第7章 移动Ad hoc网络

内容介绍

1、移动Ad hoc网络技术概述
2、移动Ad hoc网络的体系结构
3、移动Ad Hoc网络信道接入协议
4、移动Ad Hoc网络的路由协议
5、移动Ad Hoc网络的功率控制
6、移动Ad Hoc网络的IP地址分配
7、移动Ad hoc网络的安全问题
8、移动Ad hoc网络的服务质量

移动Ad Hoc网络的需求背景

- 我们正在从个人计算机时代(即一个人一个计算装置)过渡到随遇计算时代(Ubiquitous Age)

- 提供所需要的连接和网络服务就成为一种挑战。

涉及的问题

- 移动问题
- 不需要基础设施支持的问题
- 动态自组织组网问题
- 网络必须能够快速展开的问题

解决方案

- 研究人员提出了不需要基础设施支持的移动Ad Hoc解决方案
- 移动Ad Hoc网络是复杂的分布式网络系统，是自组织、自愈网络，由无线移动节点组成；无线移动节点可以自由而动态地自组织成任意临时性“Ad Hoc”网络拓扑
- 允许人们和装置在没有预先存在的通信基础设施(如灾后重建环境)的环境中进行无缝地互连互通。

Ad hoc术语的来源

- Ad hoc来源于拉丁语—本意是“向这个”

英文名称：Ad hoc network, Self-organizing network, Infrastructureless network, Multi-hop network

- Ad hoc在英语中的含义是“for the specific purpose only”
- 1991年5月：IEEE正式采用“Ad hoc网络” — 一种特殊的自组织、对等式、多跳、无线移动网络

Ad hoc网络的发展历史

- 早在1972年，美国DARPA就启动了分组无线网项目PRNET（Packet Radio NETwork），研究在战场环境下利用分组无线网进行数据通信，但是不能支持大型网络环境的需要。
- 1983年，启动了高残存性自适应网络项目SURAN（SURvivable Adaptive Network），研究如何将无线分组网技术用于支持更大规模的网络，开发了能够适应战场快速变化的自适应网络协议。
- SURAN计划的三个具体的目标：

开发出符合分组无线网络协议的产品

开发并验证适合上万个结点的组网方法

开发并验证存复杂电子干扰条件下可生存的分组无线网络技术

Ad hoc网络的发展历史

GloMo计划

- 1994年： DARPA又启动了全球移动信息系统GloMo（Globle Mobile Information Systems）计划项目，并一直研究至今。
- 1996年—2000年WINGs研究项目

无线自适应移动信息系统WAMIS —多跳、移动环境下支持实时多媒体业务的高速分组无线网络

主要目标：如何将无线移动自组网与Internet无缝地连接起来

Ad hoc网络的发展历史

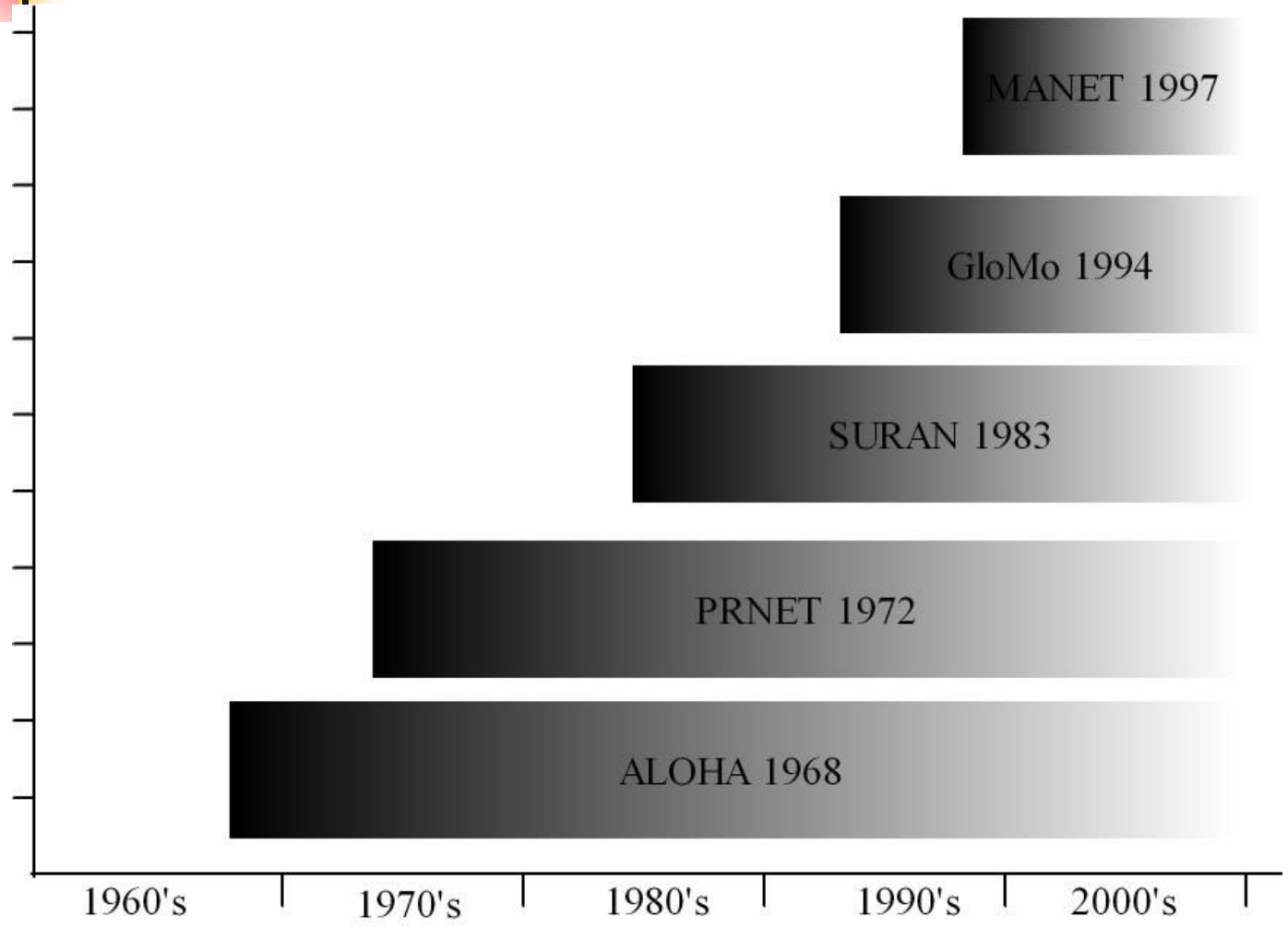
- 成立于1991年的IEEE 802.11标准委员会采用了“Ad hoc网络”一词来描叙这种网络，自组织、对等式、多跳无线移动通信网络，Ad hoc网络就此诞生。
- Internet工作组：

  IETF1997年成立 MANET 工作组（mobile ad hoc network）

  利用多跳无线网构造基于IP的移动互联网

  IRTF在2003成立了ANS 研究组（Ad Hoc Networks Scalability）

Ad hoc网络的发展历史



移动 ad hoc网络（MANET）

移动Ad hoc网络/多跳无线网络

- 由一组带有无线通信收发装置的移动终端节点组成
- 网络中每个移动终端自由移动
- 网络中所有移动终端地位相等
- 可以在任何时候、任何地点快速构建
- 不需要现有信息基础网络设施的支持
- 是一个多跳、临时、无中心网络。

MANET网络特点1

具有移动通信和计算机网路的特点

- 移动通信和计算机网络相结合
  - 报文交换采用分组交换机制
  - 移动终端是配有无线收发设备的移动便携式终端
- 移动终端兼并双重角色
  - 作为主机要运行面向用户的应用程序
  - 作为路由器要运行相应的路由协议
- 终端之间通过多个中间节点完成转发

MANET网络特点2

网络拓扑动态变化

- 用户终端随意移动
- 移动节点的开机/关机
- 无线电发送功率变化
- 无线信道间的相互干扰
- 地形等综合因素的影响

MANET网络特点3

无中心网络的自组性

- 无控制中心
- 每个节点地位平等
- 节点随时加入/离开网络
- 任何节点故障不会影响整个网络
- 具有更强鲁棒性和抗毁性

MANET网络特点4

多跳组网方式

- 接收端和发送端可使用比两者直接通信小的多的功率进行通信->大大节约能量的消耗
- 中间节点参与分组转发->能有效降低对无线传输设备的设计难度和成本，同时扩大自组网络覆盖范围

MANET网络特点5

有限的传输带宽

- 无线信道提供的带宽比有线信道要低得多
- 竞争共享无线信道会产生碰撞
- 信号衰弱、噪声干扰以及信号之间的干扰等

移动终端的自主性

- 自组网络的移动终端之间存在某种协同工作关系
- 每个终端都将承担为其他终端进行分组转发的义务

MANET网络特点6

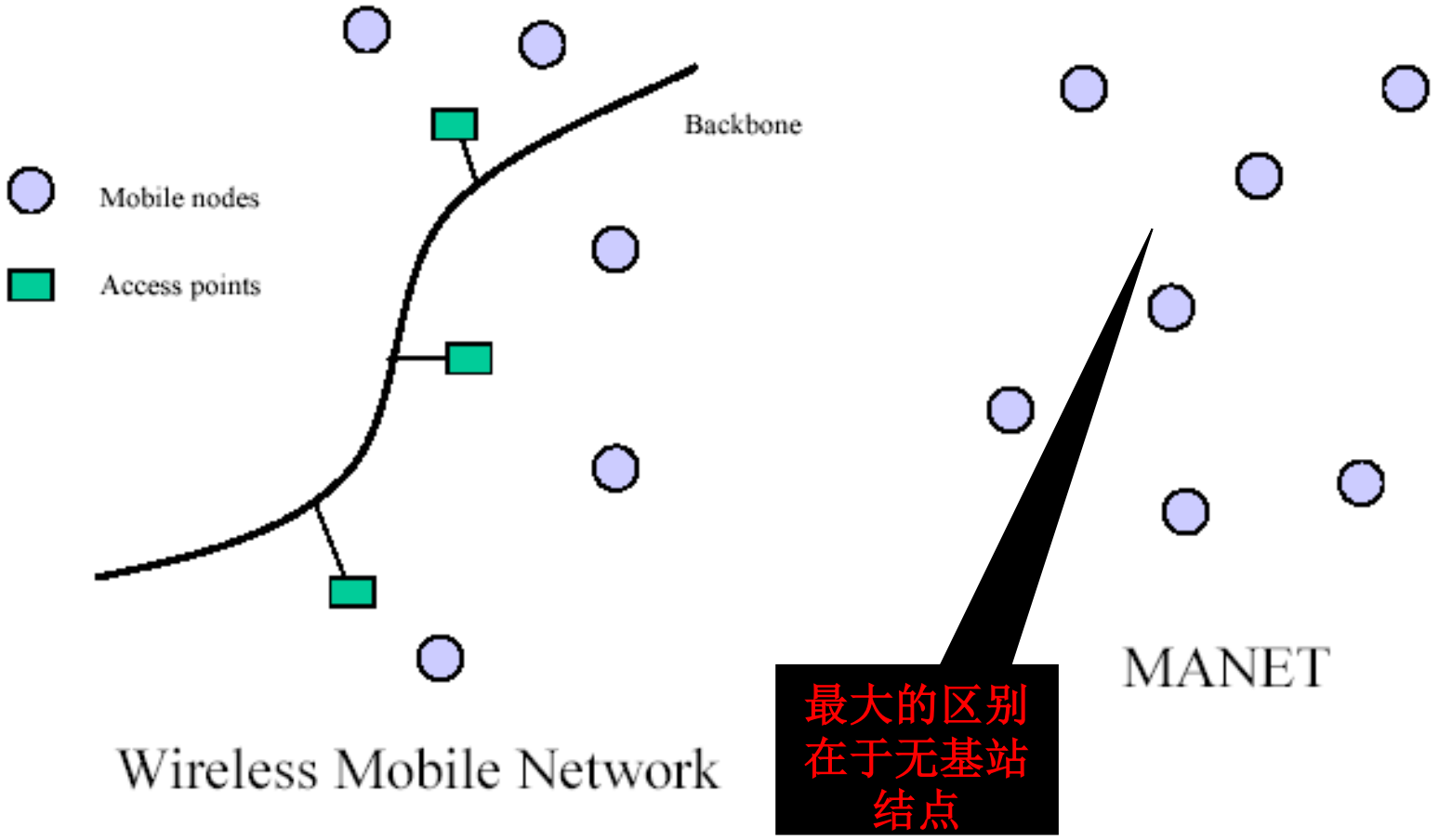
安全性差

- 无线链路使网络容易受到链路层攻击
- 节点漫游时缺乏物理保护
- 移动性使节点之间的信任关系经常变化

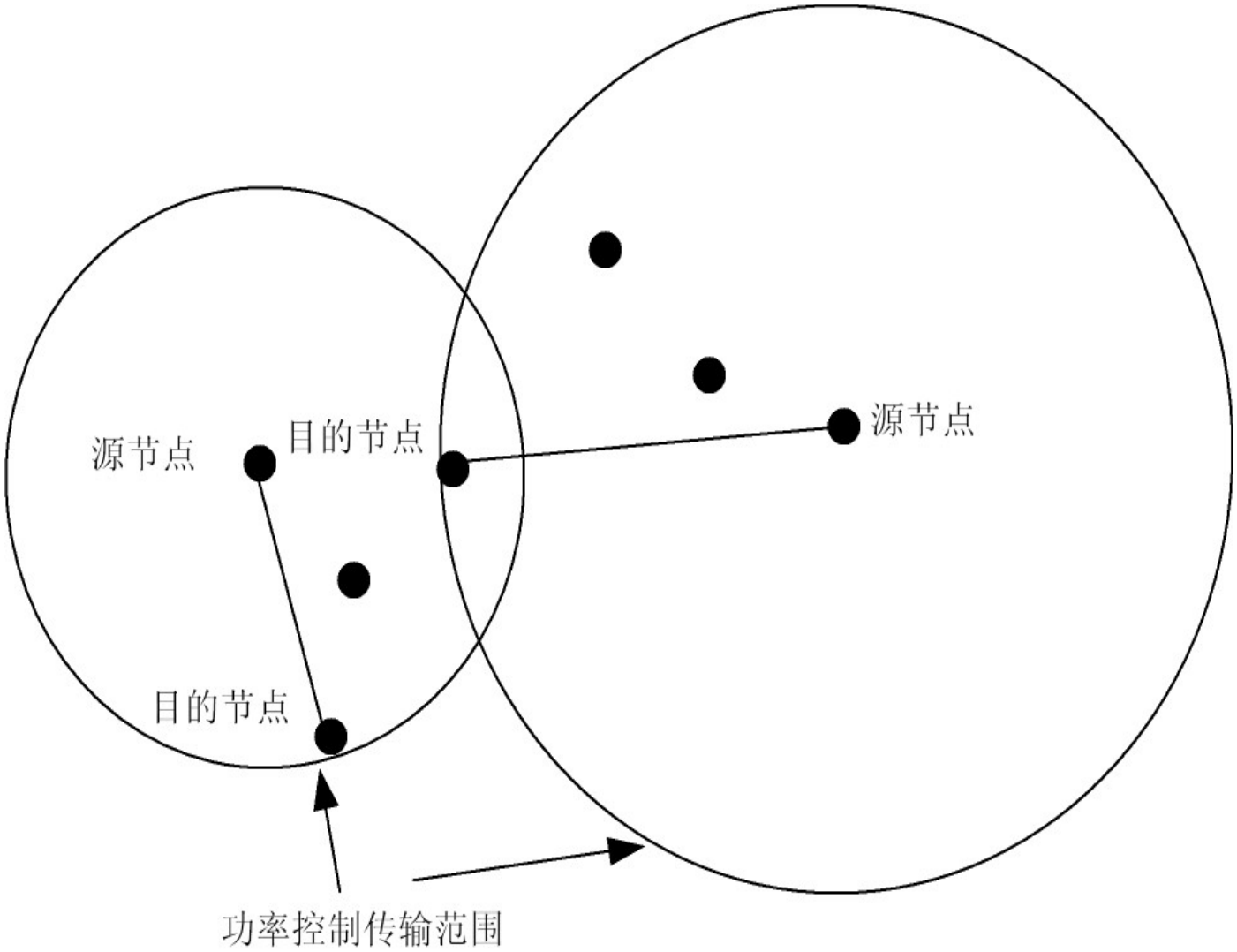
存在单向信道

- 无线终端发射功率的不同以及地形因素的影响

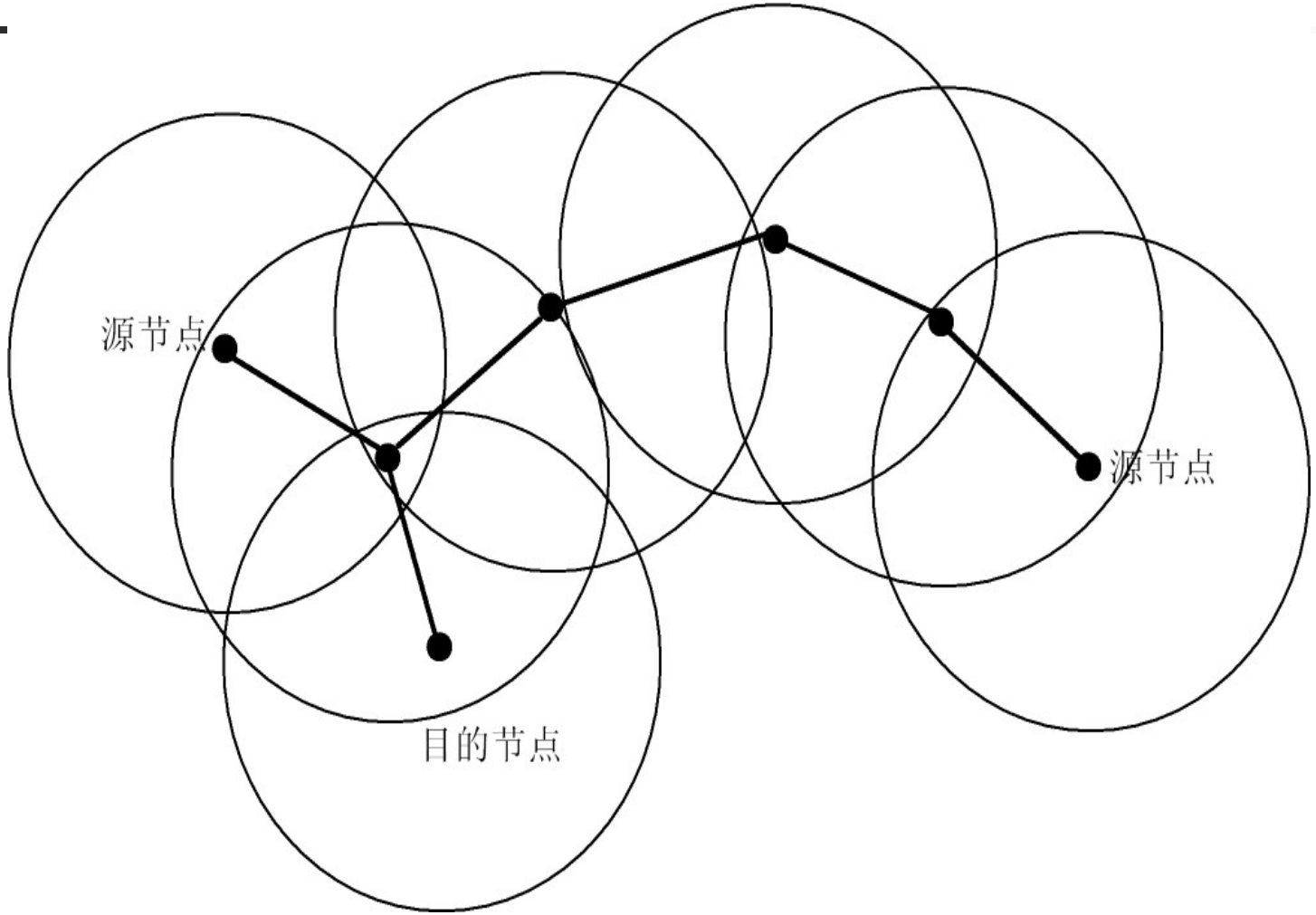
*Ad hoc*网络与常用无线网络比较



单跳Ad Hoc通信的一个例子



多跳Ad Hoc通信的一个例子



多跳网络好于单跳网络的原因

(1) 增强了网络的扩展性；

(2) 减少了干扰；

(3) 提高了整个网络的吞吐量；

(4) 降低了应用所关心的时延；

(5) 降低了数据传输中的能量消耗。

MANET与其他无线网络

- 与分组无线网、无线局域网、红外网络比较
  - 单跳与多跳

WLAN、红外网络都是单跳网络，不存在路由问题

  - 研究重点不同

主要研究内容是在网络的物理层和DL

Ad hoc网络的研究内容主要以路由协议为核心的网络层设计

  - 通信模式不同

移动终端的所有通信都要经过接入点进行

ad hoc移动终端的通信是对等的

MANET面临问题

- 特殊的信道共享方式
  - 共享信道
  - “隐藏终端”/“暴露终端”

- RTS/CTS
- MACAW
- DBTMA
- PAMAS

- 动态变化网络拓扑
  - 常规路由协议花较高代价（带宽、能源、CPU等）获得的路由信息可能已经陈旧

- 有限的无线传输带宽
  - 减少节点之间交换的信息量
  - 减少控制信息带来的附加开销

MANET面临问题

- 节能问题
  - 功率控制
  - 电池供电

- MTPR
- MBCR
- MMBCR
- CMMBCR

- 安全问题
  - 无线信道更容易受到各种攻击
  - 缺乏物理保护使得攻击可能来自内部
  - 移动性使得节点之间的信任关系不断变化
  - 安全策略应具有可扩展性

Ad hoc网络的应用

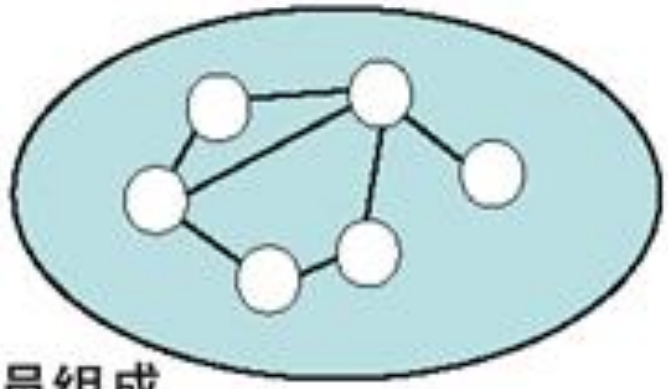
- 军事应用：因其特有的无需架设网络设施、快速、抗毁性强等特点，已经成为战术互联网的核心技术。美军研制了大量的无线自组织网络设备，用于单兵、车载、指挥所等不同的场合，并大量装备部队。
- 紧急和突发场合：在发生了地震、水灾、火灾灾难后，能够在这些恶劣和特殊的环境下提供通信支持。
- 偏远野外地区：无法依赖固定或预设的网络设施进行通信。
- 临时场合：Ad hoc网络的快速、简单组网能力使得它可以用于临时场合的通信。比如会议、庆典、展览等场合，可以免去布线和部署网络设备的工作。
- 动态场合和分布式系统：通过无线连接远端的设备、传感节点和激励器，可方便用于分布式控制，特别适合于调度和协调远端设备的工作，自动高速公路系统（AHS）中协调和控制车辆，对工业处理过程进行远程控制等。

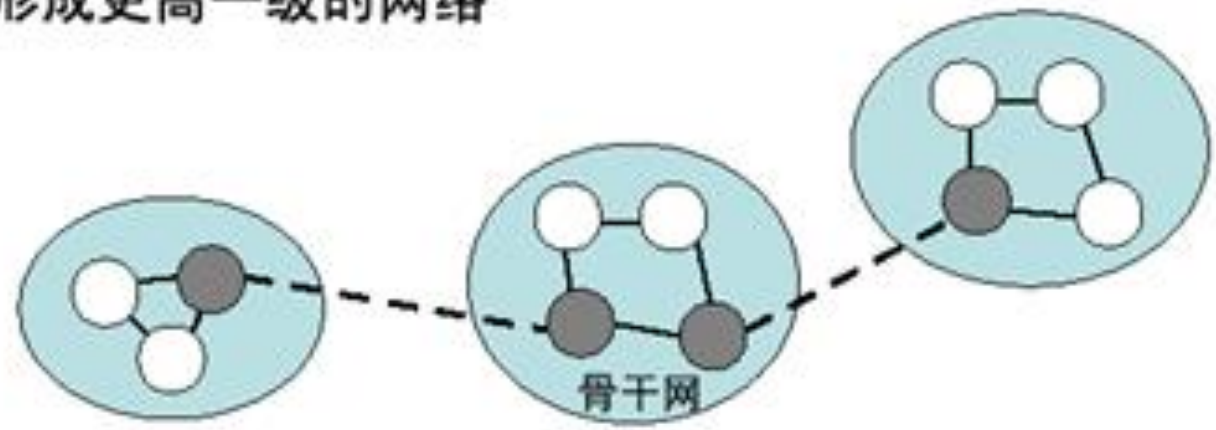
Ad hoc网络的应用

- 个人局域网：用于实现PDA、手机、掌上电脑等个人电子通信设备之间的通信，并可以构建虚拟教室和讨论组等崭新的移动对等应用。
- 传感器网络：应用的另一大领域。具有非常广阔的应用前景。
- 商业应用：组建家庭无线网络、无线数据网络、移动医疗监护系统和无线设备网络，开展移动和可携带计算以及无所不在的通信业务等。
- 其它应用：比如它可以用来扩展现有蜂窝移动通信系统的覆盖范围，实现地铁和隧道等场合的无线覆盖，实现汽车和飞机等交通工具之间的通信，用于辅助教学和构建未来的移动无线城域网和自组织广域网等。
- Ad hoc网络如何接入现有的Internet也是近年研究的一个热点。

2、Ad hoc网络的体系结构

- 平面结构（完全分布式）
  - 所有节点的地位平等
- 层次结构（分层分布式）
  - 网络被划分为簇（cluster）
  - 每个簇由一个簇头和多个簇成员组成
  - 簇头可形成更高一级的网络

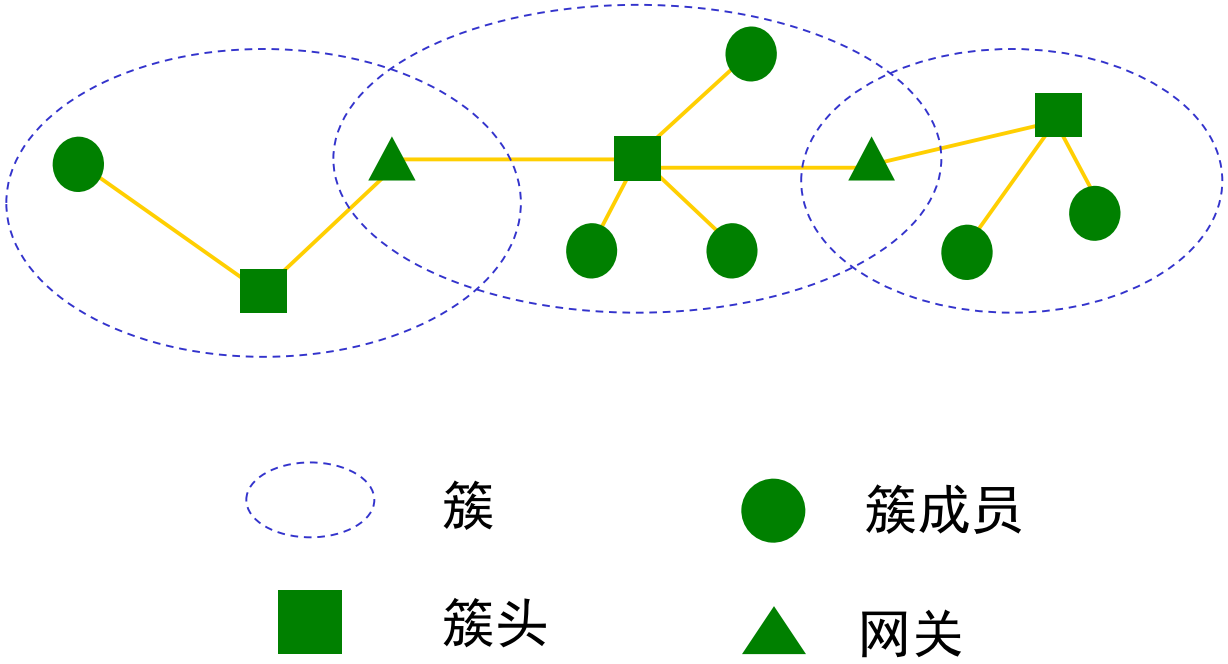




Ad hoc网络的分级结构

- 在一般应用中，平面结构或分级结构均可采用，但是在网络规模较大并需要提供一定的QoS支持时，通常需要采用分级结构。
- 根据不同的硬件配置，分级结构又可以分为单频分级和多频分级两种。
- 在单频分级网络中，所有节点使用同一个频率进行通信，簇头之间的通信需要网关支持，簇头和网关／无线网关节点形成高一级的网络，称为虚拟骨干网络(VBN)。
- 而在多频分级网络中，不同级采用不同的频率进行通信。低级节点的通信范围较小，而高级节点的通信范围较大。高级的节点常常处于多个级中，因而使用多个频率以实现与不同级的节点进行通信。

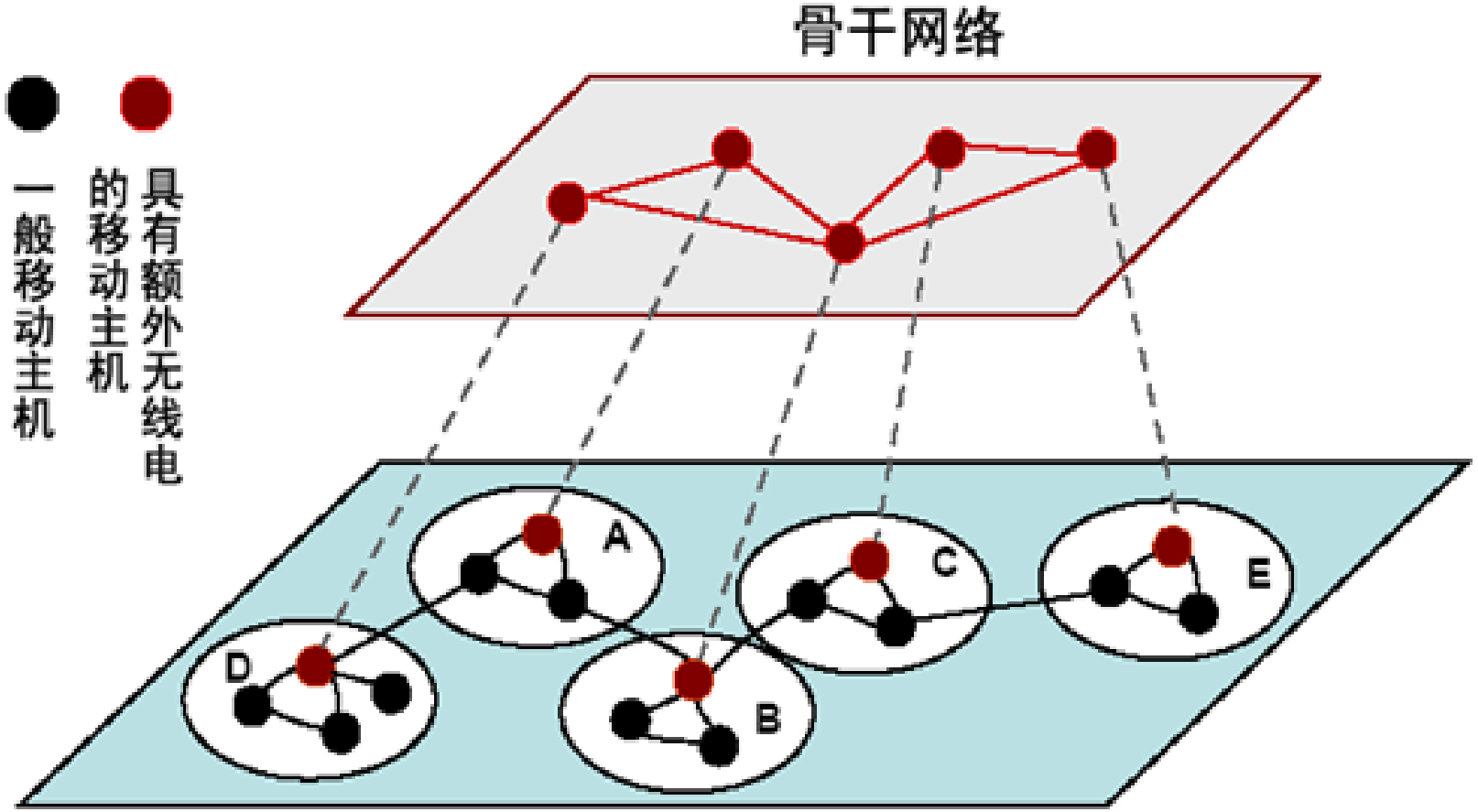
Ad hoc网络的结构-单频分级



单频分级

Ad hoc网络的结构-多频分级

- 使用多频的两级结构



Ad hoc网络中的分簇算法

- Ad hoc网络中分簇的概念很早就提出了，但是早期主要用于构造分组无线网中的分级路由，目的是减少控制开销。迄今为止已经提出了大量的分簇算法。
- 基于分簇网络结构，可以减少路由算法和洪泛广播的开销，能够方便地管理移动节点和控制节点接入无线信道，并可以提高网络的可扩展性和QoS保障能力。
- 分簇算法的选择依赖于应用的需求、网络的环境和节点的特征。不同的分簇算法具有不同的优化目标，包括最小化簇计算和维护开销、最小化簇头、最大化簇稳定性和最大化节点生存时间等。

平面结构的优缺点

- 优点

  简单：所有节点能力相同
  健壮：只要存在多条路径就可以通信
  相对安全

- 缺点

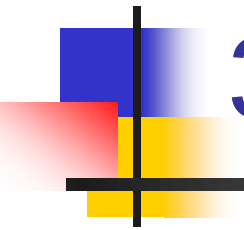
  路由开销大：节点数目多移动性强的环境下，维持网络最新拓扑的控制开销大

  可扩充性差

层次结构的优缺点

- 优点
  - Cluster成员功能简单
  - 路由信息局部化：减少路由协议开销
  - 节点定位简单
  - 可扩展性好
  - 抗毁性好

- 缺点
  - 簇头需要选择
  - 所有传输都要通过簇
  - 簇头是瓶颈
  - 经过簇头的路由不一定最佳



3 移动Ad hoc网络MAC协议

设计特殊性

- 由于Ad hoc网络应用环境等因素的特殊性，是无法采用基于固定的或有中心的网络协议的，以往在蜂窝移动通信系统中所使用的有中心的信道接入技术和传统的基于共享广播信道的信道接入技术无法直接应用，需要专门设计特定的信道接入协议。
- Ad hoc网络协议栈中，信道接入协议运行在物理层之上，负责协调网络中各节点对无线信道的接入，从而完成相邻节点的数据转发，是所有报文在无线信道上发送和接收的直接控制者，它的性能好坏直接关系到信道的利用率和整个网络的性能。

设计准则

- 高空间复用度。可以实现多对结点同时通信，实现频率的空间复用。信道接入协议应该尽量增加这种复用度，使网络中更多的节点可以同时进行通信，从而提高网络的总吞吐量。
- 避免报文间的冲突。由于特殊的信道共享方式，Ad hoc网络的信道接入协议将面临报文冲突的威胁。
- 提供冲突解决的方法。完全实现报文的无冲突发送是一种理想状态，当冲突无法避免时，协议应提供有效的冲突解决方法，尽量减小其带来的影响。

MAC层需要解决的主要问题

- 多跳信道共享方式
- 隐藏终端问题
- 暴露终端问题
- 节点移动的影响

多跳共享信道

- 虽然ad-hoc网络的无线信道也是一个共享的广播信道，但它不是一跳共享。在ad-hoc网络中，当一个节点发送报文，只有在它覆盖范围内的节点（邻居）才能够收到，而覆盖范围意外的节点感知不到任何通信的存在。
- 这恰恰也是ad-hoc网络的优势所在，即发送节点覆盖范围意外的节点不受发送节点的影响，他们也可以同时发送报文，这可以大大提高频率的空间复用度。
- 多跳共享广播信道会带来隐藏终端、暴露终端等一系列问题

隐藏终端和暴露终端

- 隐藏终端是指在接收节点的覆盖区而在发送节点覆盖范围外的节点。隐藏终端因听不到发送节点的发送而项同样的接收节点发送分组，造成分组在接收节点处冲突。隐藏终端可分为隐发送终端和隐接收终端
- 暴露终端是指在发送节点覆盖范围内，而在接收节点覆盖范围之外的节点。暴露终端因能听到发送节点的发送而可能延迟发送。但因为他在接收节点的通信范围之外，他的发送实际上不会造成冲突，引入了不必要的延迟。暴露终端也可分为暴露发送终端和暴露接收终端

MAC协议分类

- 竞争协议：使用直接竞争来决定信道访问权，并且通过随机重传来解决碰撞问题

  ALOHA，CSMA及其衍生版

- 同步分配协议:基于同步通信模式，采用某种传输时间安排算法决定每个节点访问信道的时隙。

  静态分配，动态分配

- 异步分配协议:基于异步通信模式，采用某种传输时间安排算法决定每个节点访问信道的时隙。

  协议序列、冲突避免码

- 混合协议：以上协议的综合。

竞争类MAC协议

- **MACA（Multiple Access Collision Avoidance）**
  - MACA是第一个采用了RTS/CTS信道握手机制来解决ad-hoc网络中隐藏终端和暴露终端问题的MAC协议，采用的是CSMA/CA，利用RTS和CTS进行交换，完成对共享信道的检测。不采用ACK。
  - 周围站点只有听到CTS才保持安静。
  - 部分解决了隐藏终端和暴露终端问题。

- **MACAW（MACA for Wireless）**
  - 放弃了原来针对以太网的退避算法，采用乘法增加线性减少退避算法（MILD）和退避计数器复制等技术来实现公平接入。
  - 应用载波侦听避免RTS之间的碰撞。
  - MACAW采用RTS-CTS-DATA-ACK握手机制。
  - 周围站点只有听到CTS才保持安静。
  - 为了防止ACK的碰撞，源节点发送DS控制分组提醒暴露终端保持静默。

竞争类MAC协议

- **IEEE802.11 DCF（Distributed Coordination Function）**

  IEEE802.11 DCF源于CSMA/CA，对CSMA/CA进行了扩展，加入了ACK控制分组来实现链路层的确认。IEEE802.11保留了CSMA/CA的载波监听机制，采用分组交互顺序是RTS-CTS-DATA-ACK。当数据分组较短时，也可以直接采用DATA-ACK的分组交互顺序。IEEE802.11 DCF核心是CSMA/CA信道共享技术，主要包含两方面内容：载波检测机制和随机退避。

- **FAMA（Floor Acquisition Multiple Access）**

  — FAMA是对MACA和MACAW做的进一步改进。他通过延长RTS和CTS控制报文的长度来消除隐藏终端的影响。

  — FAMA还允许一旦RTS-CTS交互成功，节点可发送多个报文，从而增加了网络的吞吐量。FAMA是基于单信道的ad-hoc网络信道接入协议中较成功的一种。

竞争类MAC协议

- **DBTMA（双忙音多点接入协议）**

  —使用控制信道上的RTS/CTS分组外，增加两个频带彼此分开的窄带忙音BTr(接收忙音)和BTt(发送忙音)，范别用来指示某站正在数据信道上接收和发送数据。相比MACA和MACAW算法，DBTMA完全解决了隐藏终端和暴露终端问题。

  —DBTMA协议采用的是忙音窄带信号，需要增加额外的硬件设备，可以通过窄带滤波器和比较器来实现，并且通过引入忙音可以传送各种长度的分组数据。

- **PCMA（功率控制的多点接入协议）**

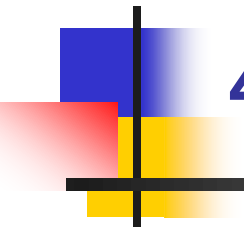
  —提出了利用功率控制的多点接入的机制来避免冲突。CSMA/CA的MAC协议避免冲突的方式是一种“开/关”模式，也就是指节点按估计的功率发送或停止发送。PCMA将这种“开/关”模式变为有约束的可调功率模式，在一定的功率限制范围内动态地调节传输功率。因此，实现这种模式的核心就是正确估计传输功率可调整的范围，保证对新的传输的建立，既不会干扰正在进行的传输，又可以尽可能地限制传输所占的区域。

- **PAMAS**

  目标是在解决信道接入问题的基础上尽量节约能源。PAMAS关闭电台的策略如下：如果节点没有数据发送，当他的某个邻居节点发送数据时，他应关闭发射机；如果他的一个邻居节在发送，另一个邻居在接收，他应关闭电台，因此此时他既不能发送也不能接收，关闭电台的时间由接收的RTS中携带的数据长度来决定。

基于多信道MAC协议

- 基于多信道的ad-hoc网络信道接入协议用于具有多个信道的ad-hoc网络。由于网络中具有多个信道，相邻节点可以使用不同的信道同时进行通信，接入控制更加灵活。
- 主要问题：信道分配和接入控制
- 信道分配负责为不同的通信节点分配响应的信道，消除数据分组的冲突，使尽量多的节点可以同时进行通信
- 接入控制负责确定节点接入信道的时机、冲突的避免和解决等问题

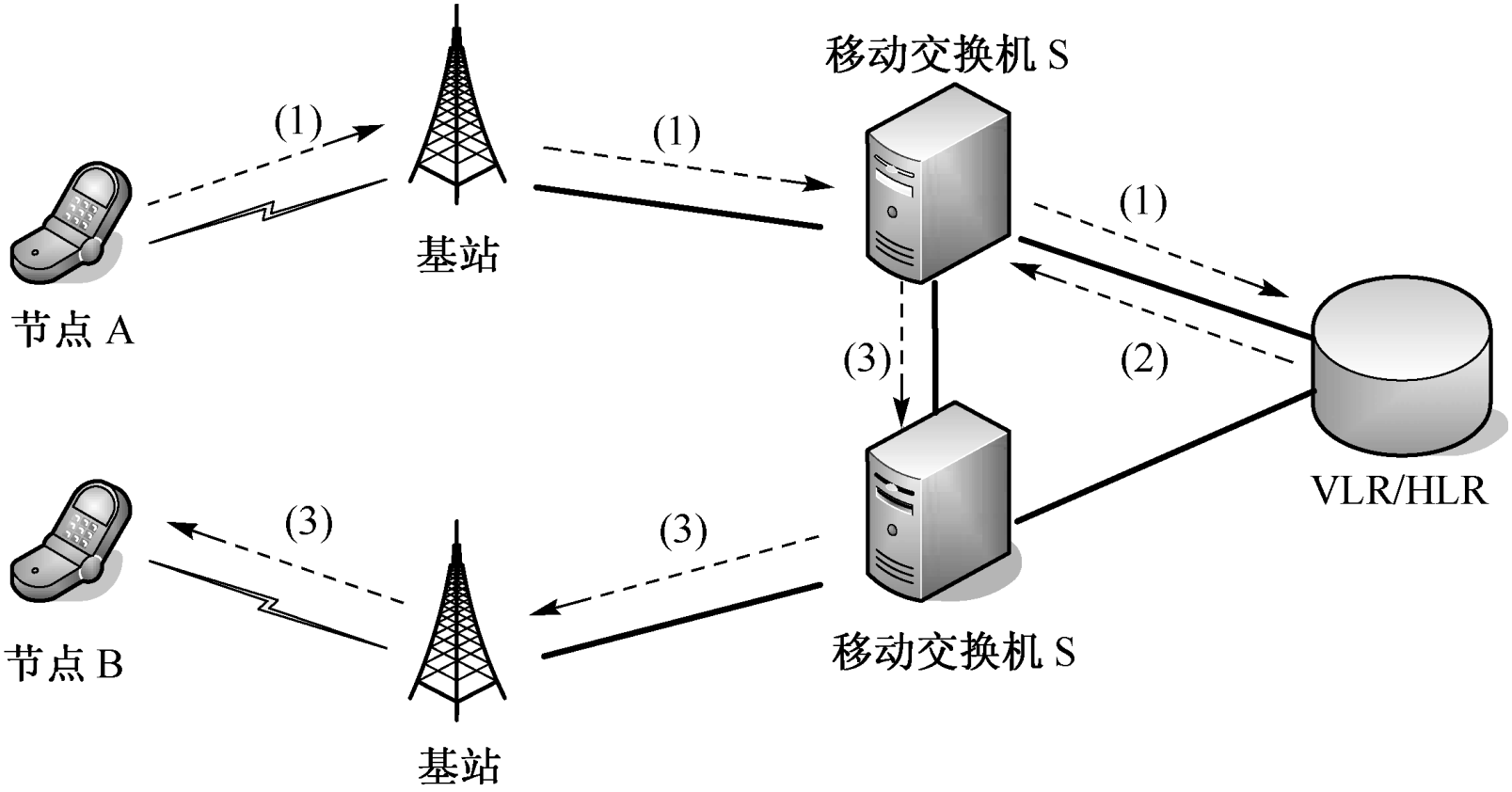


4 移动Ad hoc网络路由技术

为什么需要新的路由协议？

- 传统的路由解决方案都是假定网络拓扑结构是相对稳定的，移动Ad hoc网络的拓扑是不断变化的；
- 传统的路由方案依赖于保存在某些网络节点或特定管理节点中的分布式路由数据库，而Ad Hoc网络节点不可能永久存储路由信息，而且它们存储的信息也并不是一直真实可靠的；
- 常规路由协议不是为高移动性和低带宽网络设计的；
- DV算法存在“无穷计算”问题和慢收敛；
- 采用泛洪技术的（链路状态）协议造成额外的通信和控制开销；
- 常规路由协议周期性地路由更新消耗大量的网络带宽和节点能源；
- 无线终端功率的差异以及无线信道的干扰导致单向信道的存在。

蜂窝移动通信系统路由示意图

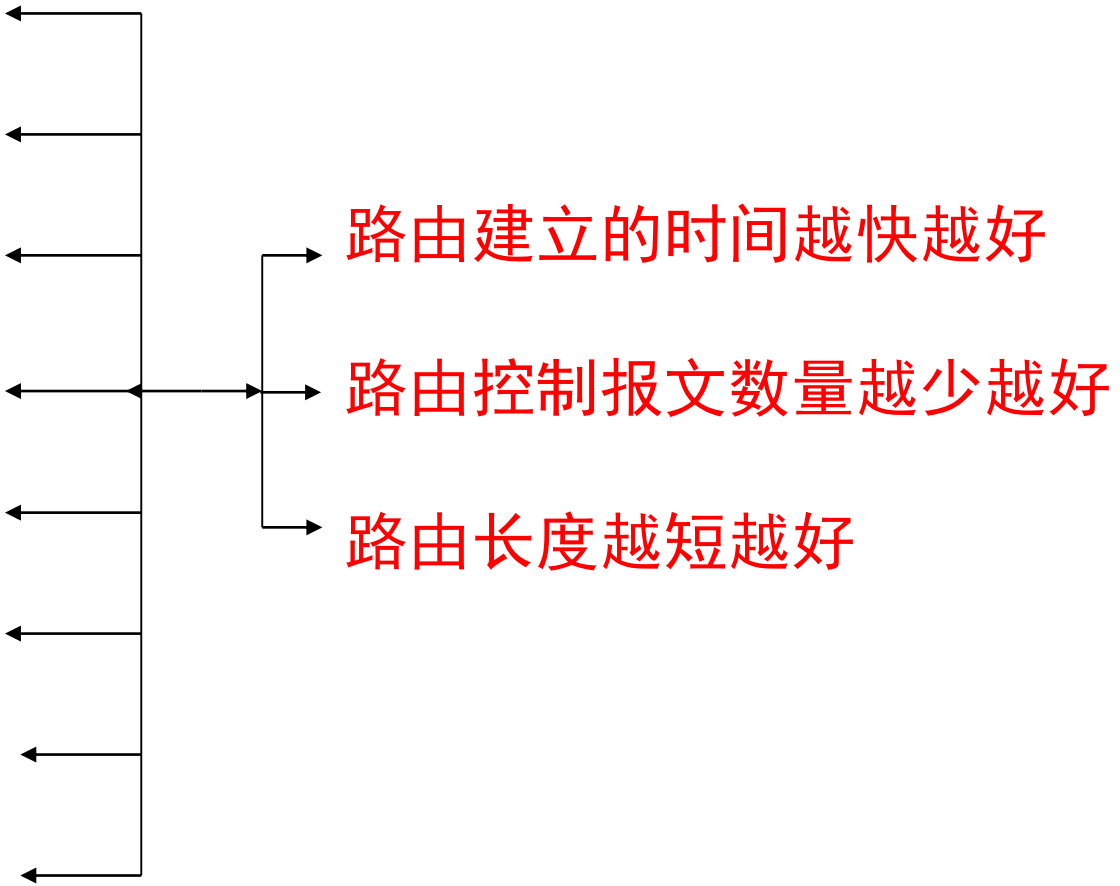


Ad hoc网络与蜂窝移动通信系统的区别

- 当移动节点A呼叫移动节点B时，节点A并不知道节点B的具体位置，而是通过网络中的基站和交换机等中间设施来建立到节点B的路由。由此不难看出，固定网络设备(交换机、VLR/HLR等)是路由选择及建立的实施者，基站主要完成信号的发送和接收。而在Ad hoc网络中，是不存在上述固定设备的，路由选择只能由移动节点自身完成 。
- 同时，在蜂窝移动通信系统中，网络结构总体而言比较稳定。而在Ad hoc网络环境下，网络拓扑结构发生经常性的变化，网络拓扑的频繁变化极大地影响着路由的选择。

Ad hoc网络对路由协议的要求

- 分布式操作
- 提供无环路由
- 维护多条路由
- 提供节能策略
- 提供安全机制
- 支持单向链路
- 提供QoS支持
- 支持组播功能



Ad hoc网络路由协议的分类

- 自20世纪70年代美军DARPA资助研究的分组无线网项目开展以来，国内外的许多研究人员从不同的角度提出了一系列的Ad hoc网络路由协议。
- 根据发现路由的驱动模式的不同，可分为表驱动路由协议和按需路由协议。
- 根据网络拓扑结构的差异，又可以将它们分为平面结构的路由协议和分簇路由协议。

表驱动路由

先验式(proactive)路由

- 传统的分布式最短路径路由协议
  - — 链路状态或者距离向量
  - — 所有节点连续更新“可达”信息
- 每个节点维护到网络中所有节点的路由
- 所有路由都已经存在并且随时可用
- 路由请求延时低
- 路由开销高

表驱动路由协议特点

- 初期，主要是修改有线网络路由协议以适应Ad hoc网络环境，大多属于表驱动路由协议。
- 表驱动路由协议的路由查找策略与传统路由协议类似，节点通过周期性广播路由信息报文，交换路由信息，主动发现路由；同时，节点须维护去往网络中所有节点路由。
- 优点：当节点需要发送数据报文时，只要去往目标节点的路由存在，所需的延时很小；
- 缺点：需要花费较大开销，尽可能使得路由更新能够紧随当前拓扑结构的变化。然而，动态变化拓扑结构可能使得路由更新变成过时信息，路由协议始终处于不收敛状态。
- 主要的表驱动路由协议：DV、DBF (Distributed Bellman-Ford)、DSDV (Destination-Sequenced Distance-Vector Routing)、WRP (Wireless Routing Protocol)。

按需(on-demand)路由协议

反应式(reactive)路由

- 在源端需要时通过路由发现过程来确定路由
  - — 控制信息采用泛洪方式
  - — 路由请求延时高
  - — 路由开销低
- 两种实现技术
  - — 源路由（报文头携带完整的路由信息）
  - — 逐跳路由（类似于现有的Internet路由）

按需路由协议的特点

- 根据发送节点的需求进行路由发现过程，网络拓扑结构和路由表内容也按需建立（只是整个网络拓扑结构的一部分）。
- 对建立路由进行维护，直到路由中断或不再需要。
- 优点：不需周期性广播路由信息，节省网络资源。
- 缺点：发送分组时，必须临时启动路由发现过程来寻找路由，因而延迟大
- 主要路由协议：

DSR (Dynamic Source Routing), AODV (Ad Hoc on Demand Distance Vector Routing),TORA (Temporally Ordered Routing Algorithm)

两种路由机制的权衡

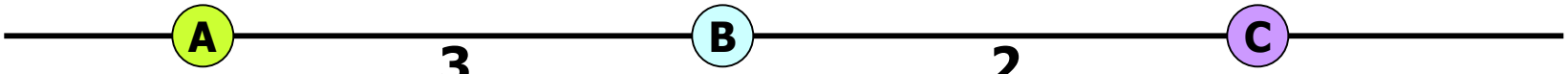
- 路由发现的延迟
  - —主动路由因全程维护所有的路由而具备低延迟
  - —按需路由因只在需要时才发现所需路由而导致高延迟
- 路由发现/维护的开销
  - —按需路由因只在需要时才维护路由而具备低开销
  - —主动路由因连续更新路由可能导致高开销
- 哪种途径表现更好取决于流量和移动模式
  - —对于节点移动性低，网络流量高的网络中，主动路由协议性能较好
  - —在网络流量受限、节点移动性强的网络中按需路由协议更加适合。
  - —使用分级路由协议结合两种路由机制

DV算法概述

- 基于分布式Bellman-Ford算法
  寻找从源点到某个点的最短路径
- 每个节点都维护一张路由表
  —所有可达的目的地
  —到达目的地的下一跳
  —到达目的地的“距离”（开销）
- 节点向邻居节点发送路由更新消息
  —定期更新：即使节点路由表无变化
  —触发更新：节点路由表中某条路由发生变化
- 路由更新消息包含列表格式
  <目的地，开销>
- 节点在收到“更好”路由的情况下更新路由表
  —具有更小的开销：对于同一个目的地，来自不同的下一跳
  —更新开销：对于同一目的地，来自相同的下一跳

DV算法过程

- 初始化

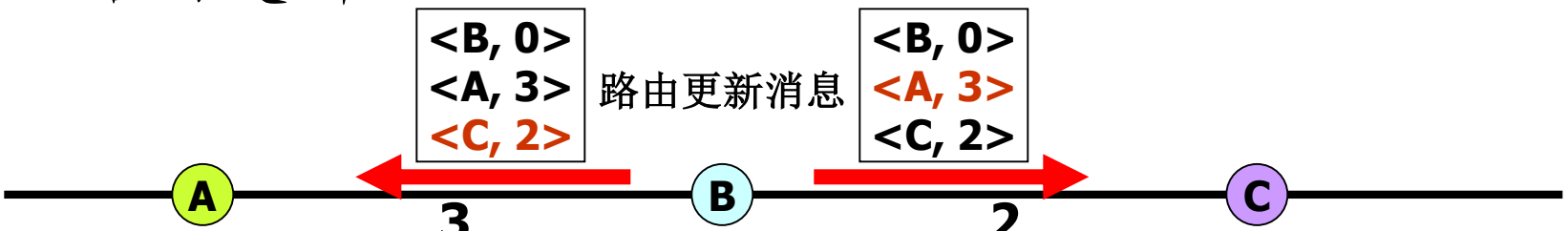


Dest.	Next	Metric
A	A	0
B	B	3
C	-	∞

Dest.	Next	Metric
B	B	0
A	A	3
C	C	2

Dest.	Next	Metric
C	C	0
B	B	2
A	-	∞

- 路由更新



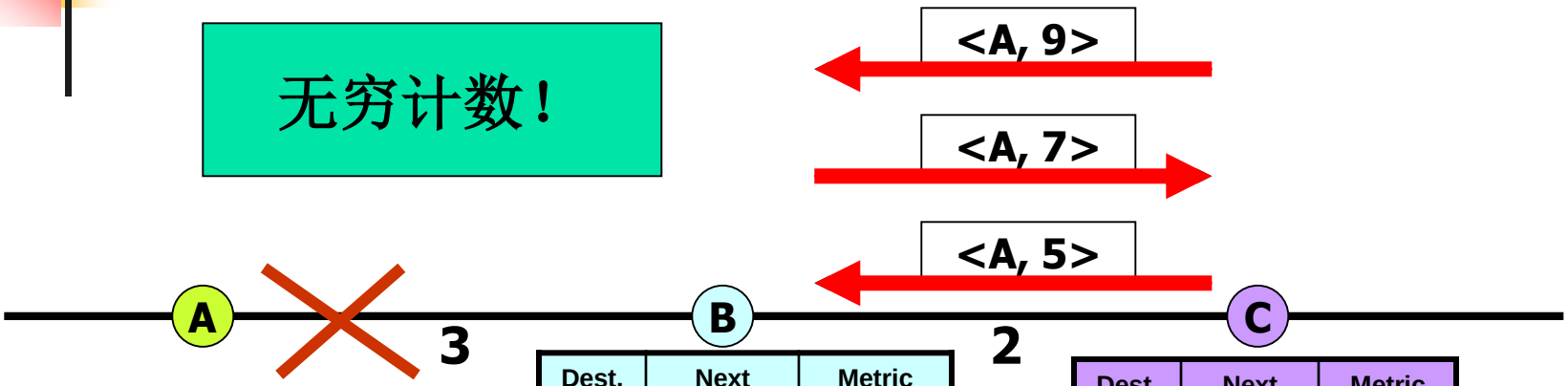
Dest.	Next	Metric
A	A	0
B	B	3
C	B	5

Dest.	Next	Metric
B	B	0
A	A	3
C	C	2

Dest.	Next	Metrict
C	C	0
B	B	2
A	B	5

DV算法中的计数到无穷问题

无穷计数！



Dest.	Next	Metric
B	B	0
A	A	3
C	C	2

Dest.	Next	Metric
B	B	0
A	A	∞
C	C	2

Dest.	Next	Metric
B	B	0
A	C	7
C	C	2

Dest.	Next	Metric
C	C	0
B	B	2
A	B	5

Dest.	Next	Metric
C	C	0
B	B	2
A	B	9

DSDV协议概述

- 基于DV算法
  - —简单，易于实现
  - —存储空间小（只须和邻居节点交换路由信息）
- 确保无路由回路

  路由表中的每个表项都带有目的地序列号（由目的节点生成）
- 对拓扑变化能作出快速反应
  - —路由表有显著变化时立即启动路由公告
  - —但是等待不稳定路由的公告，以减缓路由波动
- 先应式（表驱动）路由
  - —节点维护到所有目的地的路由信息
  - —路由信息必须周期性的更新（无休眠节点）
  - —即使网络拓扑无变化也存在着通信开销
  - —维护的路由可能从不使用

DSDV路由表

Dest.	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr-C
D	B	4	D-312	001200	Ptr_D

- 序列号（Sequence number ）
  由目的端产生，用来防止出现路由回路，并确保路由信息是最新的
  格式： Dest_NNN
- 加入时间（Install Time）
  路由表项的创建时间，用来删除过期表项
- Stable Data
  - 指向一个包含有路由稳定状态信息的表
    —目的节点地址
    —最近沉淀时间（last settling time）
    —平均沉淀时间（average settling time）
  - 用于缓解网络中的路由波动

对于同一个目的地，节点可能接收到来自其它节点的多条路由信息，settling time定义为第一条路由和最佳路由之间的时间间隔

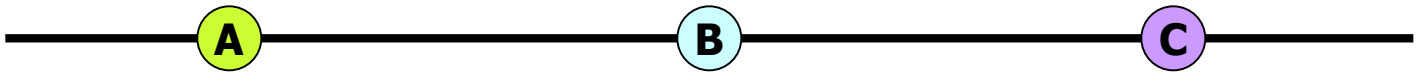
DSDV路由公告

- 向每个邻居公告自己的路由信息
  - —目的节点地址
  - — Metric：到目的节点的开销，一般为到目的节点的跳数
  - —目的地序列号
  - —其它信息（例如硬件地址等）
- 设置序列号信息的规则
  - —每次公告增加自己的目的地序列号（只用偶数值）
  - —如果一个节点不再可达（timeout）,则将该节点的序列号加1（奇数序列号），并且设置metric为∞

DSDV路由选择

- 将更新信息与自己的路由表比较
  - 选择具有更大目的地序列号的路由，这将保证始终使用来自目的地的最新信息
  - 当序列号相等时，选择具有更好metric的路由

DSDV协议操作：更新前路由表

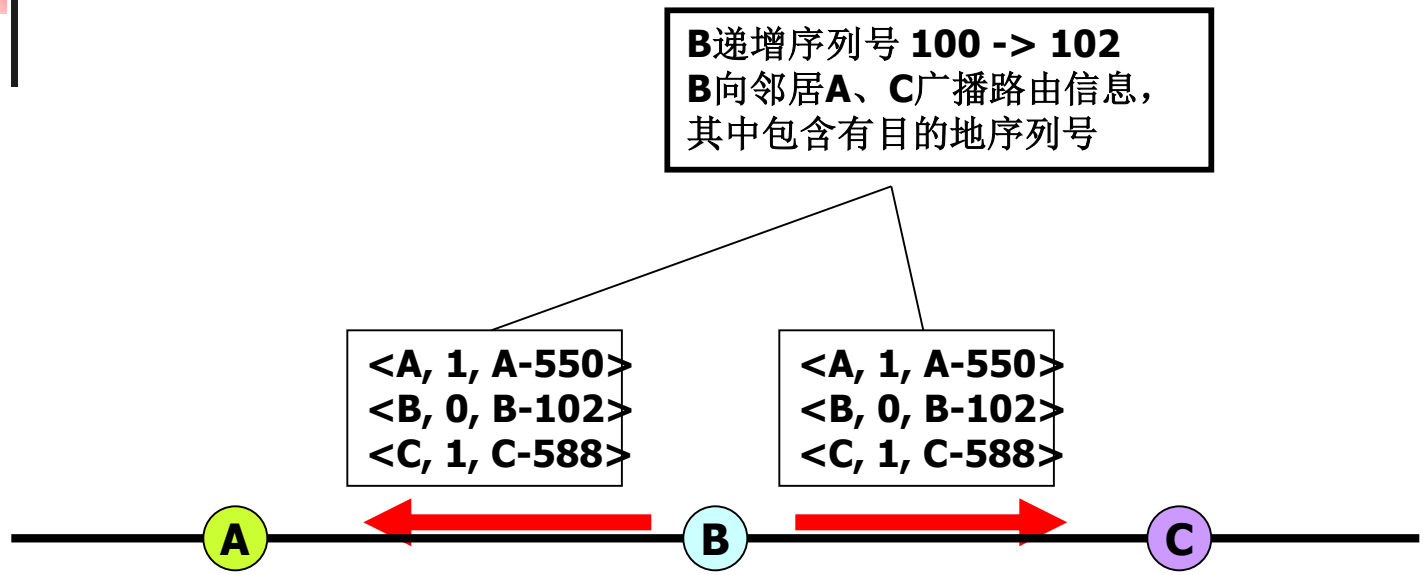


Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-100
C	C	0	C-588

DSDV协议操作：路由公告

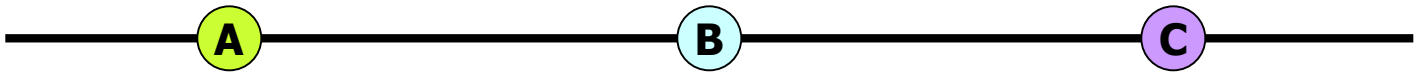


Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-100
C	C	0	C-588

DSDV协议操作：更新后路由表



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

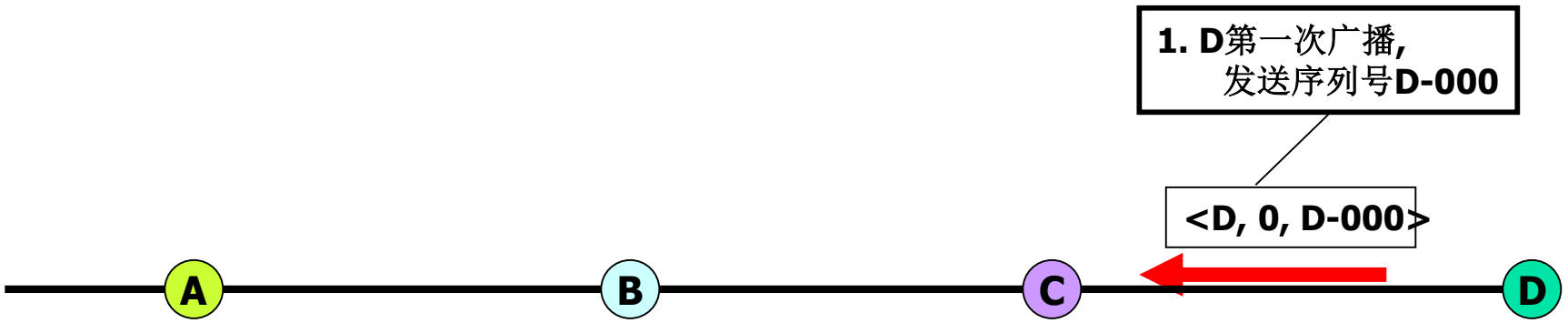
Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

对拓扑变化的反应

- 立即公告
  - 有关新路由、链路断开和metric变化的信息立即传递给邻居节点
- 完全/增量更新
  - 完全更新：发送自己路由表中的所有路由信息
  - 增量更新：只发送路由表中那些发生变化的表项（能包含在一个单独的分组中发送）

DSDV协议操作：新节点加入



Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590

DSDV协议操作：新节点加入

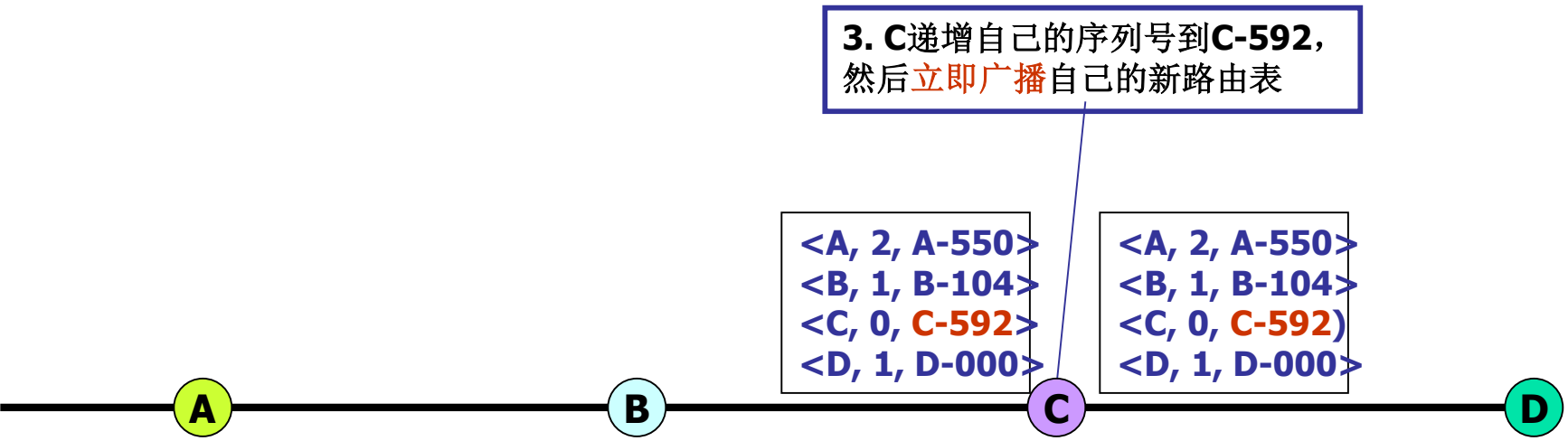
2. 插入到**D**的表项，
序列号为**D-000**

Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590
D	D	1	D-000

DSDV协议操作：新节点加入

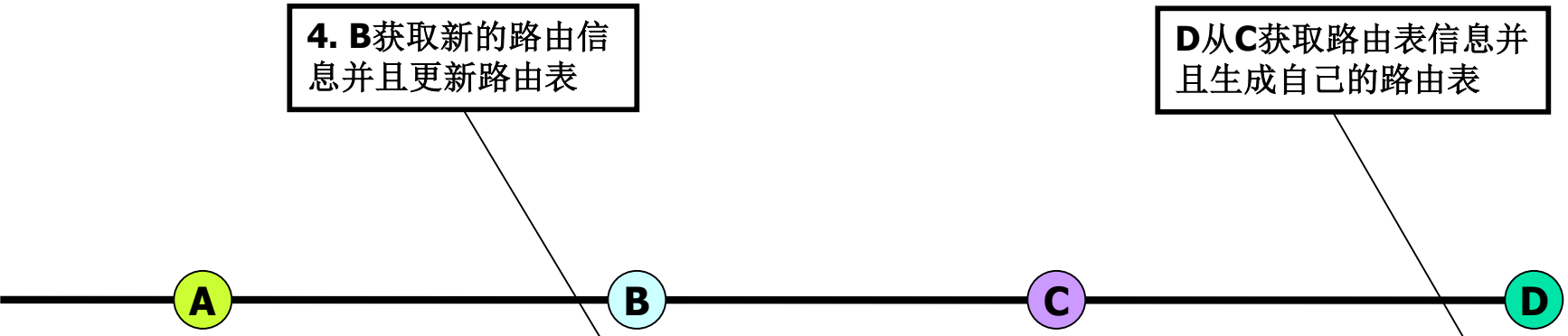


Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

DSDV协议操作：新节点加入



Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-592

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

Dest.	Next	Metric	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-000

DSDV协议操作：链路断开

1. C 检测到链路断开-〉序列号递增1 (当且仅当这种情况不是目的节点设置序列号-〉奇数序列号)

2. B广播到达D的路由信息

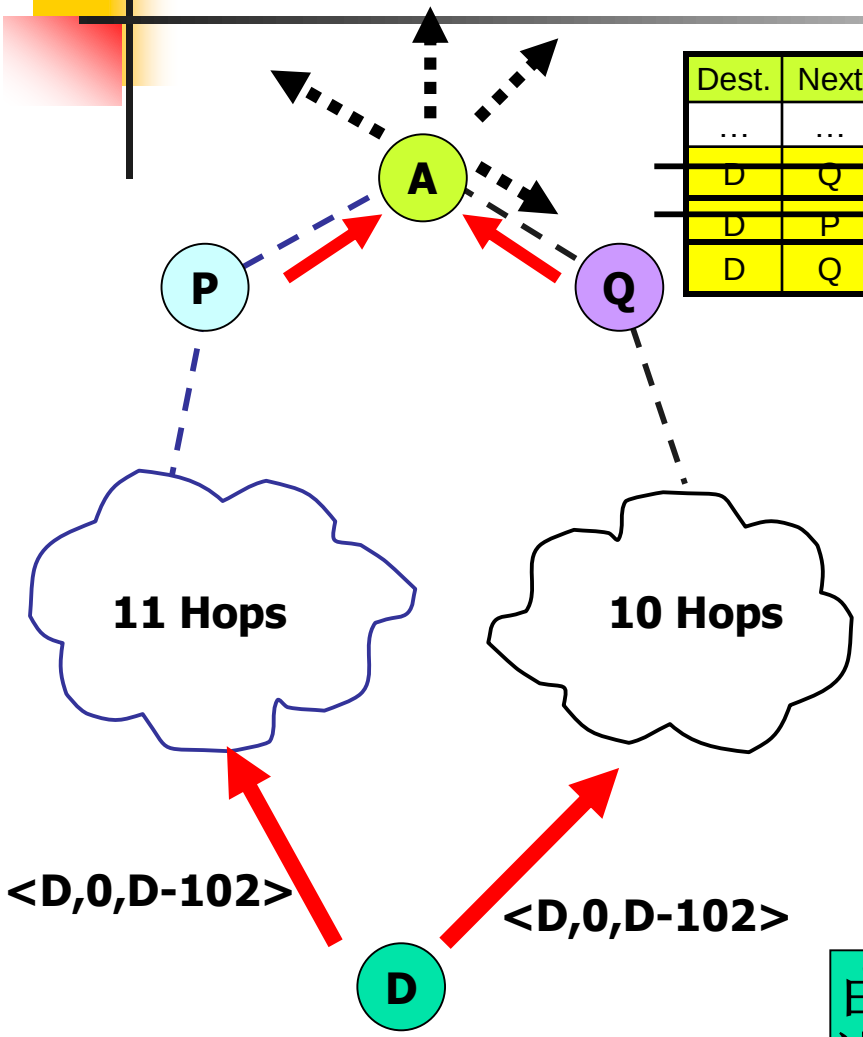
Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

Dest.	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~D~~	~~1~~	~~D-100~~
D	D	∞	D-101

因为B广播的到达D的路由信息中的序列号小于C维护的D的序列号，因此C认为B的广播的是过期路由信息，不予采纳 → 避免了循环 → 避免了计数到无穷

DSDV协议操作：路由波动



Dest.	Next	Metric	Seq.
…	…	…	
D	Q	14	D-100
D	P	15	D-102
D	Q	14	D-102

1. D公告序列号为D-102的路由

2. A收到来自P的路由更新消息<D, 15, D-102>

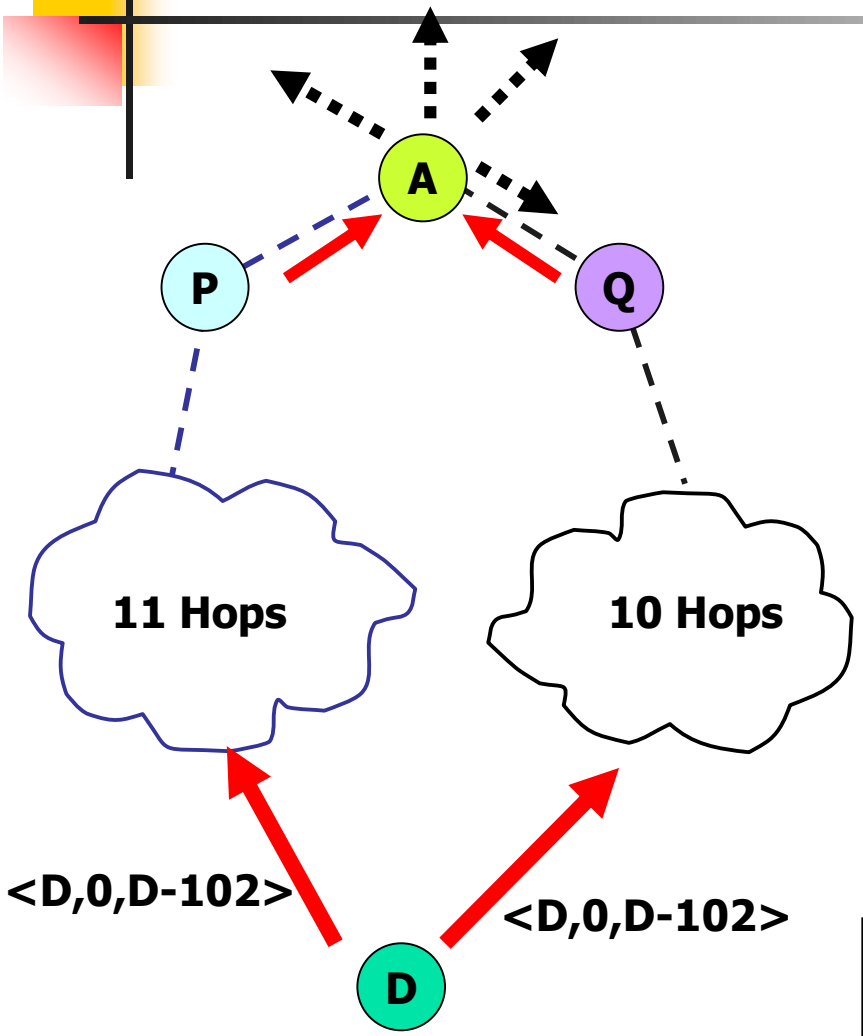
更新路由表中到D的表项
立即进行路由公告

3. A收到来自Q的路由更新消息<D, 14, D-102>

更新路由表中到D的表项
立即进行路由公告

由于D或者任何一个节点的路由更新消息到达节点A时存在着时间差,就会导致不必要的路由公告→路由表波动

DSDV协议操作：减缓路由波动



- 在一个单独的表中记录每条路由的最近的和平均的Settling Time
  - **Settling Time**：第一条路由和最佳路由之间的时间间隔
  - 路由表中的**stable data**指向该表
- A在包含新序列号的第一条路由到达时更新路由表，但是等待一段时间再广播该条路由
  - 等待时间=**2*(avg. Setting Time)**

可缓解大型网络的路由波动问题，
从而避免不必要的公告，节约了带宽

DSDV总结

优点

- 简单（基本上与DV算法一致）
- 通过目的地序列号避免了路由循环，解决了DV算法中的计数到无穷问题
- 无路由发现延时（先应式路由）

缺点

- 所有节点都必须公告路由，因此不支持休眠（不能直接用于传感器网络）
- 收敛慢（DV路由的特性）
- 开销大：大部分的路由信息从不使用
- 可扩展性是一个主要问题（所有先应式路由都存在的问题）

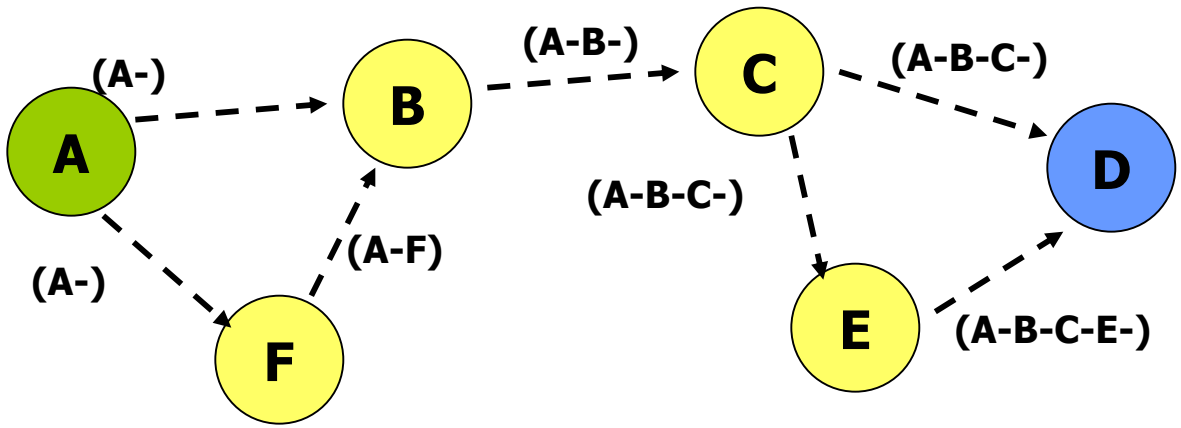
DSR协议组成

- 路由发现（Route Discovery）
  - 只有在源节点需要发送数据时才启动
  - 帮助源节点获得到达目的节点的路由
- 路由维护（Route Maintenance）
  - 在源节点在给目的节点发送数据时监测当前路由的可用情况
  - 当网络拓扑变化导致路由故障时切换到另一条路由或者重新发起路由发现过程

路由发现和路由维护都是按需进行的
- ✓ 不需要周期性路由公告
- ✓ 不需要感知链路状态
- ✓ 不需要邻居检测

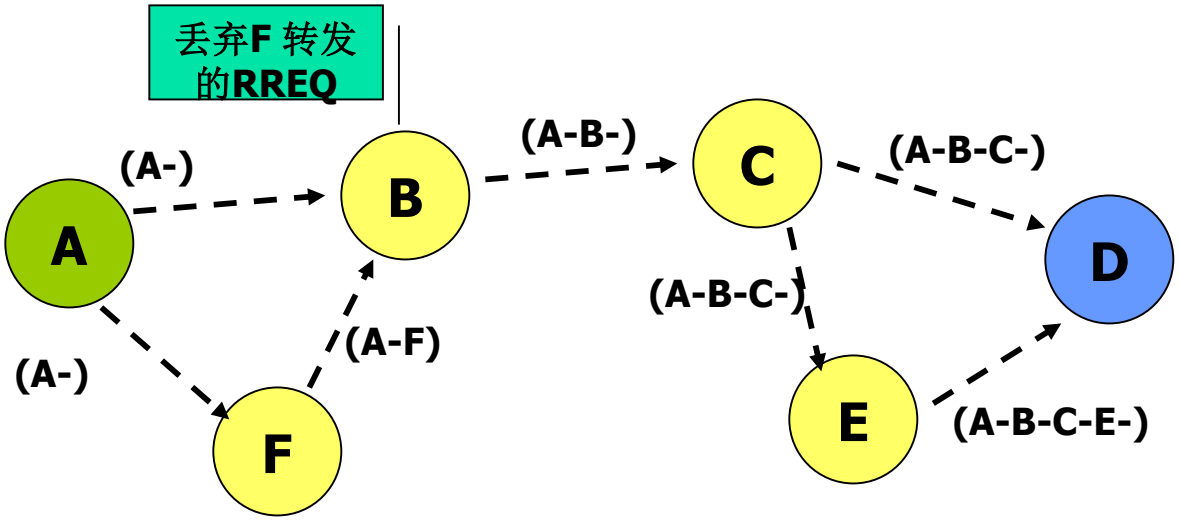
DSR路由发现：路由请求

- 源节点向邻居节点广播路由请求（RREQ：Route Request）消息
  - 源节点地址
  - 目的节点地址
  - 路由记录：记录源节点到目的节点路由中的中间节点
  - 请求ID
- 中间节点接收到RREQ后，将自己的地址附在路由记录中



DSR路由发现：中间节点处理

- 中间节点维护<源节点地址、请求ID>序列对列表
- 重复RREQ检测
  - 如果接收到的RREQ消息中的<源节点地址、请求ID>存在于本节点的序列对列表中
  - 如果接收到的RREQ消息中的路由记录中包含本节点的地址
- 如果检测到重复，则中间节点丢弃该RREQ消息

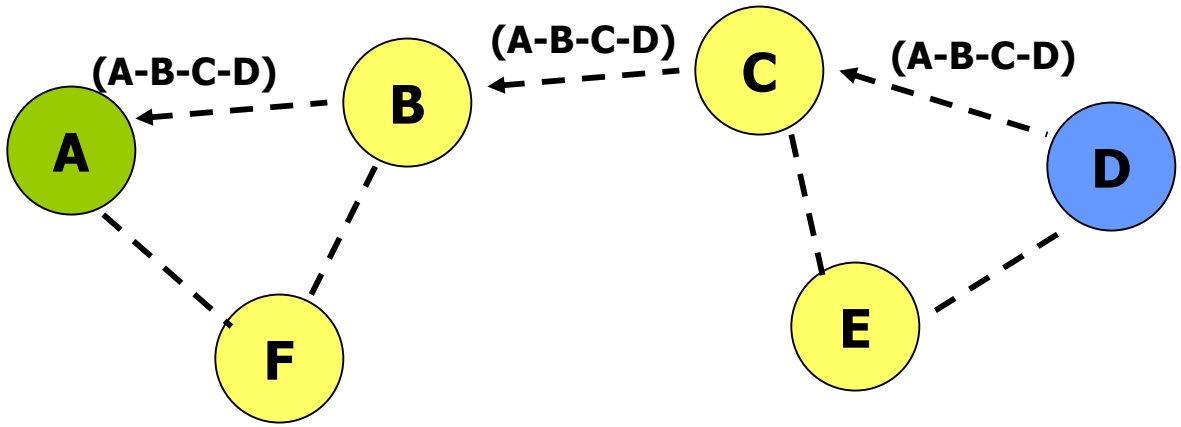


DSR路由发现：路由应答

- 目的节点收到RREQ后，给源节点返回路由应答（RREP：Route Reply）消息

  拷贝RREQ消息中的路由记录

- 源节点收到RREP后在本地路由缓存中缓存路由信息



DSR路由发现：非对称信道

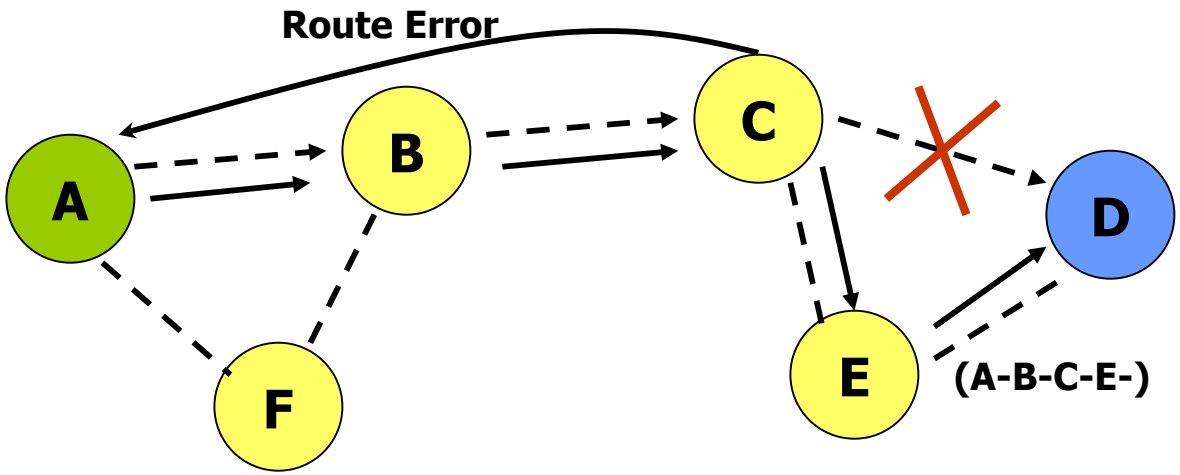
- 对称信道
  - 目的节点到源节点的路由即为源节点到目的节点的反向路由
- 非对称信道
  - 如果目的节点的路由缓存中有到达源节点的路由，则直接使用
  - 否则目的节点需要发起到源节点的路由请求过程，同时将RREP消息附加在新的RREQ消息中

DSR路由维护

- 逐跳证实机制
  - 链路层
    - ✓ 确认
    - ✓ 被动确认（监听其它节点间的数据发送）
  - 其它高层
    - ✓ 要求DSR软件返回确认
- 端到端证实机制
  - 无法确定故障发生的位置

DSR逐跳证实机制

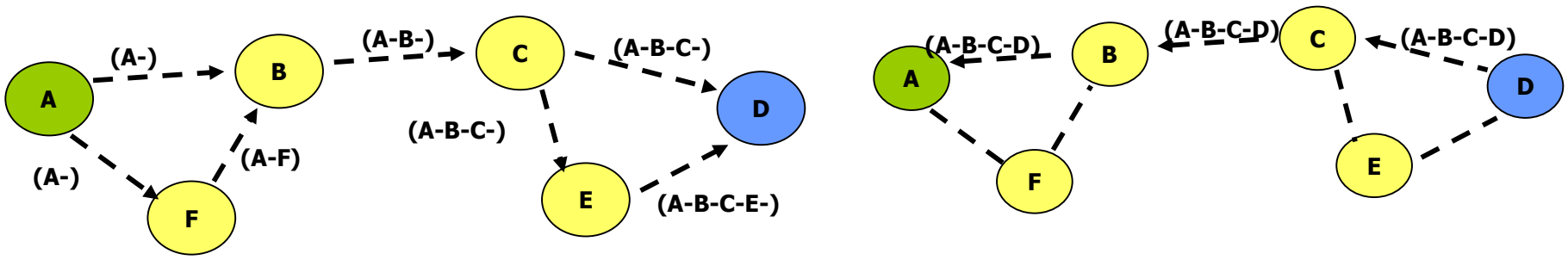
- 如果数据分组被重发了最大次数仍然没有收到下一跳的确认，则节点向源端发送路由错误（Route Error）消息，并且指明中断的链路
- 源端将该路由从路由缓存中删除
- 如果源端路由缓存中存在另一条到目的节点的路由则使用该路由重发分组
- 否则重新开始路由发现过程



DSR优化：路由缓存(1)

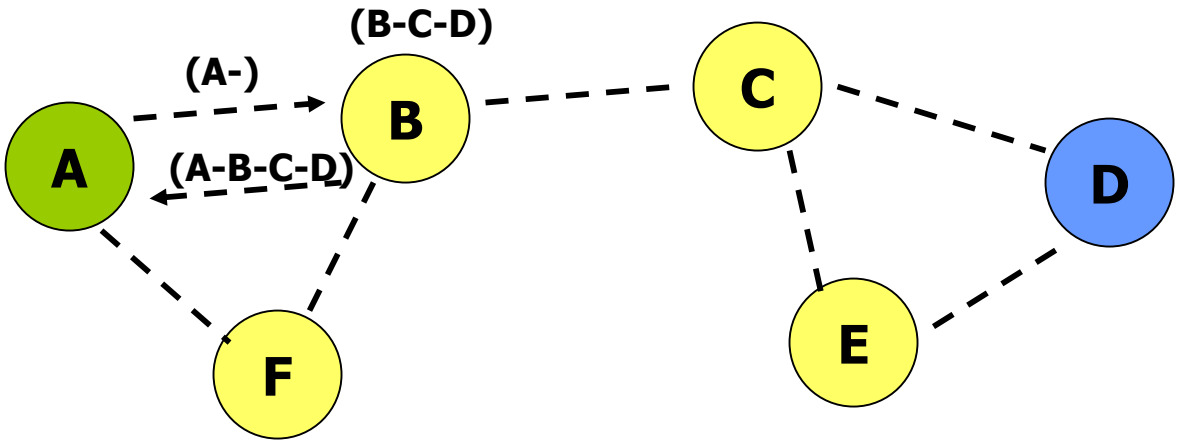
- 每个节点缓存它通过任何方式获得的新路由
  - 转发RREQ
    - ✓ 获得从本节点到RREQ路由记录中所有节点的路由，例如E转发RREQ(A-B-C)获得到到A的路由(C-B-A)
  - 转发RREP
    - ✓ 获得本节点到RREP路由记录中所有节点的路由，例如B转发RREP(A-B-C-D)获得到D的路由(C-D)
  - 转发数据分组
    - ✓ 获得从本节点到数据分组节点列表中所有节点的路由，例如E转发数据分组(A-B-C)获得到A的路由(C-B-A)
  - 监听相邻节点发送的分组
    - ✓ RREQ、RREP、数据分组等

以上均假设信道是对称的!



DSR优化：路由缓存(2)

- 中间节点使用缓存的到目的节点的路由响应RREQ
  - ✓ RREP中的路由记录=RREQ中的路由记录+缓存的到目的节点的路由



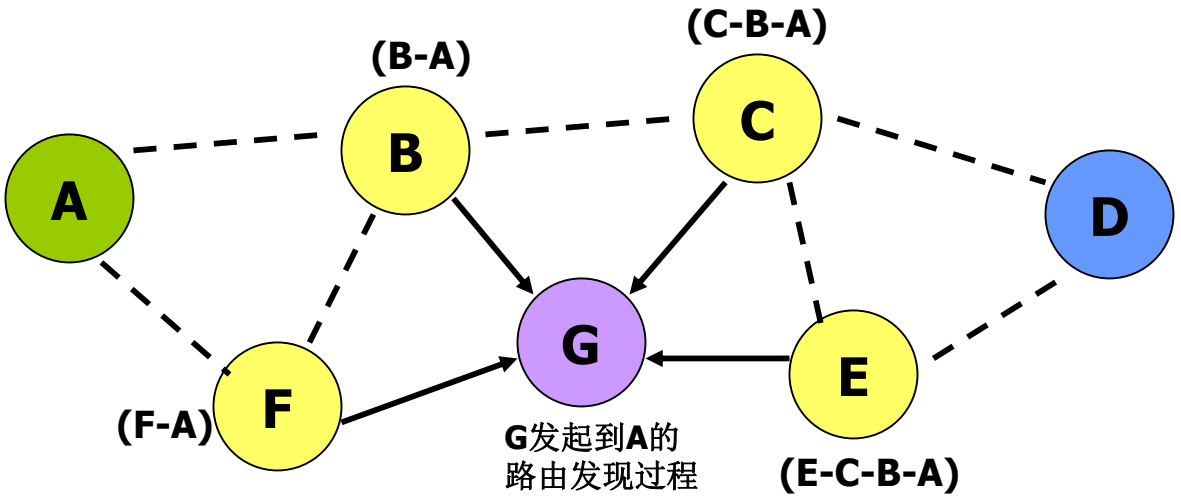
DSR优化：路由缓存(3)

- 错误路由缓存
  - 网络拓扑的变化使得缓存的路由失效
  - 影响和感染其它节点，使用该路由缓存的路由将不可用
  - 当节点根据路由缓存回应RREP时，其它监听到此RREP的节点会更改自己缓存的路由，从而感染错误路由缓存

设置缓存路由的有效期，过期即删除

DSR优化：路由缓存(4)

- RREP风暴
  - 节点广播到某个目的节点的RREQ，当其邻居节点的路由缓存中都有到该目的节点的路由时，每个邻居节点都试图以自己缓存的路由响应，由此造成RREP风暴
  - RREP风暴将浪费网络带宽，并且加剧消息冲突



DSR优化：路由缓存(5)

- 预防RREP风暴
  - 每个节点延时D发送RREP
  - D与节点到目的节点的跳数成正比，使得到目的节点有最短路径的RREP最先发送
  - 节点监听是否存在有比自己更短的到目的节点的路径，如果有，则不发送本节点的RREP

DSR总结

- 优点
  - 仅在需要通信的节点间维护路由，减少了路由维护开销
  - 路由缓存技术能够进一步减少路由发现的代价
  - 通过采用路由缓存技术，能够发现多条到达目的节点的路由
  - 支持非对称信道
- 缺点
  - 采用源节点路由，每个数据分组头标中都要携带路由信息，增加了网络开销
  - 由于采用广播，用于路由发现的控制消息可能波及到全网节点
  - RREP风暴问题
  - 错误路由缓存问题

DSDV与DSR优缺点分析

- DSDV

  优点：简单；无路由发现延时

  缺点：收敛慢（DV路由的特性）；开销大（大部分路由信息从不使用）

- DSR

  优点：

  - 采用源路由机制、避免了路由环路
  - 较少了路由维护开销
  - 采用路由缓存技术，减少了路由请求对信道的占用

  缺点：

  - 随着路径跳数的增加，分组头长度线性增加、开销大；
  - 来自邻居节点的RREQ分组在某个节点可能发生碰撞。解决办法：在发送RREQ分组时引入随机时延；
  - 在源节点发送RREQ时，可能会受到多个节点缓存的到达目的节点的路由信息，引入竞争。解决办法：若某节点听到其他节点发出的RREQ分组中路由信息含有较少跳数，此节点推迟发送。

分级路由协议的优缺点

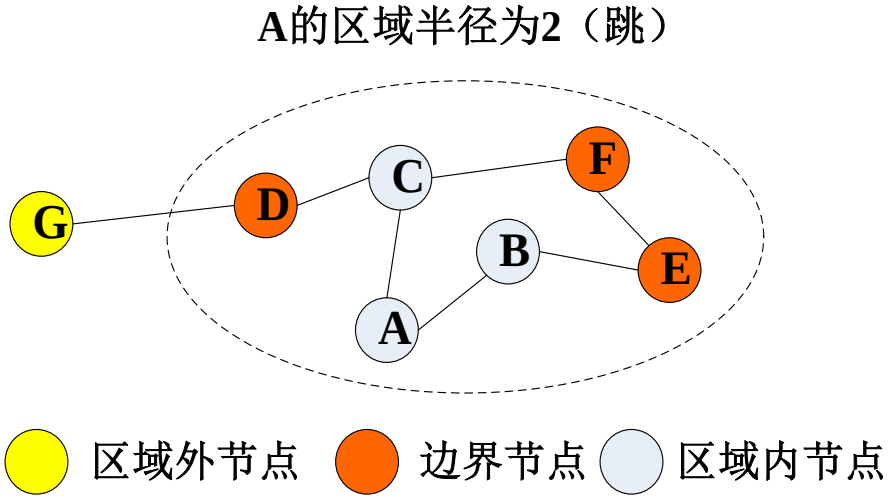
- 优点——具有较好的伸缩性
  - 网络拓扑结构的细节通过节点的层层聚合被隐藏起来，大大降低了大型网络的存储要求。
  - 路由信息分层传播，需要在全局传播的路由信息较少
  - 有限的链路状态维护
  - 按需建立路由
- 缺点——可靠性受到一定影响
  - 分级路由协议的移动管理比较复杂
  - 某些节点（cluster head/gateway）比其他节点承担更多的通信和计算负载

分级路由协议

- 区域路由协议 ZRP（Zone Routing Protocol）
  - ZRP是混合使用了主动和按需路由策略的自组网路由协议，结合了两种路由协议的特点。
  - 属于分区路由协议，网络被分成若干个以节点为中心、一定跳数为半径的虚拟区（区半径与跳数有关，因此ZRP的区重叠程度较高）
  - 节点采用主动路由协议维护区内路由，采用类似DSR协议的按需路由机制寻找去往区域外节点的路由（当区半径为1时，ZRP协议演变为按需路由协议、当区半径为MANET网络最大直径时，ZRP协议即为纯粹的主动式路由协议）
  - 协议性能很大程度上取决于区域半径参数值（小的区域半径适合节点移动较快的网络，大的区域半径适合在节点移动慢的稀疏网络）

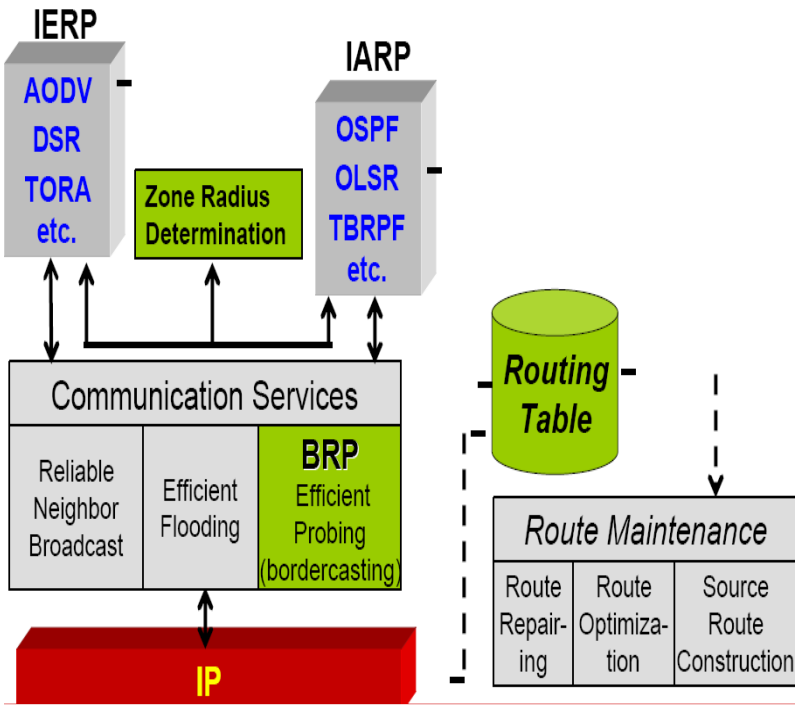
区域路由协议(ZRP)

- Zone Routing Protocol
  - 区域(zone)的划分
    - 整个网络被划分为若干个以节点为中心,一定跳数为半径的区域
    - 区域内节点数与设定的区域半径有关
  - 路由策略
    - 每个节点在区域内部采用表驱动路由
    - 对于区域外节点采用按需路由

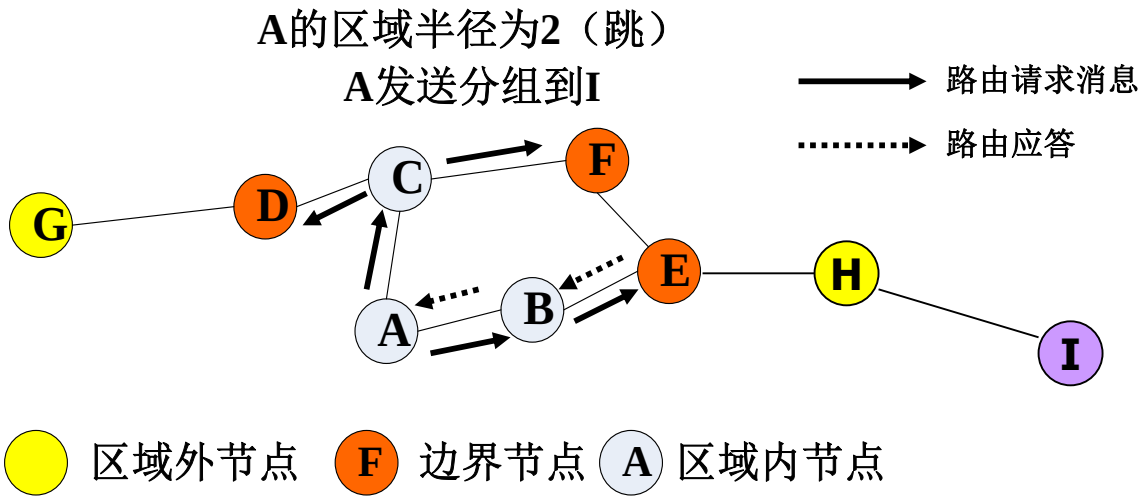


ZRP路由架构

- 区域内路由协议(IARP: IntrAzone Routing Protocol)
  - 采用表驱动路由协议，节点之间周期性地交换路由信息获得到域内各个节点的最新路由
    - 距离向量路由协议DSDV等
    - 链路状态路由协议OLSR等
  - 完成区域内部节点间的路由功能
- 区域间路由协议(IERP: IntErzone Routing Protocol)
  - 采用按需路由协议
  - 完成与区域外节点间的路由功能
- 边界传播协议(BRP: Bordercast Resolution Protocol)
  - BRP协议使得路由查询分组只在边界节点之间广播



ZRP路由过程

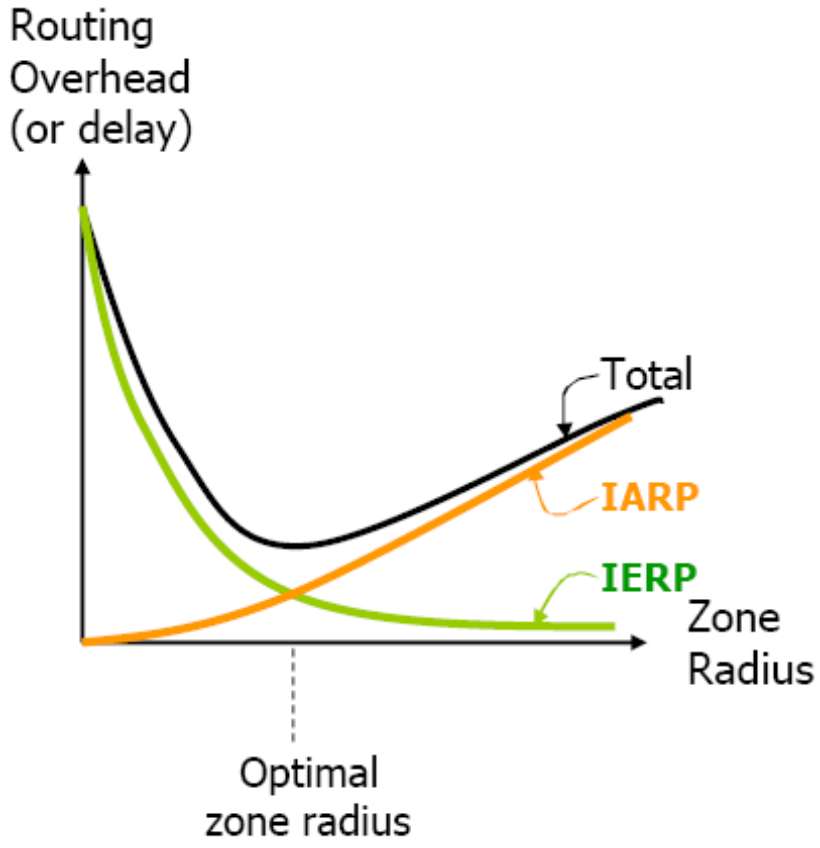


Z(A)={A, B, C, D, E, F}

- ✓ A发现节点I不在自己的区域内，向边界节点E、F、D广播路由请求消息
- ✓ 边界节点E收到路由请求消息后，发现节点I在自己的区域内，直接回复路由应答消息

ZRP总结

- 综合利用了按需路由和表驱动路由的优点
  - 在区域内减少了路由发现时间
  - 在区域间减少了系统开销
- 区域半径的设置将直接影响到路由的效率



多径路由技术

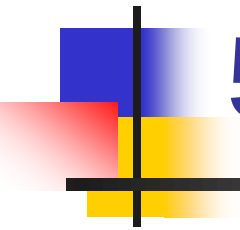
- 多径路由可以降低泛洪的频次，其方法是在一次泛洪查询过程中探测多条可能的路由，以低成本提供足够的冗余度。
- 多径路由能够提高通信节点对带宽的有效利用，响应网络拥塞和突发传输，提高分组交付的可靠性。

多目标路由协议

- 多目标协议也叫多播或组播路由协议。
- 多目标传输(也叫组播或多播)是将数据分组发送给由一个目的地址指定的一组主机。
- 多目标用于面向节点组的计算，越来越多的应用必须是点对多点传输。
- 多目标服务对于团队密切协作的应用非常重要，如要求共享文本和图片、召开音频和视频会议。

路由协议的性能分析与评价

- 定性性能指标：
  - ✓ 分布式操作
  - ✓ 开环
  - ✓ 基于需求的操作
  - ✓ 主动式操作
  - ✓ 网络安全
  - ✓ “休眠”操作
  - ✓ 单向链路的支持
- 定量性能指标：
  - ✓ 端到端的数据吞吐量和数据时延
  - ✓ 路由获取时间
  - ✓ 乱序交付百分率
  - ✓ 效率



5 功率控制

功率控制

- 可达性(Accessibility)和便携性(Portability)在移动Ad Hoc网络中是一对矛盾的综合体。
- 功率管理是无线通信领域中最富挑战性的一个问题。
- 功率消耗源：
  - 与通信有关的功率消耗源
  - 与计算有关的功率消耗源

与通信有关的功率消耗源

- 在移动Ad Hoc网络中，通信涉及源节点、中间节点，以及目的节点对收发信机的使用。
- 一部典型的移动电台可能存在三种工作方式：发射、接收、备用。
- 发射方式功耗最大，备用方式功耗最小。
- 在能量资源有限条件下的协议开发目标是：对于一个给定通信任务，收发信机的使用最优化。

与计算有关的功率消耗源

- 主要集中在协议处理方面，包括CPU和主存储器的使用，以及在极小程度上使用磁盘或者其他组件；
- 数据压缩技术(用于减小分组的大小，因而减少能量的使用)由于增加了计算而可能增加功耗；
- 需要对计算成本和通信成本进行综合、平衡考虑。

功率控制

- 移动Ad Hoc网络的功率控制就是每个节点按照分布式方式为每个分组选择发射功率。
- 功率等级的选择从根本上影响移动Ad Hoc网络许多方面的操作：

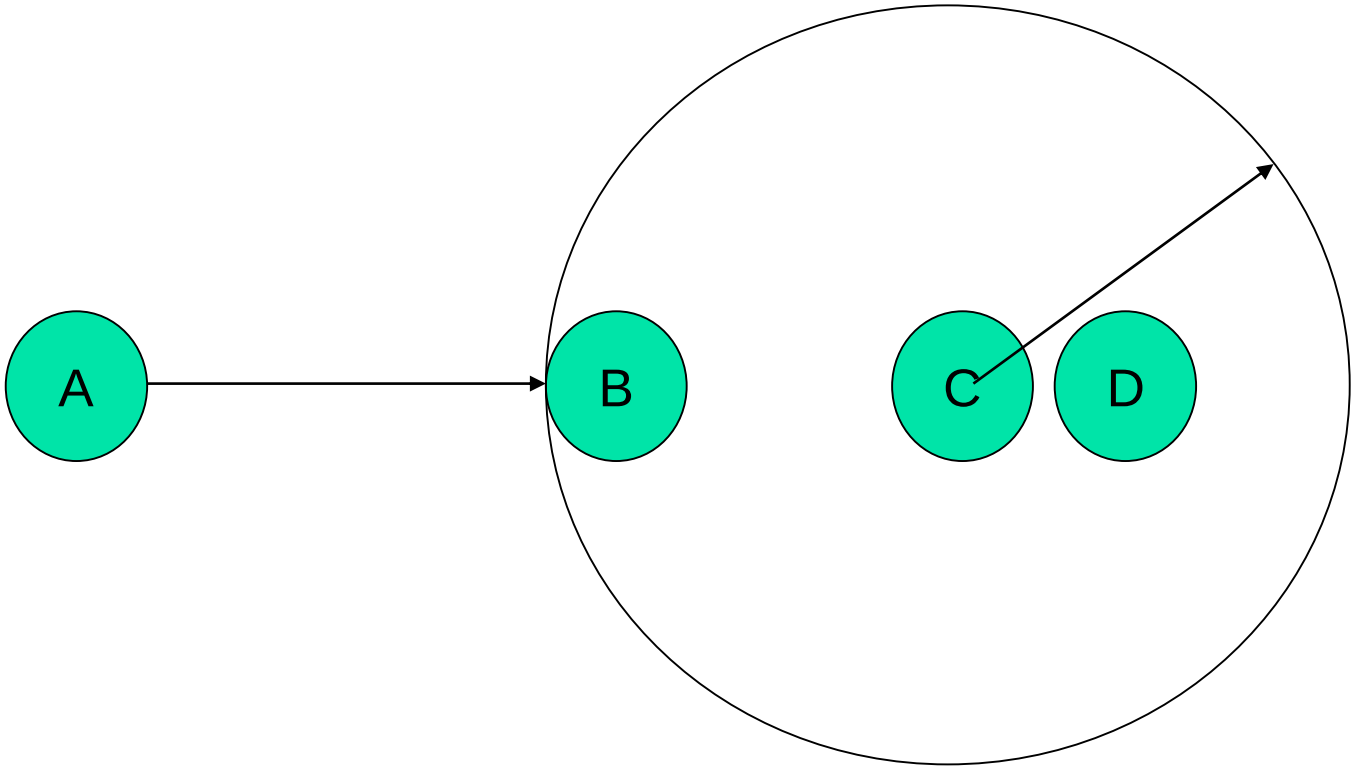
  (1) 发射功率等级决定接收节点接收信号的质量；

  (2) 发射功率等级决定发射的传输距离；

  (3) 发射功率等级决定干扰其他接收节点的量级。
- 发射功率控制影响到协议栈各个层次，影响吞吐量，时延，能量消耗等多个关键性能。

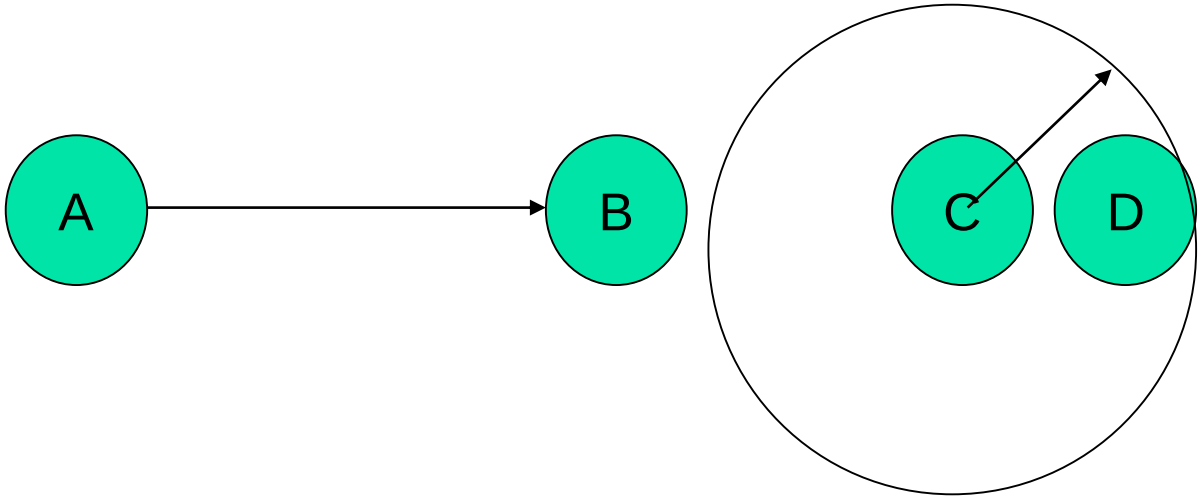
功率控制

- When C transmits to D at a high power level, B *cannot* receive A's transmission due to interference from C



功率控制

- If C reduces transmit power, it can still communicate with D
  - Reduces energy consumption at node C
  - Allows B to receive A's transmission (spatial reuse)



不利因素

- 功率控制影响物理层；
- 由于传输距离影响路由算法，所以功率控制影响网络层；
- 由于干扰产生碰撞，所以功率控制影响传输层。

如何进行功率控制

- 如果在OSI协议栈的很多协议设计中采用固定功率等级，那么功率等级的变化将引起故障。

（1）改变功率等级可能产生单向链路

（2）但大部分协议假定双向链路及路由

- 发射功率控制是一个交叉层设计问题，影响协议栈的各个层次，影响吞吐量、时延、能量消耗等几个关键性能的测量。

通用节能途径

(1) 通过以下方式尽力减少分组重传

- 在链路层采用检错、纠错能力强的编码，通过自动重传请求和前向纠错来节省功率
- 提高物理层抗干扰能力
- 在MAC层尽可能排除分组传输碰撞。
- 尽早发现节点不可达

(2) 收发信机的高效使用

- 允许接收节点一段时间无需接收数据时，可关闭该节点
- 由于收发转换带来功耗，可将邻近时隙分配给终端发射或者接收，从而降低功耗。

通用节能途径

(3) 设置优先级，根据节点供电能力调度

- 将电能紧张的节点设为较高优先级，立即发送分组。

(4) 节点能耗的控制与管理

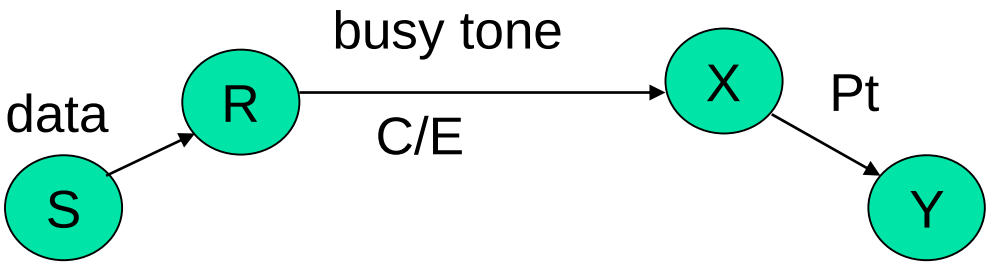
- 尽可能保证全部节点同等的耗尽各自的电池能量。
  - ✓ 避免低电量节点路由；减慢路由更新
  - ✓ 善用广播和多目标传输；改变节点功率控制网络拓扑

(5) 暂停组成单元的操作

- OS层节能控制

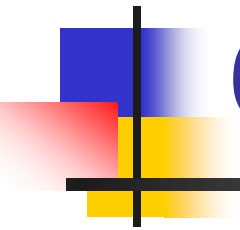
PCMA

- If receiver node R can tolerate noise E, it sends a busy tone at power level C/E, where C is an appropriate constant
- When some node X receives a busy-tone at power level Pr, it may transmit at power level Pt <= C/Pr



PCMA

- Advantage
  - Allows higher spatial reuse, as well as power saving using power control
- Disadvantages
  - Need a separate channel for the busy tone
  - Since multiple nodes may transmit the busy tones simultaneously, spatial reuse is less than optimal



6 IP地址分配技术

IP地址分配技术

- IP网络中，移动装置的IP地址分配是最重要的网络配置参数之一。
- 一个移动装置在没有分得一个空闲IP地址及其相应子网掩码地址之前无法参与网络单目标通信。
- 地址分配是面向MANET网络实际应用的第一步。
- 相同MANET的所有节点共享一个网络地址，使用IPv4专用地址或IPv6相同特定前缀。
- 对于大规模MANET，需要使用动态IP分配技术。

三种必需应对情形

- A：一个移动节点加入一个MANET，然后永久离开。
- B：一个MANET分割成互不连接部分，随后又合并。
- C：两个孤立的MANET合并。

五种分配要求：

- IP地址不存在冲突。
- 节点加入网络分得地址，退出网络必需释放地址。
- 除非无可分配地址，否则不能拒绝节点分配请求。
- 解决合并及分割带来的IP地址冲突问题。
- 节点必需得到授权才能被分配IP地址。

目标：开销低、均匀分布、时延小、扩展性强、复杂性低。

分配方法

1. 冲突检测分配法

—采用“试验和错误”策略为新节点寻找空闲IP地址，

—需要得到所有已配置节点认可。

2. 无冲突分配法

—根据假定互不相交的地址池分配给新节点空闲地址。

—已配置节点将地址池一分为二，一半给新节点。

—解决分割问题。

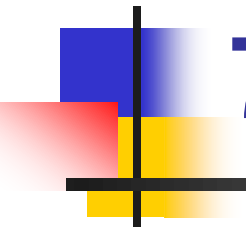
3. 最大努力分配法

—负责地址分配节点尽其所知分配给新节点空闲地址。

—当多个新节点几乎同时加入，容易发生地址冲突。

—新节点采用地址冲突检测保证地址空闲。

—考虑了分割和合并问题。



7 移动Ad Hoc网络的QoS问题

移动Ad Hoc网络的QoS问题

- 在移动Ad Hoc网络上运行多媒体应用，正在成为普适计算和普适通信环境中的一个完整部分，如视频电话和按需多媒体。
- 将多媒体应用和移动Ad Hoc网络综合在一起的一个重要的认可准则就是提供端到端的服务质量QoS，如访问多媒体数据的高成功率，以及数据恢复时的有限制的端到端时延和满意的吞吐量。

服务质量参数

- 服务质量通常定义为把分组流从源节点传输到目的节点的时候网络必须满足的一个服务要求集合。
- 例如，时延、带宽、分组丢失概率、时延变化(抖动)，等等。
- 功率消耗和服务覆盖范围是另外两个QoS属性，这两个属性对移动Ad Hoc网络很特别。

提供QoS支持所面临的问题与困难

(1) 不可预测的链路特性。

(2) 隐藏终端和暴露终端问题。

(3) 节点移动。

(4) 路由维护。

(5) 有限的电池寿命。

(6) 安全。

折 中 原 理

- 移动Ad Hoc网络的动态性归因于多种原因。例如，易变和多变的链路特性、节点移动、变化的网络拓扑、可变的应用要求。
- 在这种动态环境下提供QoS是非常困难的。为移动Ad Hoc网络提供QoS的两个折中原理是：软QoS和QoS自适应。

折中原理

- 软QoS

通过在总的连接时间内的总的未满足时间之比来量化QOS满足等级，并使得这个比率不高于某个门限值。

- QoS自适应

允许在一个预留指定范围内，随着有效资源的变化，重新调整资源分配。

—物理层通过自适应提高或降低发射功率来跟踪传输质量变化。

—链路层自动对链路差错率变法做出反应，包括使用自动重传，自适应误码纠错机制等。

—网络层自动对网络的有效带宽和时延做出反应。

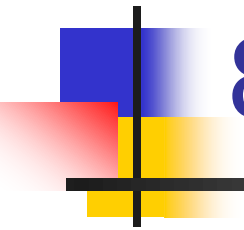
处理方法

1. 从单一网络层次上支持QoS

按照层次化观点讨论移动Ad Hoc网络提供QoS的问题。首先从物理层开始，然后到应用层。

2. 层间处理法

除了在单一网络层上研究QoS支持以外，现在已经做了一些努力引导设计和实现移动Ad Hoc网络的层与层之间的QoS框架体系。



8 Ad hoc网络安全性问题

安全性问题（1）

- 使用无线信道使Ad hoc网络容易受到诸如被动窃听、主动入侵、信息阻塞、信息假冒等各种方式的攻击。
- 窃听可能使敌方获取保密信息。
- 而主动攻击可能使敌方删除信息、插入错误信息、修改信息、或者冒充某一节点，从而破坏了可用性、完整性、安全认证和抗抵赖性。
- 由于节点能源有限，且I/O 计算能力较低，无法实现复杂的加密算法，这增加了被窃密的可能性

安全性问题（2）

- 当节点在战场上移动时，由于缺乏足够保护，很有可能被占领。因此，恶意攻击不仅来自Ad hoc网络之外，且可能从网内产生。
- 为了获得更高的生存能力，Ad hoc网络应该具有分布式结构。所以，在安全机制中引入中心控制节点。将使网络更易于受到攻击。
- 由于节点移动性，Ad hoc网络的拓扑结构和成员处于动态的变化之中。节点之间的信任关系也在不断变化，因此任何只具有静态配置的安全方案在Ad hoc网络中是不可行的。

安全性问题（3）

- Ad hoc网络中可能包括成百上千个节点。
- 安全策略应该具有可扩展性，以适应大规模的网络。
- 由于Ad hoc网络的应用环境有很多，针对不同的环境所应采取的安全策略也应有所不同。例如，在无线网络会议系统中，节点物理上的安全 保障是没有问题的，而在特殊领域（如战场环境）中则不然，因此还需要适当增加物理安全防范措施。

安全目标

- 实用性：密钥管理服务在任何层次应对DoS
- 机密性：保证某些信息永远不会暴露
- 完整性：保证消息不会被破坏
- 认证：确保能识别对方身份
- 非否定性：探测和隔离可疑节点

可以采用安全策略和机制

- 基于口令的认证协议

与传统的口令认证不同的地方是密钥和口令的产生是由多台机器决定，而不是集中由一台机器产生，且还提供了一种完善的口令更新机制。

- 单一模式

主要针对传感器网络里，传感器与控制者之间可能存在的不安全问题，提出传感器在“死亡”之前，只受其拥有者的控制。

- 异步的分布式密钥管理

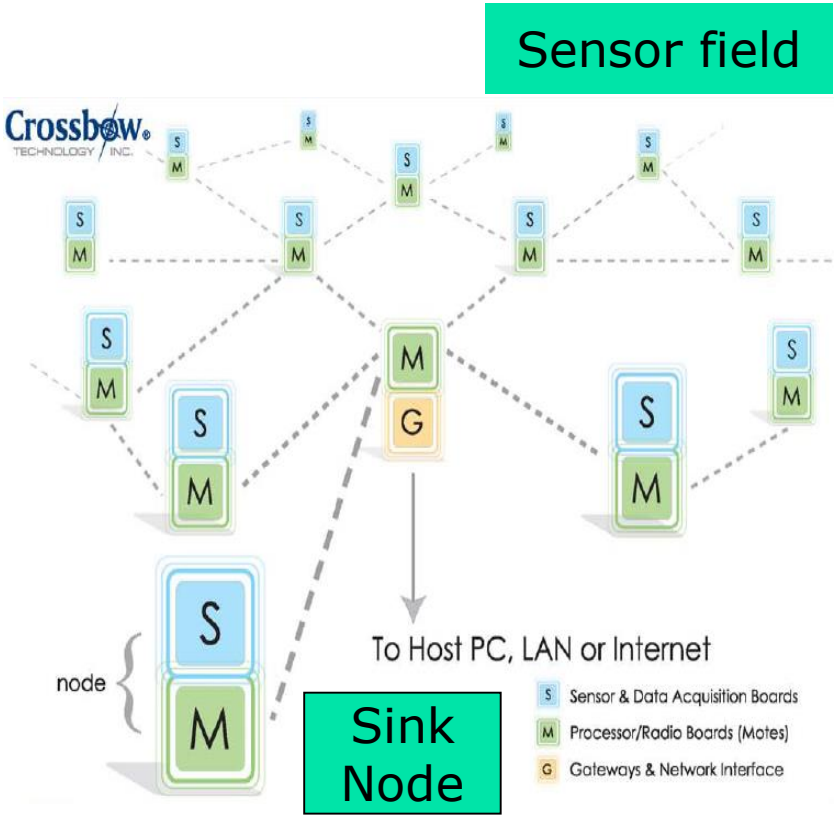
密钥管理服务是由多个节点(一个集合)来管理，而不是单个节点来管理。

MANET与WSN

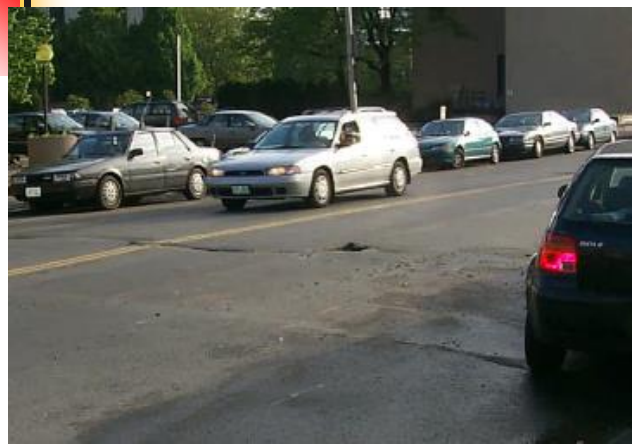
- Sensor networks
  - Ad hoc network of sensors
  - Addressing based on data (or function) instead of name
    - “send this packet to a temperature sensor”

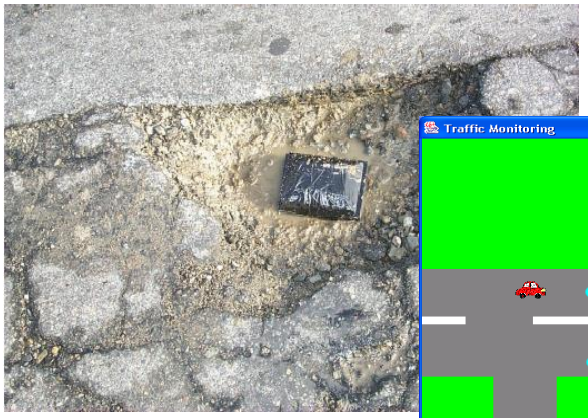
Wireless sensor networks (WSN)

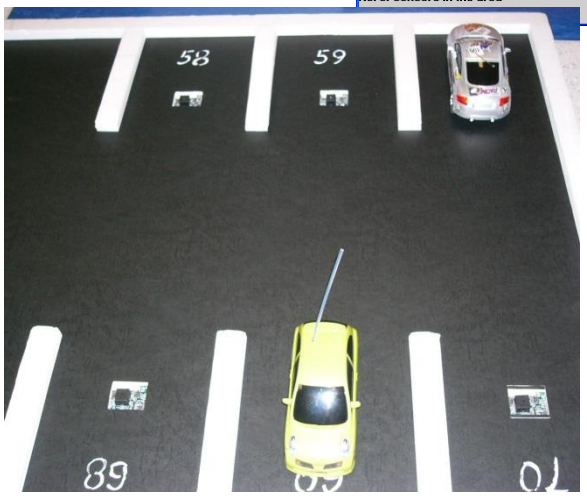
- Composed of a large number of sensor nodes (hundreds or thousands)
  - The nodes are constantly mobile or in fixed positions
- Sensor nodes communicate through wireless connections
- There is a lack of a fixed infrastructure
  - Sensor nodes are deployed, either randomly or with plan, over the designated site or very close to it



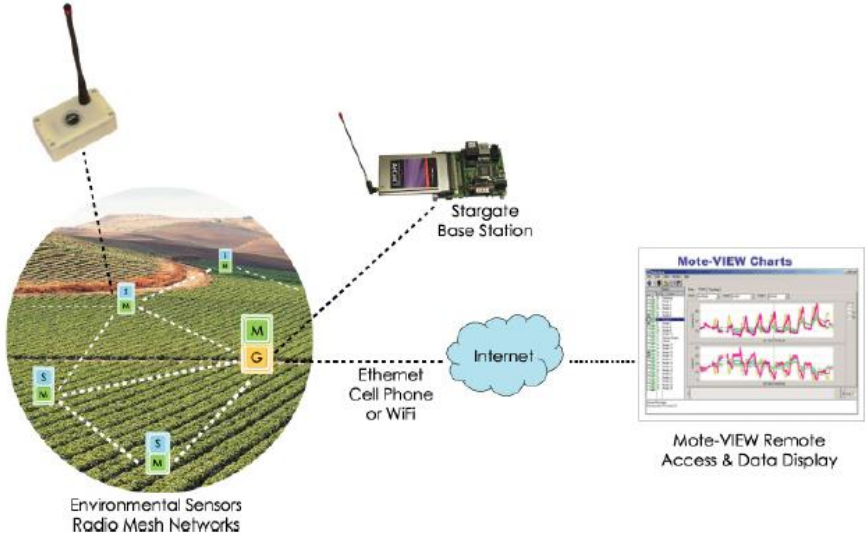
Applications of WSNs



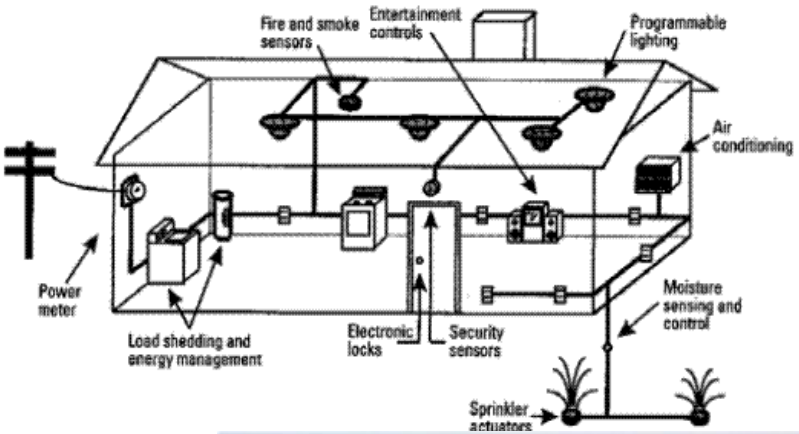


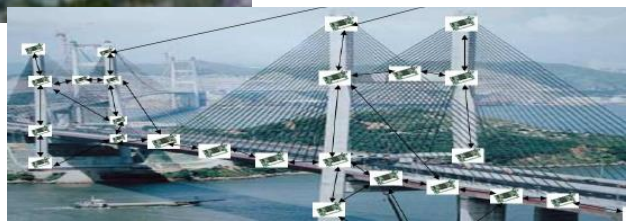


Applications of WSNs



Applications of WSNs





Differences from MANET

- The number of sensor nodes are much higher than the nodes in a MANET
  - Sensor nodes are densely deployed
- Senor nodes are more likely to failure (due to power lost or damaged)
- Sensor nodes are much more limited in power, memory, and computational capacities
- Senor nodes mainly use broadcast communication (or flooding)
- Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors involved
- Data is requested based on certain attributes

作业七

1 简述MANET信道接入中的隐藏终端和暴露终端问题，并举例解决方法。

2 简述主动式路由及按需式路由的工作方式，并比较其优缺点。

3 阐述MANET中路由无穷计算问题及解决办法。

4 阐述MANET中RREP风暴问题及解决办法。

5 阐述MANET中路由波动问题及解决办法。

6 简述功率控制对MANET性能的影响。

7 简述MANET中QOS折中原理。

8 简述MANET最大努力地址分配方法。

课堂报告

- 每1-3名同学学习调研某一无线网络专题，并以ppt演讲的形式在课上作介绍，并回答问题，占平时成绩30%。
- ppt要求15-20页，时间10-15分钟。
- 无线网络专题内容限于移动自组织网络和无线传感器网络的某一个MAC、路由、拓扑控制协议或功率控制算法，要着重具体算法流程和工作原理。
- 时间安排：

  待定