式系统)是一个抽象系统，用来连接不同BSS的通信信道(通过路由服务)，这样就可以消除BSS中STA与STA之间直接传输距离受到物理设备的限制。

Portal：门户认证

DSS：连接地面网络。发布服务系统。提供的服务是一端连接到BSS，另一端延伸到网络中任意可能的端点中去，来实现逻辑和物理区域的网间互联。

802.11 MAC/PHY：多台ap级联，跨局域网通信

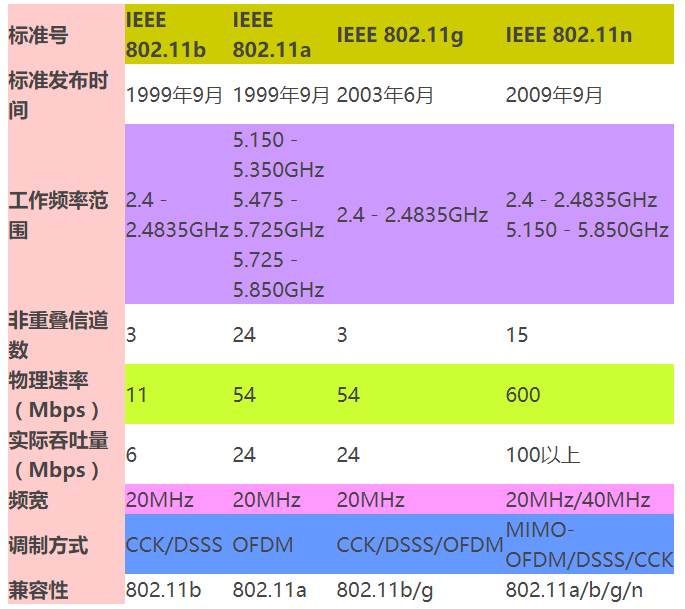
ESS：扩展服务集（ESS），多个BSS可以构成一个扩展网络，称为扩展服务集（ESS）网络，一个ESS网络内部的STA可以互相通信，是采用相同的SSID的多个BSS形成的更大规模的虚拟BSS。

SSID/BSSID：SSID，服务集的标识，在同一SS内的所有STA和AP必须具有相同的SSID，否则无法进行通信。SSID是一个ESS的网络标识(如:TP\_Link\_1201)，BSSID是一个BSS的标识，BSSID实际上就是AP的MAC地址，用来标识AP管理的BSS，在同一个AP内BSSID和SSID一一映射。在一个ESS内SSID是相同的，但对于ESS内的每个AP与之对应的BSSID是不相同的。如果一个AP可以同时支持多个SSID的话，则AP会分配不同的BSSID来对应这些SSID。

IBSS：BSS的一种特殊结构，这种结构内没有提供DSS功能的STA，所有的STA都自组实现对等通信。

AD Hoc模式：可以在无AP的环境下实现两台或多台STA的对等通讯功能

4、802.11简介



5、频谱划分

1）IEEE 802.11b/g标准工作在2.4G频段，频率范围为2.400—2.4835GHz，共83.5M带宽

2）划分为14个子信道

3）每个子信道宽度为22MHz

4）相邻信道的中心频点间隔5MHz

5）相邻的多个信道存在频率重叠(如1信道与2、3、4、5信道有频率重叠)

6）整个频段内只有3个（1、6、11）互不干扰信道

6、802.11协议

802.11

IEEE最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到2Mbps。由于它在速率和传输距离上都不能满足人们的需要，因此，IEEE小组又相继推出了802.11b和802.11a两个新标准。

802.11a

802.11a标准工作在5GHzU-NII频带，物理层速率最高可达54Mbps，传输层速率最高可达25Mbps。可提供25Mbps的无线ATM接口和10Mbps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。

根据需要，数据率还可降为48，36，24，18，12，9或者6Mb/s。802.11a拥有12条不相互重叠的频道，8条用于室内，4条用于点对点传输。它不能与802.11b进行互操作，除非使用了对两种标准都采用的设备。

802.11b

IEEE802.11b是无线局域网的一个标准。其载波的频率为2.4GHz，传送速度为11Mbit/s。IEEE802.11b是所有无线局域网标准中最著名，也是普及最广的标准。它有时也被错误地标为Wi-Fi。实际上Wi-Fi是无线局域网联盟（WLANA）的一个商标，该商标仅保障使用该商标的商品互相之间可以合作，与标准本身实际上没有关系。在2.4-GHz-ISM频段共有14个频宽为22MHz的频道可供使用。IEEE802.11b的后继标准是IEEE802.11g，其传送速度为54Mbit/s。

802.11g

IEEE 802.11g2003年7月，通过了第三种调变标准。其载波的频率为2.4GHz（跟802.11b相同），原始传送速度为54Mbit/s，净传输速度约为24.7Mbit/s（跟802.11a相同）。802.11g的设备与802.11b兼容。802.11g是为了提高更高的传输速率而制定的标准，它采用2.4GHz频段，使用CCK技术与802.11b后向兼容，同时它又通过采用OFDM技术支持高达54Mbit/s的数据流，所提供的带宽是802.11a的1.5倍。从802.11b到802.11g，可发现WLAN标准不断发展的轨迹：802.11b是所有WLAN标准演进的基石，未来许多的系统大都需要与802.11b向后向兼容，802.11a是一个非全球性的标准，与802.11b后向不兼容，但采用OFDM技术，支持的数据流高达54Mbit/s，提供几倍于802.11b/g的高速信道，如802.11b/g提供3个非重叠信道可达8-12个；可以看出，在802.11g和802.11a之间存在与Wi-Fi兼容性上的差距，为此出现了一种桥接此差距的双频技术——双模（dual band)802.11a+g(=b），它较好地融合了802.11a/g技术，工作在2.4GHz和5GHz两个频段，服从802.11b/g/a等标准，与802.11b后向兼容，使用户简单连接到现有或未来

802.11n

IEEE802.11n，2004年1月IEEE宣布组成一个新的单位来发展新的802.11标准。资料传输速度估计将达475Mbps（需要在物理层产生更高速度的传输率），此项新标准应该要比802.11b快45倍，而比802.11g快8倍左右。802.11n也将会比之前的无线网络传送到更远的距离。的802.11网络成为可能。

802.11ac

主流厂商（Qualcomm，Broadcom，Intel等）正在开发的协议版本，它使用5GHz频段（也可以说是6GHz频段），采用：更宽的基带（最高扩展到160Mhz）、更多的MIMO、高密度的调制解调（256 QAM）。理论上，11ac可以为多个站点服务提供1Gbit的带宽，或是为单一连接提供500Mbit的传输带宽。支持千兆网络

世界上第一只采用802.11ac无线技术的路由器,于2011年11月15日, 由美国初创公司Quantenna推出了。2012年1月5日，业界巨头Broadcom发布了它的第一款支持802.11ac的芯片。

802.11i

IEEE802.11i是IEEE为了弥补802.11脆弱的安全加密功能（WEP,Wired Equivalent Privacy）而制定的修正案，于2004年7月完成。其中定义了基于AES的全新加密协议CCMP（CTR with CBC-MAC Protocol），以及向前兼容RC4的加密协议TKIP（Temporal Key Integrity Protocol）。

无线网络中的安全问题从暴露到最终解决经历了相当的时间，而各大厂通信芯片商显然无法接受在这期间什么都不出售，所以迫不及待的Wi-Fi厂商采用802.11i的草案3为蓝图设计了一系列通信设备，随后称之为支持WPA（Wi-Fi Protected Access）的；之后称将支持802.11i最终版协议的通信设备称为支持WPA2（Wi-Fi Protected Access 2）的。

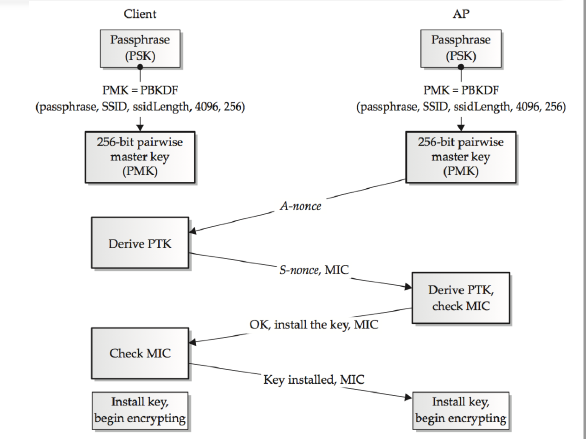
1. 传输时协议的属性包含在beacon frame里
2. 802.11的三种工作模式具有排他性，混杂模式下也为监听模式，不需要建立连接
3. 路由器：交换机具有网络功能
4. man + 命令名称：查阅命令帮助信息
5. 无线接入网监听
6. dhcp无法获取ip地址，就无法建立网络层连接
7. 2.4G：1~13 channel
8. 无线网卡可以工作在多种模式之下。常见的有Master，Managed，ad-hoc，monitor等模式。
9. 对于Master模式，它主要使用于无线接入点AP提供无线接入服务以及路由功能。可以想象我们使用的无线路由器就是工作在Master模式下了，不过对于普通的pc机来说，如果有合适的硬件它也可以变成一台无线AP。在LINUX下使用软件HOSTAP可以使一台linux pc具有ap功能，但目前HOSTAP的所支持的无线网卡有限，我的INTEL Centrino PRO 4965 wireless card就不被hostap所支持。对于一般的无线网卡来说，它们最常见的模式还是managed，ad-hoc和monitor。Managed模式用于和无线AP进行接入连接，在这个模式下我们才可以进行无线接入internet上网。对于需要两台主机进行直连的情况下可以使用ad-hoc模式，这样主机之间是采用对等网络的方式进行连接。Monitor模式主要用于监控无线网络内部的流量，用于检查网络和排错。
10. 连接服务：存储转发的过程
11. 当ap过多时网速时快时慢，这与冲突检测有关
12. 隐藏节点和暴露节点问题

隐藏节点：比如说网络中有三个节点A,B,C。A,C都想传数据给B，但A,C都不在彼此的传输范围内。因而也就不会感知到对方，但都能向B传输数据，在这种情况下，来自A & C的数据会在B处碰撞，造成数据丢失，网络性能下降。这样因为传送距离而发生误判的问题称为隐藏节点问题。

暴露节点：当有一个节点要发送数据给另一个节点，但因为邻居节点也正发送数据时，因此影响了原本节点的数据传送。如有四个节点R1， S1，S2，R2,但R1，R2不在彼此的传送范围内，而s1和s2，r1和s1，s2和r2都在彼此的传输范围内。当s1传数据给r1时，s2却不能传数据给r2,此时s2检测到s1正在传送数据，就会影响s1传送，事实上s2可以将数据传送到r2，因为r2不在s1的传输范围内。

可以用RTS（request to send）和CTS(clear to send)的控制封包来避免碰撞。在传输之前，传送端先传送一个RTS封包，告知在传送端传送范围内所有节点不要有任何传送操作。如果接收端目前是空闲的，则响应CTS封包，进而传输数据。从而可有效解决隐藏节点的问题。

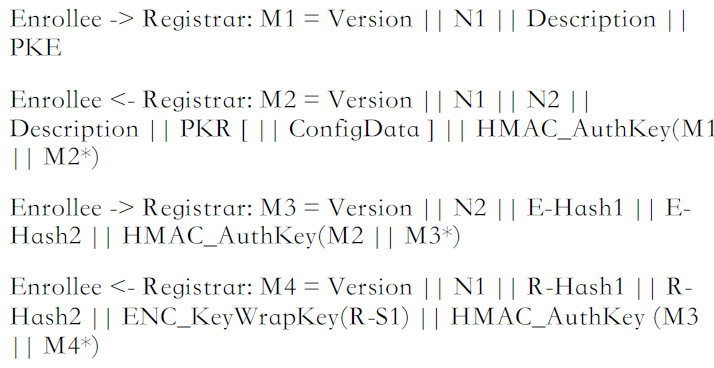
1. wep非常不安全
2. 向前兼容：backward
3. 四次握手认证



1. PBKDF：密码算法
2. Passphrase：明文口令
3. 4096，256：输出长度和迭代次数
4. PMK：随机数
5. Install the key：密钥每隔时间更换会话加密密钥，给攻击留出可能
6. Client前两步在本地完成
7. wps工作模式中

带内传输：带内传输（intraband transmission）是指一种利用话路频带内的一段窄频带，使电话与时间离散信号得以同时传输的传输方式。主数据协议以外的传输，和主数据协议位于同样的传输介质之上。管理协议是一种带内传输的例子。

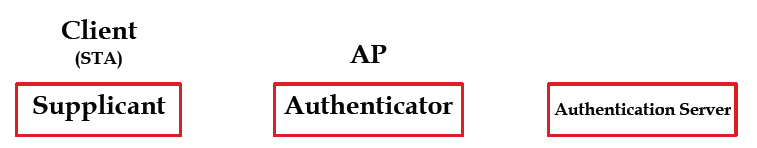
带外传输：使用一个分离的控制链接，控制信息和数据传输由不同的进程控制。数据传输机制和密钥协商不在一个信道内



抓包可以获得前四次数据包

HMAC——AuthKey：校验消息完整性

1. 注册消息协议版本号会决定如何发送和解析数据
2. 随机数防止重放攻击
3. 802.11状态机中第一步需查看是否经过认证和是否进入关联状态
4. 802.1x技术架构



Supplicant：提供认证凭据（STA包含路由器）

Authentication：完成验证逻辑（在数据库中查询计算）

Authentication Server：比如数据库，在物理层

17、802.11中提供STA和认证服务器之间的端到端认证

功能：收和转发，不会修改数据包，保证端到端通信

1. 服务端证书保证服务器认证客户端真实身份，有可能遭受降级攻击
2. 根ca预制在操作系统或软件内部，是离线过程
3. U盾存储客户端安全证书
4. 自签发证书问题：无法区分是攻击者构造的还是自己构造的证书
5. TLS对称加密主密钥不在AP上存储，但要在传输过程中协商

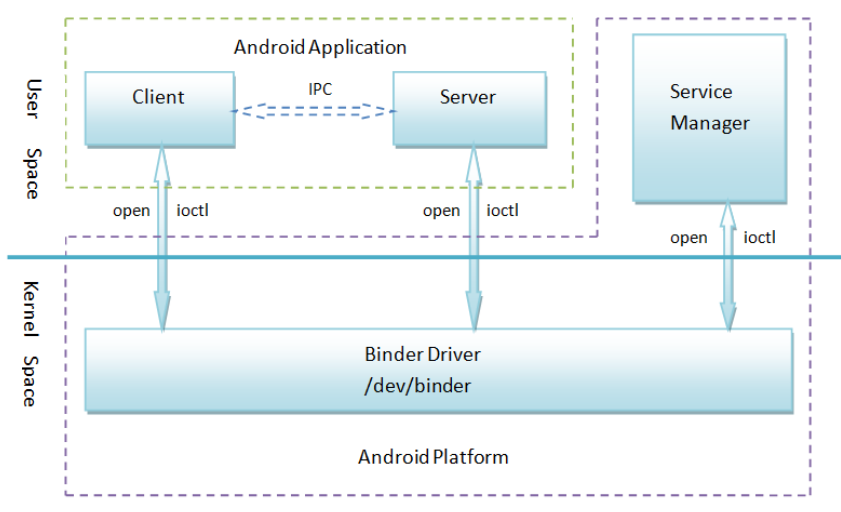
第六章

Android进程间通信（IPC）机制Binder简要介绍

Android系统没有采用上述提到的各种进程间通信机制，而是采用Binder机制，难道是因为考虑到了移动设备硬件性能较差、内存较低的特点？不得而知。Binder其实也不是Android提出来的一套新的进程间通信机制，它是基于OpenBinder来实现的。OpenBinder最先是由Be Inc.开发的，接着Palm Inc.也跟着使用。现在OpenBinder的作者Dianne Hackborn就是在Google工作，负责Android平台的开发工作。

前面一再提到，Binder是一种进程间通信机制，它是一种类似于COM和CORBA分布式组件架构，通俗一点，其实是提供远程过程调用（RPC）功能。从英文字面上意思看，Binder具有粘结剂的意思，那么它把什么东西粘结在一起呢？在Android系统的Binder机制中，由一系统组件组成，分别是Client、Server、Service Manager和Binder驱动程序，其中Client、Server和Service Manager运行在用户空间，Binder驱动程序运行内核空间。Binder就是一种把这四个组件粘合在一起的粘结剂了，其中，核心组件便是Binder驱动程序了，Service Manager提供了辅助管理的功能，Client和Server正是在Binder驱动和Service Manager提供的基础设施上，进行Client-Server之间的通信。Service Manager和Binder驱动已经在Android平台中实现好，开发者只要按照规范实现自己的Client和Server组件就可以了。说起来简单，做起难，对初学者来说，Android系统的Binder机制是最难理解的了，而Binder机制无论从系统开发还是应用开发的角度来看，都是Android系统中最重要的组成，因此，很有必要深入了解Binder的工作方式。要深入了解Binder的工作方式，最好的方式莫过于是阅读Binder相关的源代码了，Linux的鼻祖Linus Torvalds曾经曰过一句名言RTFSC：Read The Fucking Source Code。

总结一下，Android系统Binder机制中的四个组件Client、Server、Service Manager和Binder驱动程序的关系如下图所示：



1. Client、Server和Service Manager实现在用户空间中，Binder驱动程序实现在内核空间中

2. Binder驱动程序和Service Manager在Android平台中已经实现，开发者只需要在用户空间实现自己的Client和Server

3. Binder驱动程序提供设备文件/dev/binder与用户空间交互，Client、Server和Service Manager通过open和ioctl文件操作函数与Binder驱动程序进行通信

4. Client和Server之间的进程间通信通过Binder驱动程序间接实现

5. Service Manager是一个守护进程，用来管理Server，并向Client提供查询Server接口的能力