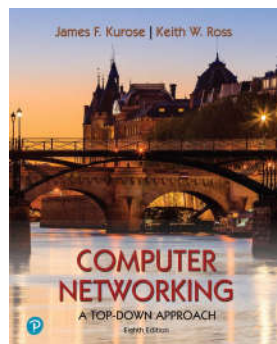


# 无线与移动网络（上）

中国科学技术大学  
自动化系 郑烜  
改编自Jim kurose, Keith Ross



*Computer Networking: A Top-Down Approach*  
8<sup>th</sup> edition  
Jim Kurose, Keith Ross  
Pearson, 2020

## 无线和移动网络：背景

- 无线（移动）电话的订户数量已经超过了有线电话（2019年10:1）！
- 移动宽带连接上网设备数量>固定宽带（2019年5:1）！
- 4G/5G蜂窝网络融合了互联网协议栈，包括SDN
- 2个重要的（但是不同的）挑战
  - 无线: 通过无线链路通信
  - 移动: 需要网络处理移动（不停变换所接入的网络）用户

Wireless and Mobile Networks: 7-2

## 第七章 提纲

### ■ 引论

#### 无线

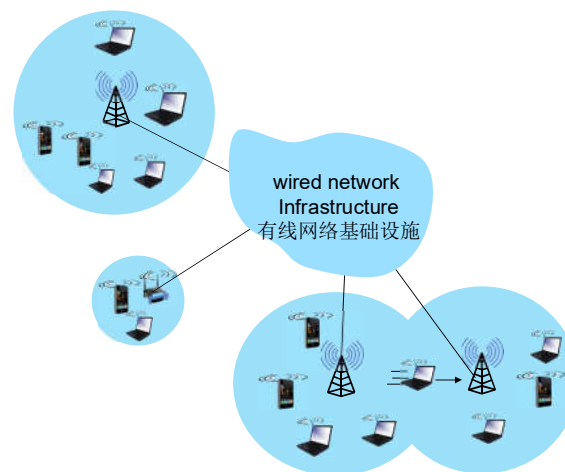
- 无线链路和网络特征
- WiFi: 802.11 无线局域网
- 蜂窝网络: 4G 和 5G

#### 移动性

- 移动性管理：原理
- 移动性管理：实践
  - 4G/5G networks
  - Mobile IP
- 移动性：对于高层协议的冲击



## 无线网络中的组件

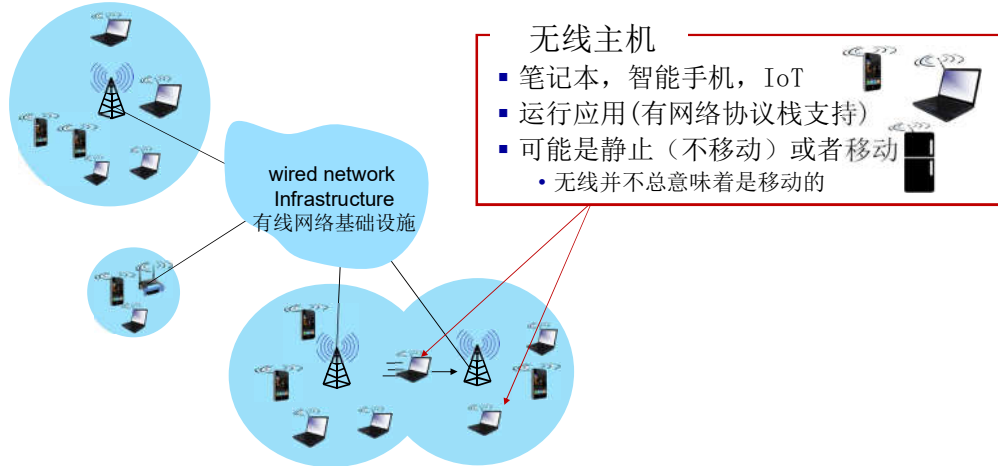


2021 中科大高网

Wireless and Mobile Networks: 7-3

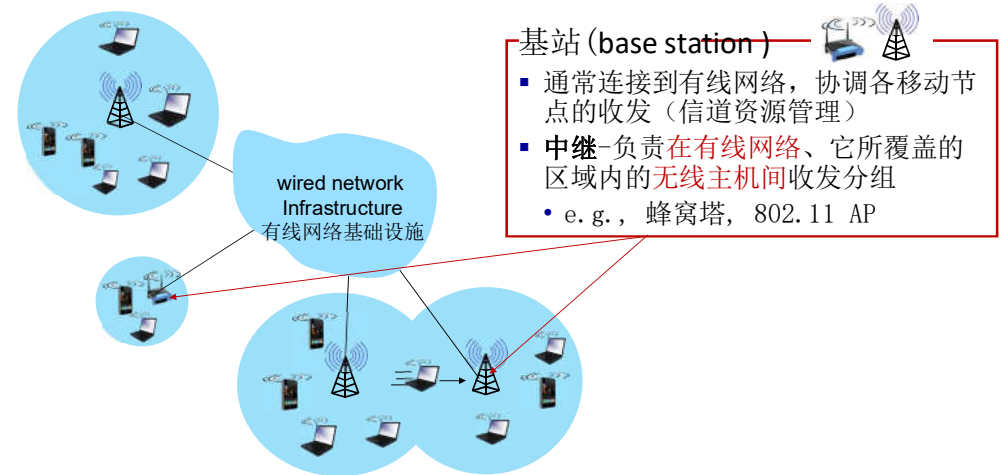
Wireless and Mobile Networks: 7-4

## 无线网络中的组件



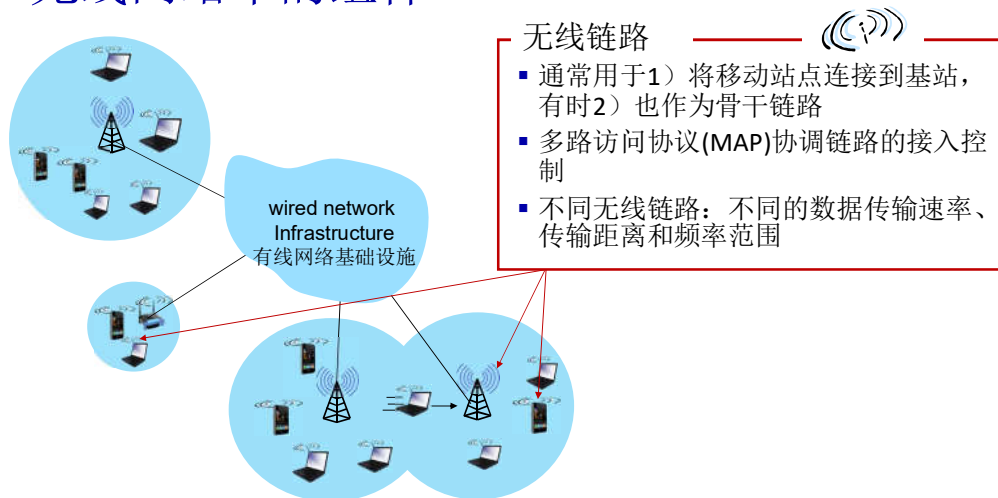
Wireless and Mobile Networks: 7- 5

## 无线网络中的组件



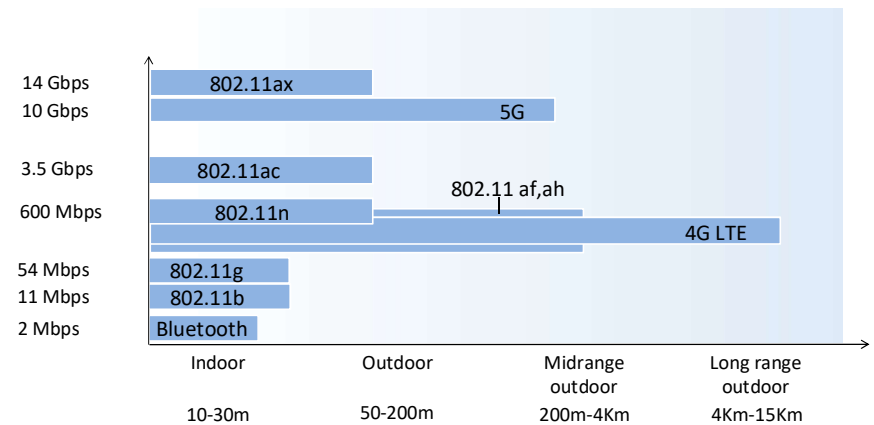
Wireless and Mobile Networks: 7- 6

## 无线网络中的组件



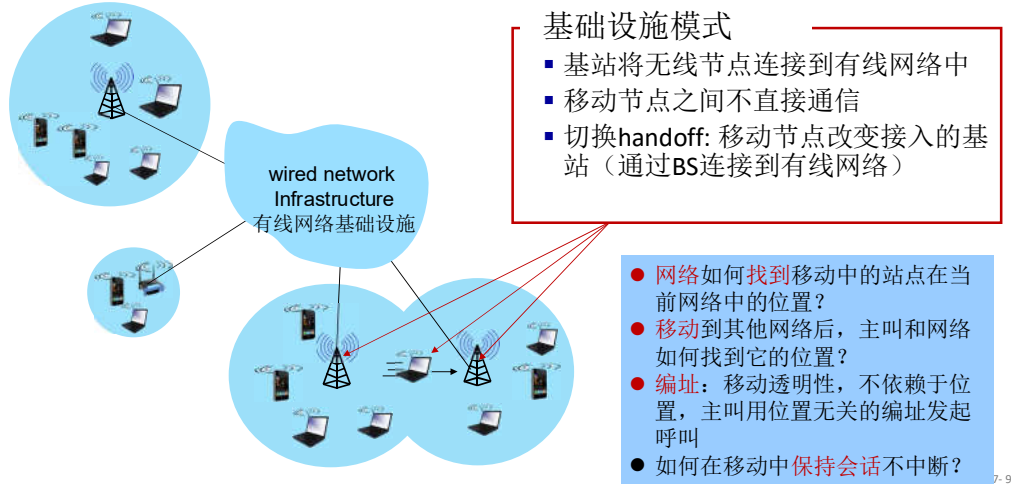
Wireless and Mobile Networks: 7- 7

## 一些无线链路的特征



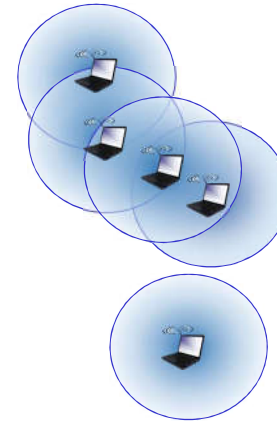
Wireless and Mobile Networks: 7- 8

# 无线网络中的组件



7-9

# 无线网络中的组件



## 自组织模式

- 没有基站这样的基础设施
- 节点只可以在其链路覆盖范围内将数据传输给其他节点
- 节点自动组织形成一个可以通信的网络: 相互路由

Wireless and Mobile Networks: 7- 10

# 无线网络分类

	单跳	多跳
有基础设施 (e. g. , APs)	主机连接到基站 (WiFi, WiMAX, cellular) 通过基站连接到 Internet 大网	主机可能不得不通过其他多个无线节点的中继来连接到更大的 Internet: mesh net 无线网状网络
无基础设施	没有基站, 也不连接到更大的 Internet (Bluetooth, ad hoc nets) 一个站点协调其他节点的传输	无基站, 也不连接到更大的 Internet. 可能不得不借助中间节点的中继到达目标节点 MANET, VANET

重点

# 第七章 提纲

## ■ 引论

## 无线

- 无线链路和网络特征
- WiFi: 802.11 无线局域网
- 蜂窝网络: 4G 和 5G

## 移动性

- 移动性管理: 原理
- 移动性管理: 实践
  - 4G/5G networks
  - Mobile IP
- 移动性: 对于高层协议的冲击



## 无线链路特征(1)

与有线链路的重要差别表现在:

- **衰减的信号强度**: 无线电波信号在通过物体 (即使是开放空间时) 时衰减(路径损耗)
  - ✓ 随着距离的平方成反比, 和物体材料性质、频率等有关
  - ✓ 而在有线导引型介质中, 任何2点的信号强度变化不是那么大
- **来自其他信号源的干扰**:
  - ✓ 标准无线网络频率 (e.g., 2.4 GHz) 与其它设备如无绳电话共享频段, 相互干扰;
  - ✓ 环境中的电磁噪声 (motors) 干扰
- **多路径传播**: 无线电波信号在物体表面和地面反射, 到达目标端的时间会有轻微的差别, 让信号变得模糊
  - 源和目标之间有移动中的物体, 多路径的传播时间会变化

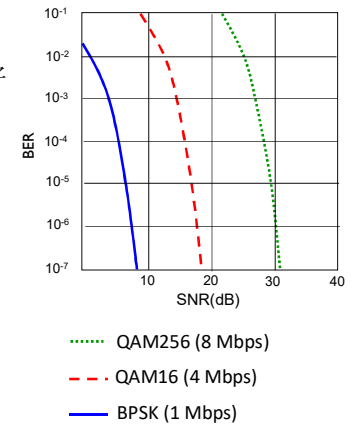


这些因素使得在无线链路上通信 (即使是点到点通信) 变得更加“困难”

Wireless and Mobile Networks: 7- 13

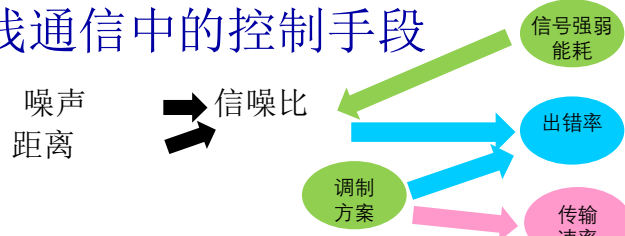
## 无线链路特征(2)

- SNR: 信噪比
  - $10 \lg(S/N)$  分贝
  - 更大的SNR - 更容易从噪声中提取信号 (“好事情”)
- SNR 与 BER 权衡
  - **给定调制方案**: 增加信号强度  $\rightarrow$  增加SNR  $\rightarrow$  降低 BER
  - **给定SNR**: 对于给定的调制方案, 高速率具有较高的BER
    - SNR 可以随着移动性的变化而变化: 给定信道条件, 自适应调整物理层调制方案 (调制技术和对应的传输速率)
    - 在可接受BER的情况下 (出错率), 尽可能快传 (速率)



Wireless and Mobile Networks: 7- 14

## 无线通信中的控制手段



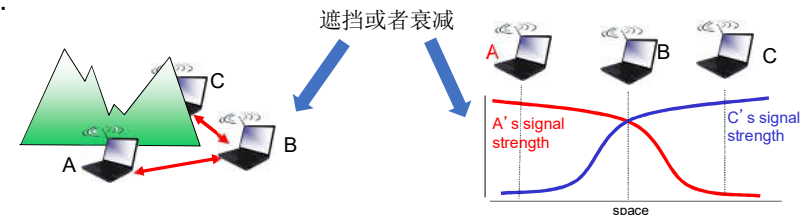
控制目标: 出错率可接收的情况下, 减少能量支出, 提高数据传输速率

- 控制方案:
  - 不改变调制方案情况 (速度不变) 下, 增或减信号强度 (能耗), 使得出错率可接受
    - 不改变传输速率: 减少出错率 (增加信号强度) or 减少能量支出 (可能增加出错率)
  - 不改变SNR (不变能耗), 改变调制方案 (速率), 出错率可控
    - 增加速率 (出错率可接受情况下) 或者降低 出错率 (通过降低调制方案, 降低速率方式)

Wireless and Mobile Networks: 7- 15

## 无线链路特征(3)

多个无线发送端和接收端带来的一些组网问题 (不仅仅是多路接入的问题):



### 隐藏终端问题

- B, A可以相互听得到
- B, C可以相互听得到
- A, C不能相互听到, 意味着A, C可能意识不到A, C在B附近的相互干扰

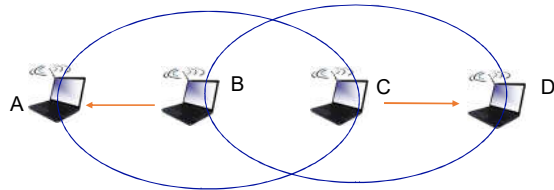
### 信号衰减

- B, A相互听得到
- B, C相互听得到
- A, C可能听不到它们在B附近的信号强度足以造成相互干扰

Wireless and Mobile Networks: 7- 16

## 无线链路特征 (3)

多个无线发送端和接收端带来的一些组网问题 (不仅仅是多路接入的问题):



### 暴露终端问题

- C向D发送
- B希望向A发送
- B在C的范围内，B侦听到C的发送，认为可能有冲突，不发送
- 影响效率

Wireless and Mobile Networks: 7- 17

## Code Division Multiple Access (CDMA)

### CDMA (code division multiple access) :

- 所有站点在同样频段上同时进行传输，采用编码原理加以区分
- 完全无冲突
- 假定：信号同步很好，线性叠加

### 比方

- TDM：不同的人在不同的时刻讲话
- FDM：不同的组在不同的小房间里通信
- CDMA：不同的人使用不同的语言讲话

Wireless and Mobile Networks: 7- 18

## Code Division Multiple Access (CDMA)

- 所有站点时钟同步，使用同一个频率
- 一个Bit时间，被分成m个时间片，芯片(chip)：64或128位
- 每个站点被分配一个m位的代码，芯片序列(chip sequence)，站点标识
- 双极性表示(1—**1**；0—**-1**)

A: 0 0 0 1 1 0 1 1  
B: 0 0 1 0 1 1 1 0  
C: 0 1 0 1 1 1 0 0  
D: 0 1 0 0 0 0 1 0

(a)

A: (-1 -1 -1 +1 +1 -1 +1 +1)  
B: (-1 -1 +1 -1 +1 +1 +1 -1)  
C: (-1 +1 -1 +1 +1 +1 -1 -1)  
D: (-1 +1 -1 -1 -1 -1 +1 -1)

(b)

Wireless and Mobile Networks: 7- 19

## Code Division Multiple Access (CDMA)

- S表示站点的芯片序列， $\bar{S}$ 表示芯片序列的反码
- 所有芯片序列都是两两正交的： $S \cdot T = 0$

$$S \cdot T = \frac{1}{m} \sum_{i=1}^m S_i T_i = 0 \quad S \cdot \bar{T} = \frac{1}{m} \sum_{i=1}^m S_i \bar{T}_i = 0$$

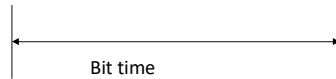
$$S \cdot S = \frac{1}{m} \sum_{i=1}^m S_i S_i = \frac{1}{m} \sum_{i=1}^m S_i^2 = \frac{1}{m} \sum_{i=1}^m (\pm 1)^2 = 1$$

正交：相应位相同的个数=相应位不同的个数

Wireless and Mobile Networks: 7- 20

## CDMA工作原理

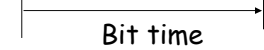
- 站点发送1: 站点将自己的芯片序列发送出去(一个bit时)
- 站点发送0: 站点将自己的芯片序列反码发送出去(一个bit时)
- 如:  $A = (-1 \ -1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1)$ 
  - 1:  $(-1 \ -1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1)$
  - 0:  $(+1 \ +1 \ +1 \ -1 \ -1 \ +1 \ -1 \ -1)$



## CDMA工作原理

- 多个站点同时发送, 信号叠加
  - 多个站点同时传输(同步)
  - 信号线性叠加在一起, 形成芯片序列

-- 1 --	<b>C</b>	$S_1 = (-1 \ +1 \ -1 \ +1 \ +1 \ -1 \ -1 \ -1)$
- 1 1 -	<b>B + <math>\bar{C}</math></b>	$S_2 = (-2 \ 0 \ 0 \ 0 \ +2 \ +2 \ 0 \ -2)$
1 0 --	<b>A + <math>\bar{B}</math></b>	$S_3 = (0 \ 0 \ -2 \ +2 \ 0 \ -2 \ 0 \ +2)$
1 0 1 -	<b>A + B + C</b>	$S_4 = (-1 \ +1 \ -3 \ +3 \ -1 \ -1 \ -1 \ +1)$
1 1 1 1	<b>A + B + C + D</b>	$S_5 = (-4 \ 0 \ -2 \ 0 \ +2 \ 0 \ +2 \ -2)$
1 1 0 1	<b>A + B + <math>\bar{C}</math> + D</b>	$S_6 = (-2 \ -2 \ 0 \ -2 \ 0 \ -2 \ +4 \ 0)$



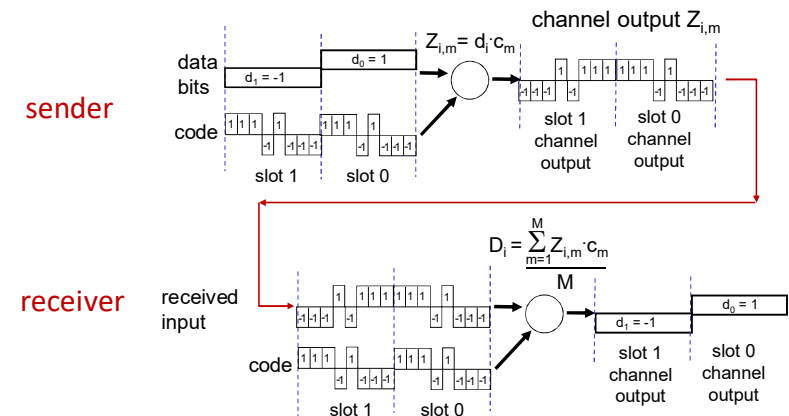
## CDMA工作原理

- 根据收到的芯片序列S(站点信号叠加而成)
- 发送站点的芯片序列C
- 计算出内积:  $S \cdot C$ , 可以还原出C原来发送的bit (流)
- 例子:  $S = A + B + C$

$$S \cdot C = (A + B + C) \cdot C = A \cdot C + B \cdot C + C \cdot C = 0 + 0 + 1 = 1$$

-- 1 --	<b>C</b>	$S_1 \cdot C = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1)/8 = 1$
- 1 1 -	<b>B + <math>\bar{C}</math></b>	$S_2 \cdot C = (2 + 0 + 0 + 0 + 2 + 2 + 0 + 2)/8 = 1$
1 0 --	<b>A + <math>\bar{B}</math></b>	$S_3 \cdot C = (0 + 0 + 2 + 2 + 0 + 2 + 0 + 2)/8 = 0$
1 0 1 -	<b>A + B + C</b>	$S_4 \cdot C = (1 + 1 + 3 + 3 + 1 + 1 + 1 + 1)/8 = 1$
1 1 1 1	<b>A + B + C + D</b>	$S_5 \cdot C = (4 + 0 + 2 + 0 + 2 + 0 + 2 + 2)/8 = 1$
1 1 0 1	<b>A + B + <math>\bar{C}</math> + D</b>	$S_6 \cdot C = (2 - 2 + 0 - 2 + 0 - 2 + 4 + 0)/8 = -1$

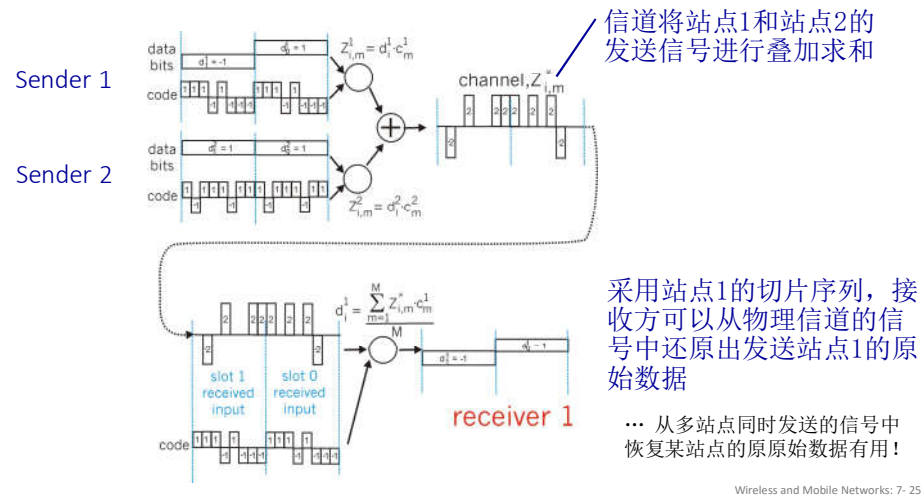
## CDMA 编码/解码



... 单站点发送和接收不是很有用!



# CDMA: 2个发送方的相互干扰



Wireless and Mobile Networks: 7- 25

## 第七章 提纲

### ■ 引论

### 无线

- 无线链路和网络特征
- WiFi: 802.11 无线局域网
- 蜂窝网络: 4G 和 5G

### 移动性

- 移动性管理: 原理
- 移动性管理: 实践
  - 4G/5G networks
  - Mobile IP
- 移动性: 对于高层协议的冲击



Wireless and Mobile Networks: 7- 26

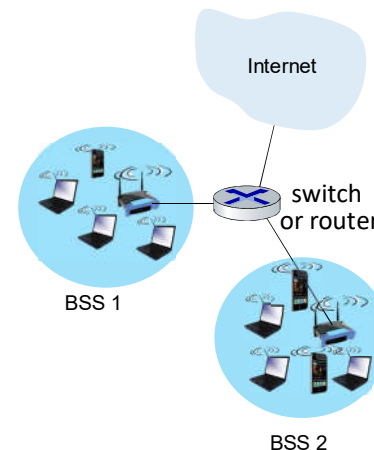
# IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- 不同点: 带宽、频率、范围和物理编码技术不同
- 共同之处: 在共享无线信道中使用CSMA/CA介质访问控制方式，而且都有基站模式和自组织模式（版本）

Wireless and Mobile Networks: 7- 27

# 802.11 LAN 体系结构



- 基础设施模式:
  - 无线主机
  - 接入点 (AP): 基站Base Station
  - 基本服务集 (BSS: Basic Service Set), cell
- 自组织模式:
  - 只有无线主机

Wireless and Mobile Networks: 7- 28

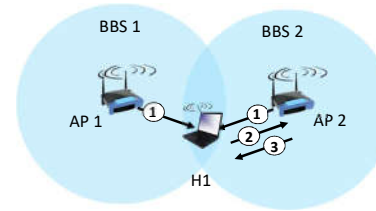
## 802.11: 信道与关联

- 频谱被分为多个不同频段的信道
  - AP管理员为AP选择一个频段
  - 可能的干扰: 邻居AP可能选择同样一个信道!
- 主机: 必须在通信之前和AP建立 *associate*
  - 扫描所有的信道, 侦听包含AP SSID和MAC地址的信标帧
    - ✓ 主动扫描: 主机发送探测, 接受AP的响应
    - ✓ 被动扫描
  - 选择希望关联的AP
  - 可能需要执行鉴别 (认证) [Chapter 8]
    - ✓ 基于MAC、用户名口令
    - ✓ 通过AP的中继, 使用RADIUS鉴别服务器进行身份鉴别
  - 将会执行DHCP获得IP地址和AP所在的子网前缀



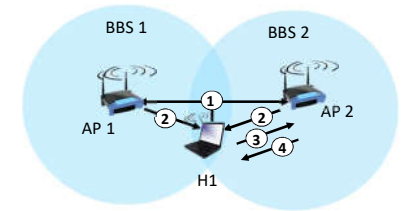
Wireless and Mobile Networks: 7- 29

## 802.11: 被动/主动扫描



### 被动扫描:

- (1) AP发送信标帧
- (2) 关联请求帧的发送: H1向拟关联的AP
- (3) 关联响应帧的发送: AP向H1



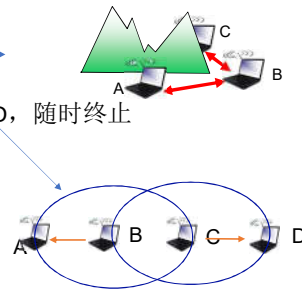
### 主动扫描:

- (1) H1广播探测请求帧
- (2) 自AP发送探测响应
- (3) H1向选择的AP发送关联请求帧
- (4) 选择的AP向H1发送关联响应帧

Wireless and Mobile Networks: 7- 30

## IEEE 802.11: MAC问题

- 802.11: CSMA – 发送前侦听信道
  - 不会和正在进行的传输发生冲突
- 无线链路及无线网络的组网特性, 无法进行冲突检测 (CD)
  - 发送站点接收到的自身信号, 要比接收到其他站点信号强很多, CD难
  - 不冲突≠成功, CD检测没有意义
    - 隐藏终端+信号衰减: 无冲突, 也不意味着成功 (下图A和C)
    - 暴露终端: 即使当前位置有冲突, 并不意味着发送是失败的;
  - 只能: 一旦发送, 一股脑全部发完, 而不是在发送过程中CD, 随时终止
  - 问题: 一旦冲突, 信道浪费严重
- 技术: C(ollision)A(voidance)
  - 只能在事前措施减少冲突, 避免2+ 站点在同一个时刻发送
  - 目标: 提高信道的利用率



Wireless and Mobile Networks: 7- 31

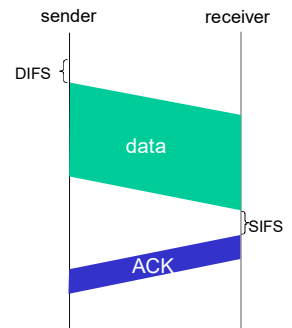
## IEEE 802.11 MAC协议: CSMA/CA

### 802.11 发送方

- 1 如果站点侦测到信道空闲持续DIFS长, 则传输整个帧 (no CD)
  - 2 如果侦测到信道忙碌, 那么 选择一个随机回退值, 并在信道空闲时按照节拍递减该值 (如果信道忙碌, 回退值不会变化)
- 计数到0时 (只发生在信道空闲时) 发整个帧  
如果没有收到ACK, 倍增回退值, 重复2

### 802.11 接收方

如果帧正确, 则在SIFS后发送ACK



(需要每帧确认; 例如: 由于无线组网中的隐藏终端问题, 在接收端可能形成发送方无法感知的干扰, 导致接收方没有正确地收到, 必须提供链路层可靠机制, 让链路层漏出去的错误比较少)

Wireless and Mobile Networks: 7- 32



## IEEE 802.11 MAC 协议: CSMA/CA

- 在count down时, 侦听到信道空闲为什么不发, 而要等到计到0时再发
  - 2个站点AB有数据帧要发送, 第三个节点C正在发送
  - 在LAN中, 有CSMA/CD: 让2者AB听完第三个节点C发完, 立即发送
    - ✓AB冲突: 放弃当前的发送, 避免了信道的浪费于无用冲突帧的发送
    - ✓代价不昂贵
  - 而在WLAN中: CSMA/CA
    - ✓无法CD, 一旦发送就必须发完, 如果冲突信道浪费非常严重, 冲突在无线网络中是一个严重的事件, 代价高昂
    - ✓如果2个站点等到信道空闲, 马上发送, 就会立即引起冲突, 代价昂贵
      - ✓因此: 需要尽量避免冲突, 而不是在发生冲突时放弃然后重发
    - ✓听到发送的站点, 分别选择随机值, 回退到0发送
      - 不同的随机值, AB中的一个站点(假设A)会胜利
      - 失败站点(假设B)会冻结计数器, 当胜利节点(假设A)发完再发

Wireless and Mobile Networks: 7- 33

## IEEE 802.11 MAC 协议: CSMA/CA

## 无法完全避免冲突

- 情况A: 两个站点相互隐藏
  - A, C相互隐藏, B在传输
  - A, C选择了随机回退值
  - 一个节点如A胜利了, 发送
  - 而C节点收不到, 顺利count down到0 发送
  - A, C的发送在B附近形成了干扰
- 情况B: 选择了非常靠近的随机回退值
  - A, B选择的值非常近, A的值小
  - A倒计到0后发送
  - 但是这个信号还没到达B时
  - B也到0了, 发送
  - 冲突



Wireless and Mobile Networks: 7- 34

## 冲突避免(续)

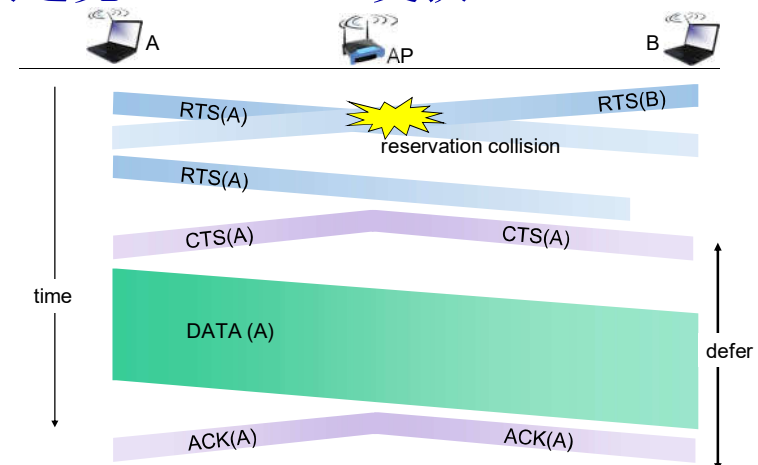
**思想:** 允许发送方“预约”信道, 而不是随机访问该信道: 避免长数据帧的冲突(可选项)

- 发送方首先使用CSMA向BS发送一个小的RTS分组
  - RTS可能会冲突(但是由于比较短, 浪费信道比较少)
- BS广播 clear-to-send CTS, 作为RTS的响应
- CTS能够被所有涉及到的节点听到
  - 发送方发送数据帧
  - 其它节点抑制发送

采用小的预约分组, 可以完全避免长数据帧的冲突

Wireless and Mobile Networks: 7- 35

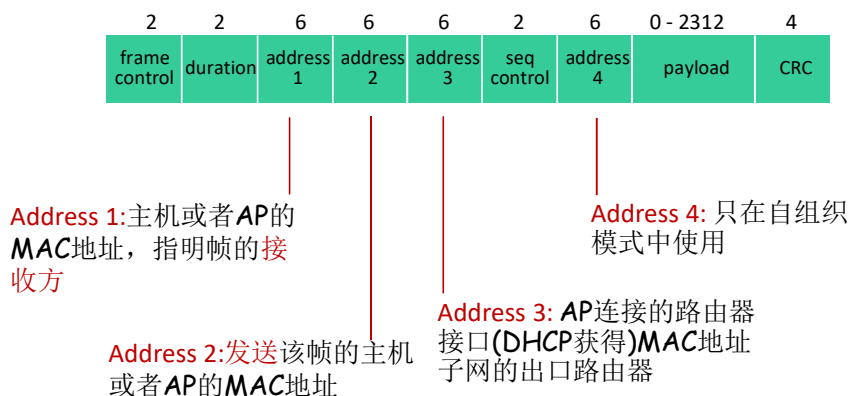
## 冲突避免: RTS-CTS 交换



Wireless and Mobile Networks: 7- 36

## 802.11 帧结构：地址

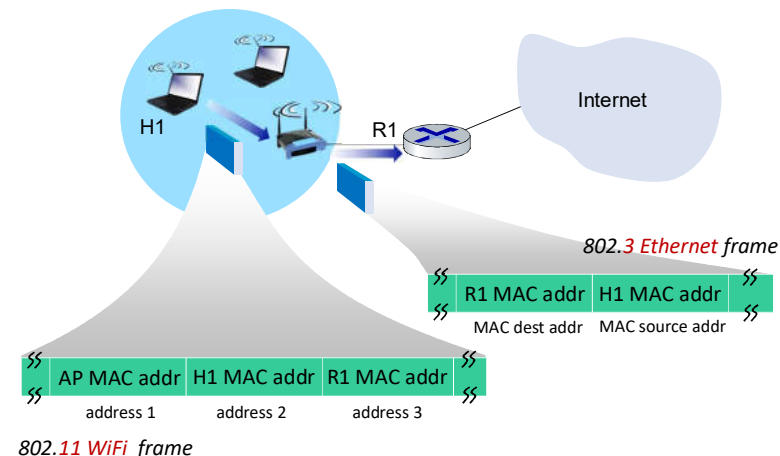
2021 中科大高网



Wireless and Mobile Networks: 7- 37

## 802.11 帧结构：地址

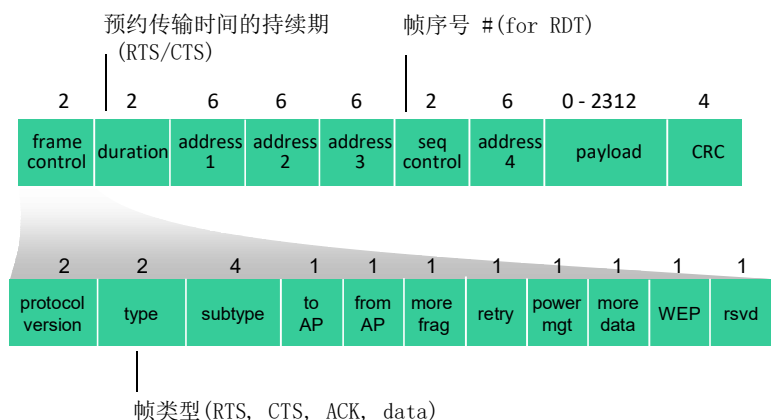
2021 中科大高网



Wireless and Mobile Networks: 7- 38

## 802.11 帧结构：地址

2021 中科大高网

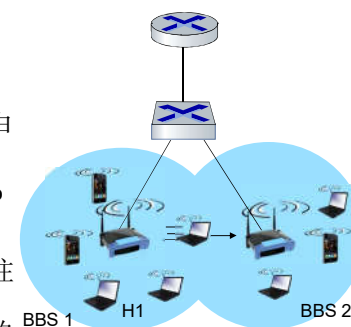


Wireless and Mobile Networks: 7- 39

## 802.11: 在相同子网中的移动性

2021 中科大高网

- H1在两个BSS间移动
- H1仍在一个IP子网范围内: IP地址保持一致
- 如何在一个子网范围内移动中保持一个TCP连接
- H1原来由AP1关联, H1感知信号变弱, H1申请改由AP2关联
- 交换机侧: 如何知道采用哪一个AP关联H1?
  - 自学习(Ch.5)
  - 原来从sw的某个端口收到来自H1-AP1的帧, 记住mac-port的映射
  - 移动并切换到AP2后, H2与AP2关联, AP2以H1的源地址向SW发送一个广播帧, 让sw记住端口-mac地址的映射

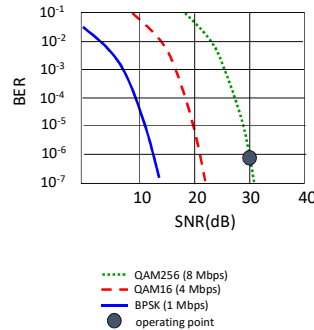


Wireless and Mobile Networks: 7- 40

## 802.11: 高级能力

### 速率自适应

- 基站，移动主机动态变换传输速率(当移动站点移动从而SNR变化时，改变物理层调制技术)
  - 连续两个帧没有确认，降低
  - 连续10帧得到确认，提高
- 移动节点离基站近，SNR高，可用高速率调制技术，BER也很低
- 移动节点离基站远，SNR变低，如果还用原来的调制技术，速率很高但是BER很高难以接受
- 改变物理调制方案，降低速率，使得BER低到可接受



1. 当站点离基站越来越远时，SNR降低，BER增加
2. 当BER变得太高时，切换到低传输速率但是低的BER

Wireless and Mobile Networks: 7-41

## 802.11: 高级能力

### 功率管理

- 目标：最小化节点侦听，传输和接收所需要的打开电路的时间 <1% =>节能，待机时间长
- 节点-AP：“我会休眠到下一个信标帧的到来”，功率标志位置1
  - ✓ AP 知道不要向该节点进行传输帧，缓存到它的帧
  - ✓ 通过定时器，节点在下一个信标帧到来时醒来，耗时250us
- 信标帧：包含一个移动节点的列表，AP需要向这些移动节点发送刚刚缓存的帧，每100ms
  - ✓ 如果有到达某个节点的帧，该节点活跃状态；向AP发送探寻报文明确地请求缓存的帧
  - ✓ 如果没有，该节点返回睡眠状态，直到下一个信标帧到来

Wireless and Mobile Networks: 7-42

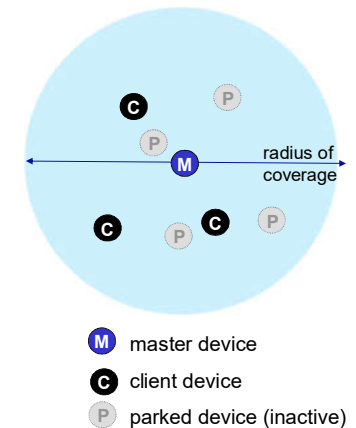
## Personal area networks: Bluetooth

- 4G、5G：大功率、中长距离（10km），高速率
- 802.11：大功率、中等距离（100m），高速率
- 802.15：小功率、近距离（10m-30m）、低成本
  - 线缆替代
  - 作用：电脑连接键盘外部设备、手机连接耳机等
- 802.15的链路层和物理层基于早期的蓝牙规范
- 各蓝牙设备之间构成了WPAN
  - 一跳、无基础设施
  - 自组织网络
- 仅在链路层就集成了大量技术：
  - TDM、FDM、随机退避、轮训
  - 检错纠错
  - Rdt、ACK和NAK等

Wireless and Mobile Networks: 7-43

## Personal area networks: Bluetooth

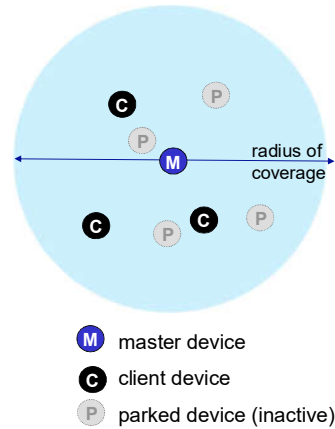
- 频段：2.4-2.5 GHz 开放频段
  - 无需注册，ISM无线电波段
  - 设备多，干扰多
- FHSS跳频扩展通信方式尽量减少干扰
  - TDM: 625  $\mu$ s/slot
  - FDM: 79个频道，每个channel不同频率
  - 站点按照预定模式在各个频道上跳频传输
- 主节点master/从节点slaves
  - 指定主节点
  - 从节点需要请求允许发送（向主节点）
  - 主节点授权请求



Wireless and Mobile Networks: 7-44

## Personal area networks: Bluetooth

- 自组织网络
  - 最多8个活跃设备
  - 主设备、其他都是客户端设备
  - 最多255个处在驻车模式的非活跃设备
- 主设备控制piconet的运行
  - Slot的同步时钟周期
  - 跳频序列
  - 客户端是否可以进入到piconet
  - 运行功率
  - 轮寻授权客户端授权其是否可以发送



Wireless and Mobile Networks: 7- 45

## Personal area networks: Bluetooth

- 组网1: 邻居发现
  - 主设备在不同频道上广播32个查询报文序列、最多128次
  - 从设备侦听指定频道
  - 从设备采用退避算法应答器，包含其设备ID
- 组网2: 寻呼Bluetooth paging
  - 主设备: 发送邀请报文
    - 32个同样的邀请，在**不同频道**上邀请不同客户端（客户端还没学到模式）
    - 包含有: 不同从设备的地址
  - 从设备回应ACK
  - 主设备发送: 跳频信息，时钟同步信息，活跃设备地址信息
  - 主设备最后采用约定跳频模式**轮询**客户端，确保从设备联网

Wireless and Mobile Networks: 7- 46