

## 主题 3:无线网络

### 第 1 章:无线网络

#### 1 - 简介

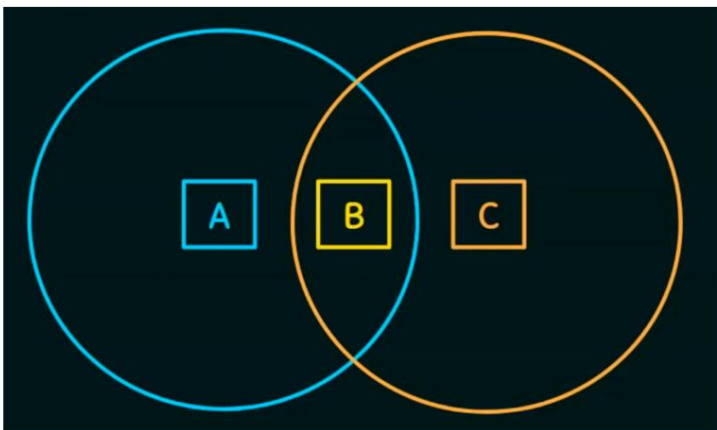
也称为 IEEE 802.11。

它可以根据两种架构运行：

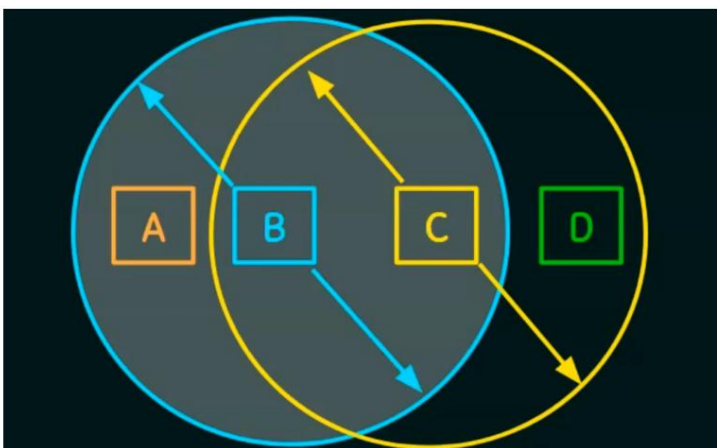
- WLAN:最著名的集中式架构,设备连接到接入点（盒子）:允许访问 Internet 并与其他网络设备通信
- Ad-Hoc:分布式架构:无接入点,允许两台机器之间进行通信而不使用基础设施（有点类似于蓝牙提供的）

在 WLAN 架构中:主要问题:接入接入点（两个站不能同时向 PA 传输）

#### 2 - 获得支持的问题



-隐藏终端问题:A和C是要传输的终端,B是接入点。A看不到C,C看不到A。因此,如果两者同时发光,他们将不知道并且会发生碰撞。我们将不得不找到解决这个问题的方法。



-暴露的终端问题:这个  
有时我们会查看航站楼 B 和 C,它们都近在咫尺。

假设 B 向 A 传输。因此,C 将假设它不能传输,因为 B 已经在传输。但这是一个错误,因为 C 可以在 B 向 A 传输的同时传输给 D。

我们还将进一步研究如何解决这个问题。

现有的 MAC 协议无法解决这些不同的问题（例如 CSMA/CD）。

-> MACA 的出现:避免碰撞的多路访问。

引入RTS/CTS协议解决以上两个问题：

- RTS/CTS解决隐藏终端：

我们以上面的例子为例：1)如果C要发

送,它发送RTS (请求发送)给B,表示发送的持续时间  
传输来

2) B (接入点)用 CTS (清除发送)响应 C

3) A 也将收到 CTS 并推断它不能传输 a  
一段时间 (用 C 表示)

4) C将数据包转发给B

- RTS/CTS解决暴露终端:应该记住,在此之前允许解决这个问题,但是新版本的 RTS/CTS 不再允许它,因为实现了  
ACK。

关于CSMA/CA:获得支持的机制。它在发送 RTS 之前使用。除了 CSMA/CA 之外,在 MAC 级别设置了 ARQ 机制 (数据的  
发送者将向发送者发送 ACK) ,并且与以太网一样,存在可能重传的 Backoff。

### 3 - 组播/广播:组播/广播可能是无线

网络中的问题,尤其是冲突问题。为避免这种情况,帧以尽可能低的速率发送。这不是最佳的,因此其他解决方案之一  
是将多播转换为完整的单播。

### 4 - WiFi 上的 QoS?

通过播放特别是在 MAC 层上引入 Wifi 中的 QoS。EDCA 协议 (增强型分布式信道访问)的开发允许流量优先级,因  
此是一种 QoS 工具。

### 5- PHY 层自从 WiFi 的

发展,速度得到了提高。但是仍然有一个不变量:不可能保证给定的速度。这有几个原因: 与有线网络相比,空中是一  
个非常复杂的环境。此外,到接入点的距离、终端在传输过程中的移动等……使得无法保证恒定的流量。

无线电信道的主要问题： - 路径丢失 - 同频信号的  
干扰 - 阴影 (穿过障碍物的信号衰减)

- 反射 (对障碍物的反射:信号不通过)

- 多路径 (终端多次接收信号)

因此,最后这些问题也解释了为什么我们的 WiFi 速度存在如此大的差异,以及为什么我们不能保  
证这样的速度。

为了克服这个问题,已经实现了几种算法:

1) ARF (自动速率回退)。这是一种算法,可以让 PA 被告知以什么速率发送。起初,算法告诉 PA 以它识别的最大速率传输,然后它的工作方式有点像 TCP:

- 如果没有 ACK (丢包):我们降低流量
- 如果有 10 个连续的 ACK:我们增加流量
- >弱点:不考虑数据包重传

2) Onoe:尝试 (长期)找到损失低于 50% 的流量。

工作起来有点像 ARF,但会查看数据包是否已被重传很多以增加或减少吞吐量: - 开始时:最大吞吐量,信用计数器为 0 然后,每秒一次: - 如果没有数据包,则增加吞吐量已成功发送或已发送 10 个或更多数据包且每个数据包的平均重传次数大于 1

- 如果借方超过 10 个贷方,则增加贷方 (贷方为分布如下:如果少于 10% 的数据包需要重新发送,我们增加信用,否则我们减少它)

->结论:小野江比较保守,可能需要时间才能稳定下来

3) Receiver Based Auto Rate (RBAR):基本上,这种机制将使用 RTS/CTS 消息来询问接收者他应该以什么速率传输。

4) Opportunistic Auto-Rate (OAR):也将使用 RTS/CTS 来控制速率。(我不理解这个协议,这是一个黑暗的东西,在过去的 20 年里一直有一篇研究论文。

5) SampleRate:基本上,将尝试找到可能的最佳比特率,事先有一个表,其中包含不同的比特率及其发送数据包的速率。然后: - 开始时,它选择可能的最高比特率 它在连续 4 次下降后改变比特率

-

- 每 10 个数据包,它需要一个随机的比特率,它应该比当前的比特率更好。(这些比特率是从他之前制作的表格中选择的)。

请记住:所有流量控制算法都是针对单播流量的,它们都需要接收器的反馈

## 第 2 章:速率控制 + Ad-hoc 网络

## 1 - Ad Hoc 网络

无需事先协调即可动态创建的网络

每个站都是一个路由器

优点：

- 轻松快速的部署
- 网络较少依赖基础设施

⇒兴趣：

- 军事 → 无需电话接线员的通信 (DARPA 分组无线电网络 1973-1987) 民用 →
- 隔离社区通信、网状网络

对称环境→所有节点具有相同的能力和职责

不对称能力 → 差异： - 传输范围 - 自主性 - 计算能力 -  
移动速度

非对称职责： - 只有某些节点是路由器 -  
某些节点是一组节点的头

Ad hoc 网络可以与基础架构模式下的网络共存

## 2 - MANET 中的单播路由

MANET = 移动自组织网络

问题：

- 节点的移动性 → 链路上的错误率↑如果节点移动迅速
- 新的性能标准：道路稳定性尽管移动性，能源消耗

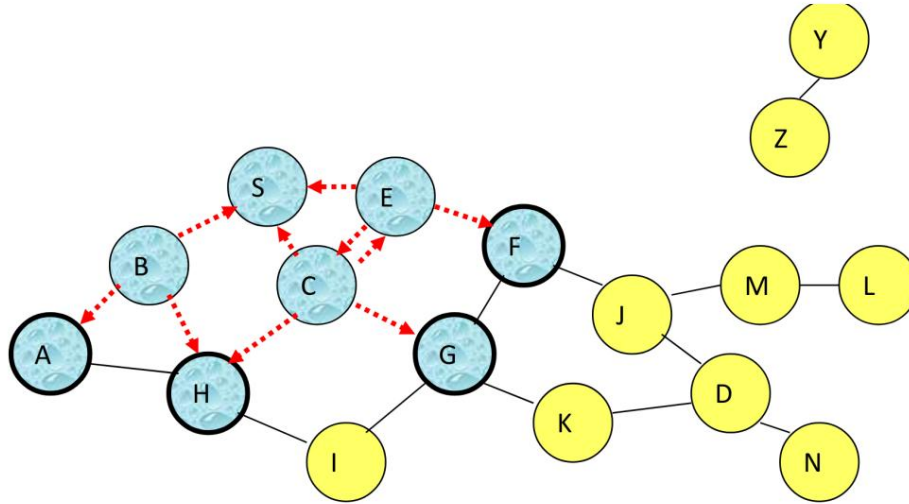
路由协议的类型：

- 主动→确定独立于交通的路线（传统）  
Overhead +, Latency - (当我们要传输的时候路由已经存在)
- 反应式→仅在需要时计算路线  
高架 -, 延迟 + (因为路由是在传输时计算的)
- 还有混合协议

## 3 - 路由方法

### 3.1 - 数据传输的洪泛 源节点 S 将

它的数据包广播给它的所有邻居,这些邻居将它传输给他们所有的邻居,等等.....直到目的地 D 收到数据包 (D 不重新传输数据包)



评论：\_\_\_\_\_

- 用于不两次传输相同数据包的序列号
- 来自站点的 2 个同时传输期间的潜在冲突  
彼此隐藏→节点可能不会收到数据包（例如D）
- **最坏情况:从 S 可达的所有节点都接收到数据包**

优点:

- 简单的
- 在传输的信息很少时比其他协议更有效,并且其他协议开销大 (小包传输不频繁,网络拓扑变化频繁时)
- 潜在 + 重要的可靠性 (1 个数据包的多路径)

缺点:\_\_\_\_\_

- 非常大的潜在开销（许多节点接收到的数据包他们不是收件人）
- 潜在的可靠性 - 很重要,因为没有开销和冲突的不可靠广播会阻止接收

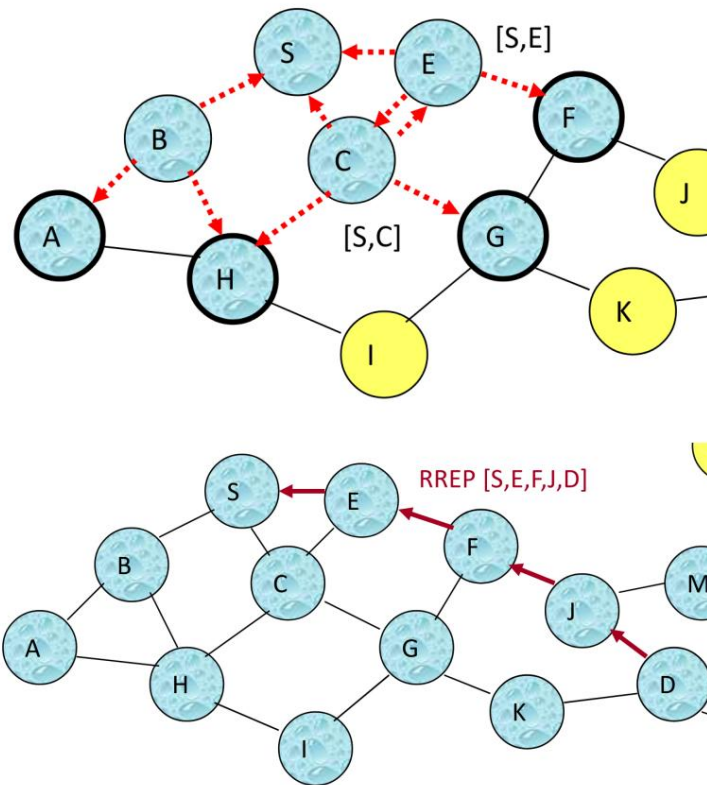
### 3.2 - 控制数据包的泛洪泛洪仅限于控制帧,用

于发现路由→这些路由稍后将用于路由数据→通过路由上传的数据量摊销的开销

### 3.3 - 动态源路由 (DSR)

如果 S 不知道到 D 的路由,它会开始路由发现: - S 用路由请求(RREQ)淹没网络

- 每个节点通过添加其标识符来转发单个 RREQ - D 不转发任何 RREQ,但发送路由回复 (RREP)
- RREP 在通过反转 RREQ 中包含的路由获得的路由上发送 (假设链路是双向,否则D在RREQD→S 上捎带 RREPS→D 向 S发发现路由)
- RREP 包含了从 S 到 D 的路由,D 收到的 RREP 通过该路由



发送数据包时,完整的路由包含在包头中。

优点: - 仅在通

信的节点之间维护路由,并放入  
缓存 → 减少开销

- 单个发现路由提供到目的地的多条路由

缺点:

- 源路由 → 标头大小 ↗ - RREQ 可能到达所有节点

- 避免 RREQ 之间的冲突

- 如果太多节点响应它们缓存的路由,则会出现拥塞 →

路由回复风暴,如果一个节点听到的 RREP 比它自己的短,那么它可以避免响应

### 3.4 - Ad Hoc 按需距离矢量路由 (AODV)

尝试通过在节点上而不是在数据包中存储路由来改进 DSR。

当一个节点收到一个 RREQ 时,它会注册一条通往该 RREQ 的路由 (反向路径)

资源。

节点只保留当前使用的路由的反向路径 (超时后过期)

通过在相邻节点之间定期发送 Hello 消息来检测链路故障 使用路由错误(RRER) 消息向源发送链路故障信号。S 收到 RRER

→ 启动新路由发现

可能的优化:RREQs 首先以低 TTL 发送以限制它们的传播,然后如果没有收到 RREP,则从 + 到 +。

### 3.5 - 链路状态路由 (LSR)

主动路由: - 每个节

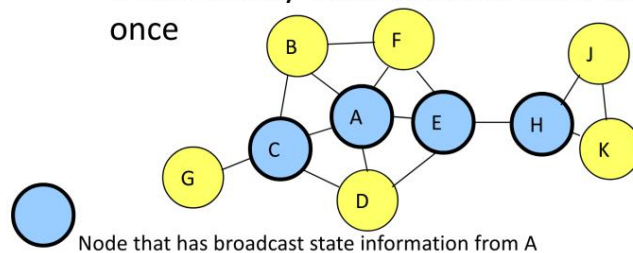
点定期发送其链接信息 - 每个节点重新传输其邻居的信息 - 每个节点使用所有这些  
信息来计算路由

### 3.6 - 优化的 LSR (OLSR)

与 LSR 相比开销更少,因为只有节点 X 的所谓多点中继节点重新传输信息,因此更少的节点重新传输信息。

节点 X 的多点中继节点是 X 的邻居,使得 X 在距离 2 处的每个邻居都是 X 的多点中继距离 1 处的邻居。

- Nodes E and K are multipoint relays for node H
- Node K forwards information received from H
  - E has already forwarded the same information once



## 第 3 章:基于 WiFi 的室内定位

GPS在建筑物内无法正常工作,可以使用WiFi替代它。

### 1 - 基于指纹的位置 (RADAR)

---

RADAR 是一种基于射频的系统,用于定位和跟踪建筑物内的用户,它允许使用现有的无线 LAN 基础设施。它基于这样一个事实,即接收信号的强度与到基站的距离之间存在相关性。

#### 1.1 - 学习阶段 (离线)

---

我们从创建一个无线电卡开始,我们可以使用两种方法:

##### 1.1.1 - 经验法

---

- 基站定期发射信标:我们将  
在很多地方保存 SS (信号强度)字段
- 保存范围内站点的SS和对应的坐标  
(还必须考虑用户方向,对于  $n$  个基站,元组的形式为  $(x,y,d,ss_1,\dots,ss_n)$ )
- 精确但有限制 (我们必须手动进行测量,如果我们  
移动一个基站,你必须重建无线电卡)

##### 1.1.2 - 数学方法

---

- 使用简单的传播模型计算 SS (考虑路径损耗和壁衰减)
- 更实用但不太精确

### 1.2 - 运营阶段

---

- 从基站信标帧中提取 SS
- 以 SS 作为输入向基站发送位置请求
- 找到与测量的 SS 最对应的无线电卡条目 (我们  
最小化测量值  $(ss_1, ss_2, ss_3)$  和无线电地图数据  $(ss_1, ss_2, ss_3)$  之间的欧几里得距离,以获得位置  $(x,y,d)$ 。

为了评估这种方法的性能,可以从无线电地图中删除一个已知点,然后尝试从其余数据中估计其位置。无线电地图包含的点越多,我们就越精确。平均而言,我们在该位置上获得了 3m 的精度。如果我们对几个邻居进行平均,我们可以下降到 2m。

对于移动它的移动用户稍微复杂一点,我们使用 10 个 SS 样本的滑动窗口以连续方式计算信号的平均强度,精度比静止用户差一点 (~ 3.5 米)。

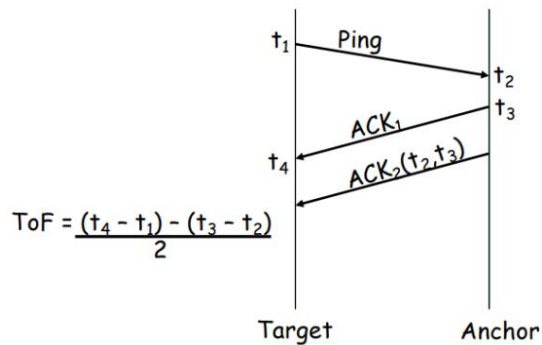
### 2 - 基于飞行时间的位置

---



定位问题简化为计算目标与坐标已知的一组点之间的距离的问题。计算两个设备之间的距离相当于计算一个信号在两个设备之间传播所需的时间 (ToF)。

双向测距 (TWR):



ACK2需要避免必须同步两台机器的时钟。

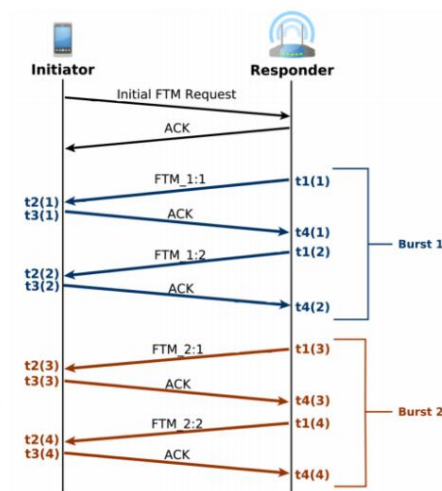
### 3 - WIFI FTM (IEEE 802.11AC)

FTM = 精细时间测量,它允许 WiFi 站计算其与范围内接入点的距离,而无需与之关联 (精度为米级)。它受到主要 WiFi 和 Android 制造商的支持。

功能:

- 该过程从一个 WiFi 站 (称为发起者) 开始,它搜索支持 FTM 的接入点。
- 如果检测到支持 FTM 的接入点,则发起方向其发送 FTM 请求帧。
- 收到此请求后,接入点可以选择忽略它或成为响应者。
- 两个站开始一系列的突发 (由电话答录机发送) FTM 数据包,然后是发起方的 ACK) ,允许发起方估计与响应方的往返时间 (RTT) 。

$$RTT = \frac{1}{N} \sum_{i=1}^N (t_4(i) - t_1(i))$$



问题:当接入点和站点之间有障碍物时,测量到的信号可能会从墙上反弹 -> 测量的距离将是信号行进的距离,因此大于在线距离。

## 第 4 章 :物联网 (IoT)

物联网的定义 :通过互联网将嵌入日常物品的计算设备互连,使它们能够传输和接收数据

物联网应用示例 :互联健康对象、智慧城市、交通等。

物联网的基本特征 :

异构性 :传感器、网络 (范围、容量、功耗、基础设施)、应用

规模 :设备数量而不是数据量 (预计有数十亿台设备 => 强制 IPv6)

### BLUETOOTH事实

上,本课程几乎没有谈到物联网,但特别是打击 jsp 的蓝牙,为什么它被称为1 - 由制造商爱立信于 1994 年创建的介绍历史标准。

\_\_\_\_\_

\_\_\_\_\_

目标 :低功耗,便宜,替代短电缆 (0-10m范围,低数据速率19.2-100kbps)

1998 年,制造商爱立信、诺基亚、IBM、东芝、英特尔……成立了一个兴趣小组,以开发满足这些目标的解决方案 => 1999 年发布的规范

=> IEEE 802.15 = WPAN (无线个域网) = 蓝牙 => 4 个工作组的定义: · 802.15.1 = 10m 范围内设备无线连接的物理层和 MAC 层规范 (也称为 POS = 个人操作空间,POS 可以是静态的或移动的) · 802.15.2 = WLAN (=WiFi) 和 WPAN 之间的共存和互操作性

(=蓝牙) ·  
802.15.3 = 多媒体的高速 (高达 20Mbps) · 802.15.4 = 低功耗和复杂性的  
的低速设备

蓝牙标准 :规定了整个系统,从无线电层到应用层。协议栈部分位于硬件级别,部分位于软件级别。

关于蓝牙的一些概念:

·与 Wifi使用相同的2.4 GHz频段。 · 它基于跳频扩频 (= 跳频扩频) :cf.蓝牙  
规格如下 · 10m 范围内的 2 个设备可以交换高达 720kbps 的

能力

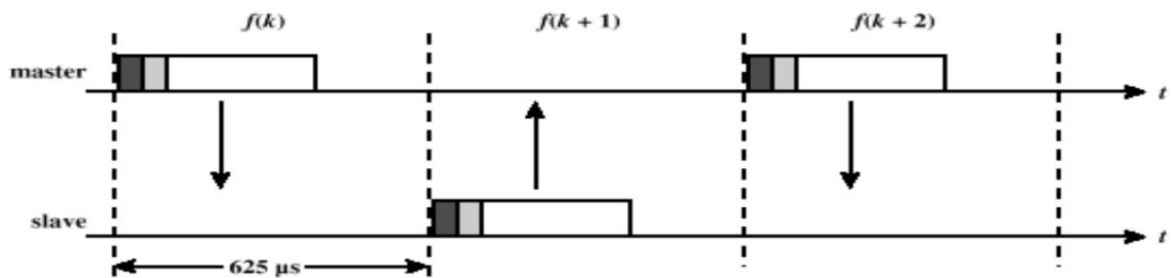
### 2 - 跳频扩频

定义 :跳频扩频 (= 通过跳频扩频)=使用无线电波传输信号的方法

根据发射机和接收机已知的伪随机序列交替分布在频带中的几个信道（子载波）。

#### 蓝牙跳频扩频特性：

- 1 MHz宽频道（=>总共 79 个频道） - 频率/频道随每个数据包而变化- 每个时隙持续  $625\mu\text{s}$ （=> 1600 希望/秒） - 数据包的传输持续 1、3 或 5 个时隙（时隙≠信道 = 频率） - 传输的跳频序列在整个 piconet 内传输（见下面的定义），主机传输给从机



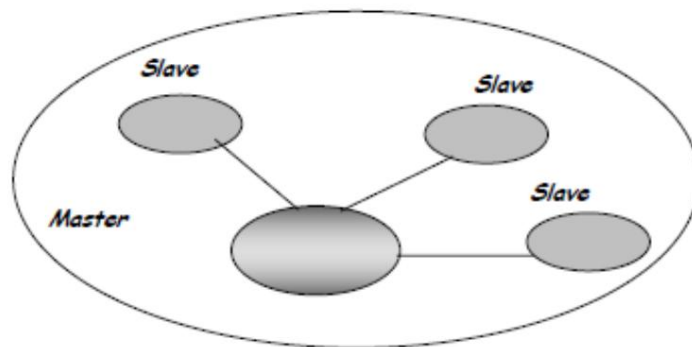
访问通道/频率 (TDD) · 主设备始终是发起数据交换

的人 · 从设备按照主设备指定的跳频顺序响应主设备 · 从设备仅响应主设备进行传输 · 主机在奇数时隙上传输,而从机在奇数时隙上传输

#### 同行

#### 3 - 微微网

微微网= 蓝牙架构 = 蓝牙网络的基本单元



我们有一个Master,最多可以有 7 个 Slave。他还控制着他的 Piconet 内的传输。微微网内部没有冲突。

另一种可能的蓝牙架构（但未见）： Scatternet （一个设备可以属于多个微微网,但一个设备只能是单个微微网的主控）

#### 创建一个微微网

一个微微网由一组微微网成员将使用的通信通道组成。一个通信信道由一系列明确定义的跳频组成。

微微网是如何创建的？ => 2个步骤：

查询和分页 (=查询/询问和分页)

#### 4 - Inquiry Procedure

Inquiry Procedure发送询

问/询问,实际上是对附近设备 (<10m)的请求。处于“可见模式”的设备会发出询问响应(此过程最多可能需要10.24 秒),之后设备必须知道 10 米内的每个人。

-

→如果查询消息有问题,可能有两种可能:发射机和接收机尚未连接,因此处于不同的跳频序列,因此处于不同的频道/频率;如果它们在同一个频道上,则可能会被噪音“杂乱无章”

#### 3.1 -询问消息的传输 发送询问的设备在 16 个不同的

频率上发送询问。这 16 个频率构成了查询跳序列,称为一系列。然后有 2 种类型的流:使用 GIAC 和 DIAC 的 28 个最低有效位(用于打印机)生成。传输在每个备用时隙上完成,而中间时隙用于侦听可能的响应。

#### 噪声管理 · 设备

始终以查询响应来响应查询消息。

允许查询设备从单个设备接收多个响应。

· 考虑到信道可能“嘈杂”并且传输可能丢失,一系列火车最多重复4次。

#### 3.2 - 查询扫描设备定

期监听一个频率(16个频率中)以查找查询消息。它保持这种状态的时间足以让询问设备覆盖所有16个频率。

#### 3.3 - 查询响应当在查询扫描

状态期间收到查询消息时,设备会发送一个包含其地址的响应包。收到请求后不直接发送此数据包,以避免冲突。设备等待随机数的完整查询扫描(介于0和127之间),然后将其FHS数据包发送到询问器,该FHS数据包包含其地址、时钟和指示设备何时进入其页面扫描状态的信息。接收响应的查询设备不直接确认后者

但继续其查询程序。仅当它想要寻呼设备时才会使用此响应。

## 5 - 寻呼程序

寻呼过程（与轮询非常相似的过程）

如果在查询过程之后需要连接 => 寻呼

这个过程只需要设备的地址来寻呼它,但是它的时钟（也包含在 FHS 数据包中)使得加速这个过程成为可能。

启动寻呼过程的设备将是由它自己和寻呼设备组成的微微网的主设备,如果后者接受连接。

## 6步程序:

1. 页面扫描:设备向其希望连接的设备发送消息页面（类似于查询消息,在2个频率列上,每列16个频率）。一旦收到响应页面,它将停止并转到步骤 2。
2. 在响应页面中,将包含从机 ID 的确认发送到  
掌握
3. 主机向从机发送一个FHS 数据包给它自己的时钟。 4. 从 FHS 数据包中的数据,从机采用主机的跳频序列并同步到它的时钟。从机发送与从机的本地时钟对齐的最后一个响应。
5. 当主机接收到一个数据包时,它返回到它的跳频模式,并为微微网中的从机分配一个活动成员地址 (AMA)。主机还探测（通过特定数据包)从机,以确保它处于其跳频模式。
6. 从机用任何数据包来响应这个轮询,以证明它在正确的通道上。主机必须在允许的时间内收到确认。在这一步结束时,主从之间建立了一个新的同步连接。

## 6 - 链接管理器他负责

所有链接的创建、管理和操作的结束。

负责系统中的所有物理链路资源（在数据传输过程中控制和协商包大小）。它控制微微网中设备的操作模式。建立、终止和管理服务之间的基带连接:根据来自 L2CAP 层（SCO 或 ACL)的请求建立不同类型的链路。

-

### 6.1 - ACL 链接（异步无连接）

专为数据传输而设计。包路由。通过错误检查和重传管理数据包完整性。主从之间的 ACL 链接。

### 6.2 - SCO 链接（面向同步连接）

专为音频或视频等实时信息而设计。定期传输数据的连接电路。不需要重传。每个微微网最多 3 个 SCO 链接。

### 6.3 - 链路管理器操作设备默认处于待机模式,直到它们连接到微微网。

有4种连接模式,允许设备调整 piconet 中的功耗、性能、角色和参与者数量:

- 活动模式:每个主站最多有7个活动从站。分配给每个活动从站的3位地址 (AM\_ADDR)。一个单元主动参与一个信道并在给定的帧上接收通信。一个单元消耗大量能量。
- 保持模式:释放从属设备参与另一个微微网,进行扫描、寻呼或查询,切换到节能模式。单元保存活跃成员的地址。该单元不再支持 ACL 数据包,但 SCO 数据包支持。主机和从机就等待时间达成一致,在此之后从机将返回与信道流量同步。低能耗。
- 嗅探模式:与保持模式非常相似。奴隶可以自由返回

固定的时间间隔。主设备只能在安排好的嗅探时隙进行通信

- 驻留模式:驻留单元离开活动成员的地址。为了管理停放单元的快速重新接纳,主机为其分配了2个临时8位地址。停放的单元与信道保持同步并以低功率空闲运行。她定期醒来以保持同步。此模式允许超过7个设备连接到一个主设备。

可以交换活动和停放的设备以允许多个连接到单个微微网。

### 6.4 - 分段和重组基带数据包的大小是有限的

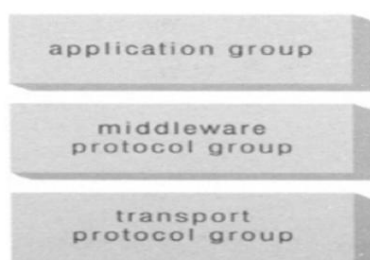
(最大有效载荷 = 2745 位)。L2CAP是蓝牙使用的一种协议,负责在上层和物理层之间进行适配(参见下面的传输组协议栈)。

L2CAP 接受最大 64kb 的数据包。L2CAP 将大数据包分割成更小更易于管理的基带数据包。然后重新组装这些数据包。

### 服务质量 一些应用程

序需要特定的服务质量参数:带宽峰值、启动、延迟变化等。L2CAP 在可能的情况下提供请求的 QoS,并在链路不能支持请求时通知应用程序。

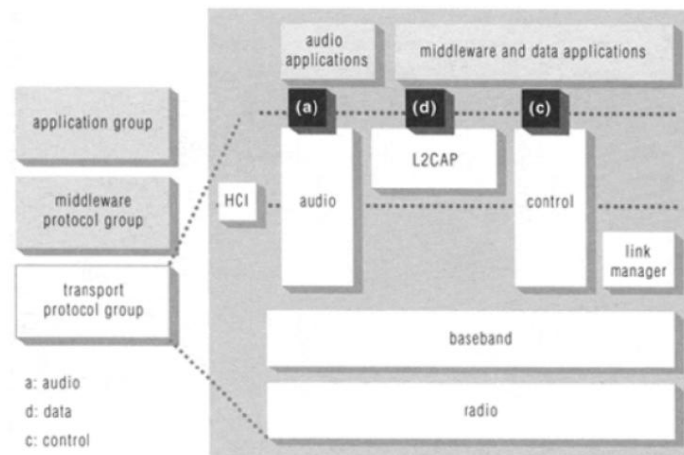
The Bluetooth Protocol Stack



传输协议组 = 允许蓝牙设备相互定位、创建、配置和管理它们的物理和逻辑链路

中间件协议组 = 新的和现有的应用程序需要在蓝牙链路上运行 => PPP、IP、TCP、RFCOMM

## Transport Protocol Group Stack



### 6.5 - 资产负债表

蓝牙的好处

- 低功耗
- 蓝牙组件价格低廉

蓝牙的缺点

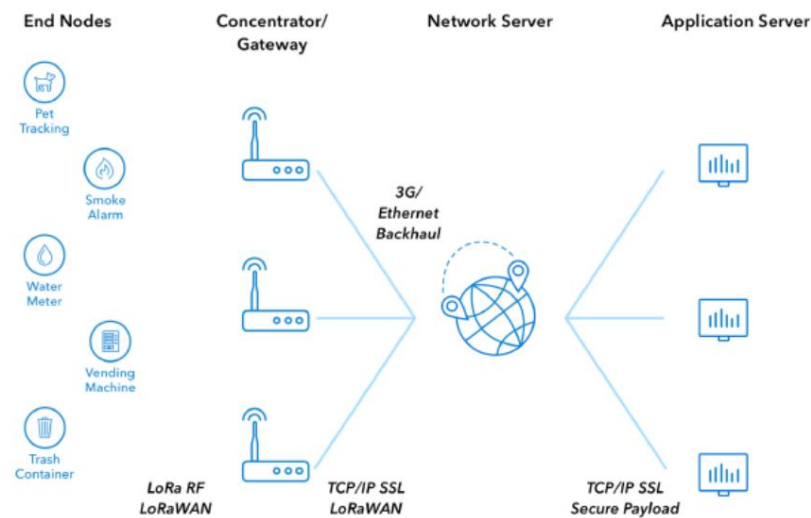
- 无线 LAN 网络提供更高的速度和更远的距离。
- 通信 - 2.4GHz 频段上的干扰可能性

### 6.6 - 更进一步LoRaWAN

= 电信协议,允许通过无线电对低功耗对象进行低速通信,使用 LoRa 技术进行通信并通过网关连接到互联网,从而参与物联网。

Specification	LoRa Technology Support
Standard	LoRa Alliance
Operational Frequencies	Unlicensed ISM band 868, 915 MHz
Modulation	Chirp spread spectrum (CSS)
Coverage Range (Km)	2 - 5 (urban) / 15 (rural)
Data Rate (kbps)	0.3 - 50 (EU) / 0.9 - 100 (US)
Topology	Star

6.6.1 - LoRaWAN 架构



LoRaWAN 架构的组件:

- 终端设备 (ED) :传感器可以在任何通道上传输，
- 随时使用可用速度
- GW :提供与 Internet 的连接并避免冲突
- 网络服务器 :监控 GW 和 ED,收集数据避免

- 副本,由哪个 GW 选择与 ED 通信
- 应用服务器 :有问题的物联网应用

终端设备类

