



# 第5章 WSN 支撑技术

---

## 学习目标

- ◆掌握时间同步
- ◆了解节点定位
- ◆了解数据融合
- ◆了解能量管理
- ◆了解容错技术
- ◆了解QoS保证
- ◆了解安全性



## 第5章WSN的支撑技术

---

虽然传感器网络用户的使用目的千变万化，但是作为网络终端节点的功能归根结底就是**传感、探测、感知**，收集应用相关的数据信号。

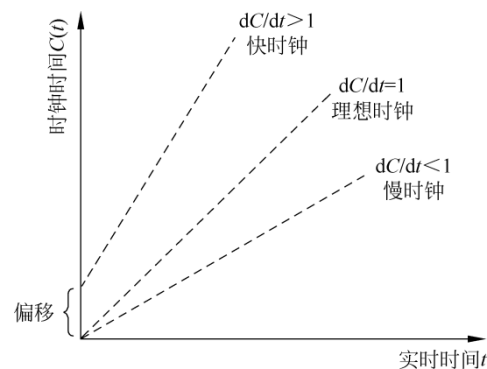
本章所设及到的基础性技术是支撑传感器网络完成任务的关键，包括**时间同步机制、定位技术、数据融合、能量管理和安全机制**等。

## 5.1.1 时钟同步

基于硬件振荡器的计算机时钟是所有计算设备的重要组成部分。典型的时钟由一个稳定的石英振荡器和一个计数器组成，这个计数器随着每次石英晶体的振荡递减。

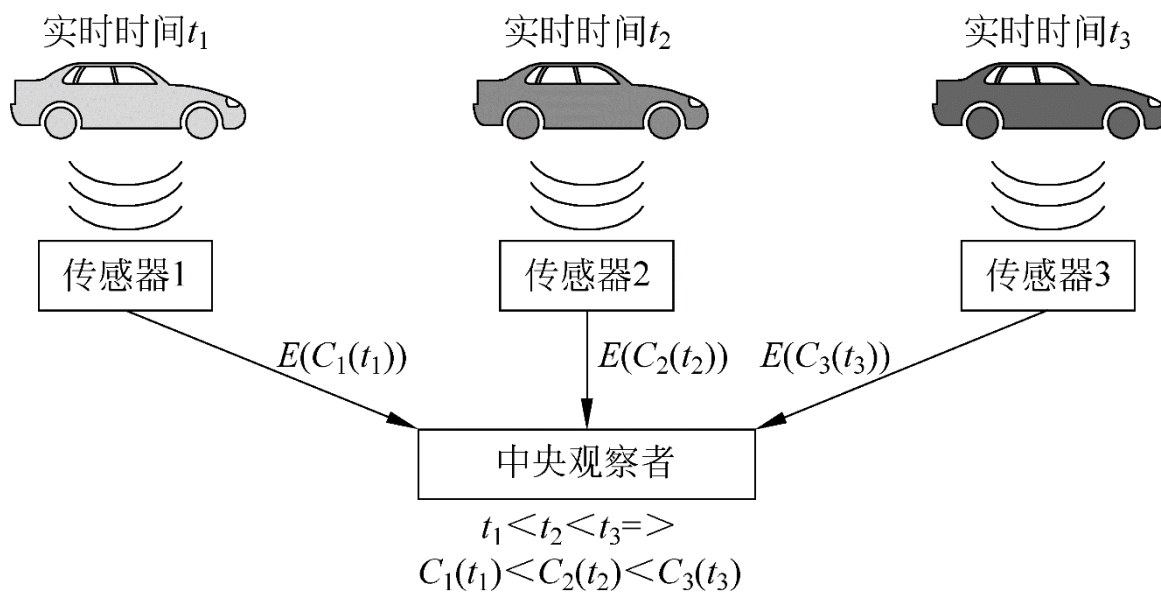
对于两个节点的本地时间而言，**时钟偏移**量表示时钟之间的时间差。**同步**是指调整一个或者两个时钟，从而使它们的读数匹配。

$$1 - \rho \leq \frac{dC}{dt} \leq 1 + \rho$$



## 5.1.2 时间同步问题

### 1. 时间同步的必要性





---

## 2.时间同步面临的挑战

(1)环境影响

(2)能量限制

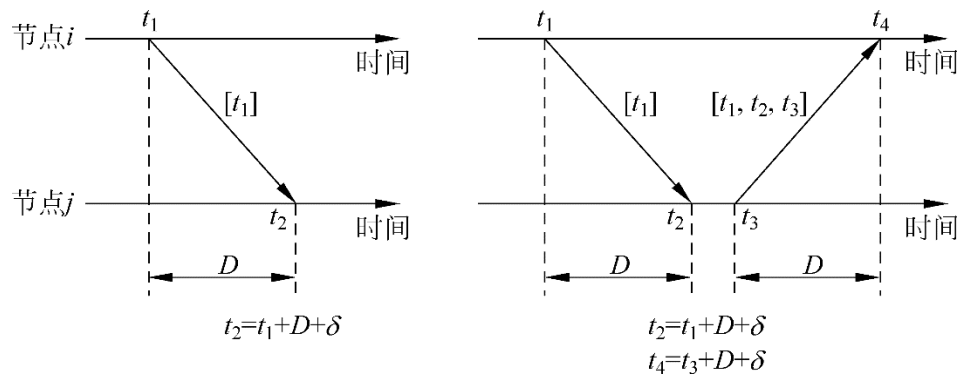
(3)无线介质和移动性

(4)其他约束

## 5.1.3 时间同步基础

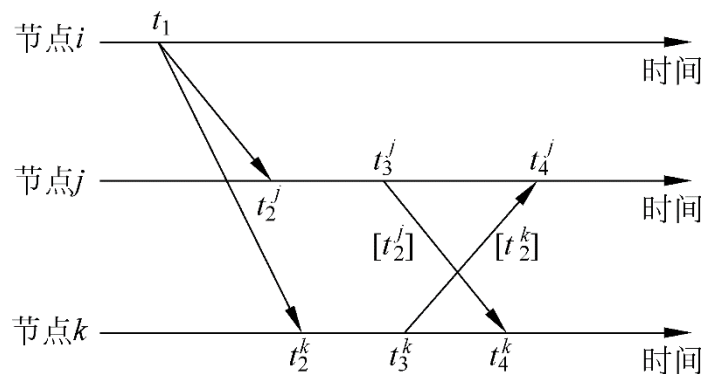
### 1. 同步消息

#### (1) 单向消息交换



#### (2) 双向消息交换

#### (3) 接收端-接收端同步



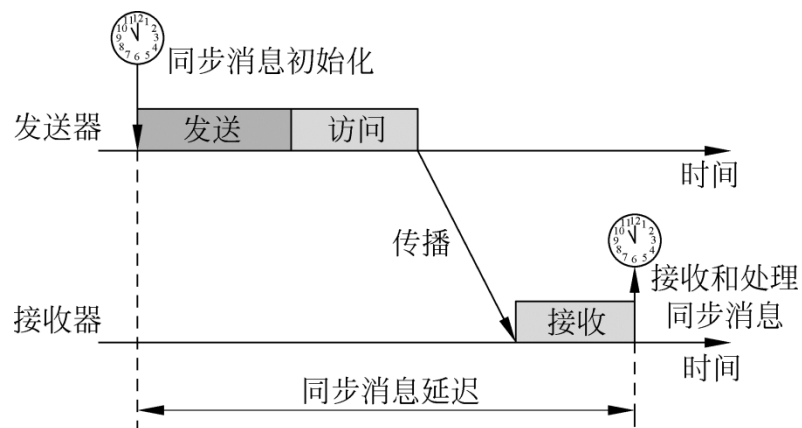
## 2.通信延时的不确定性

(1)发送延时

(2)访问延时

(3)传播延时

(4)接收延时

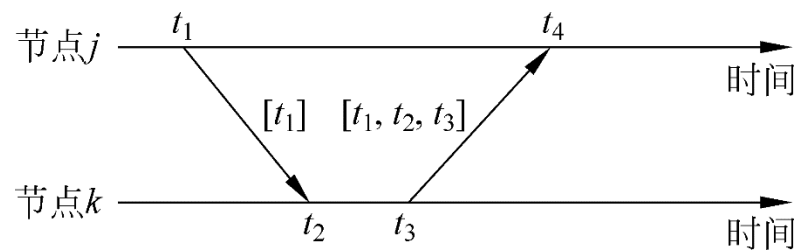


## 5.1.4时间同步协议

### 1. 基于全球时间源的参考广播

全球定位系统GPS

### 2. 基于树的轻量级同步



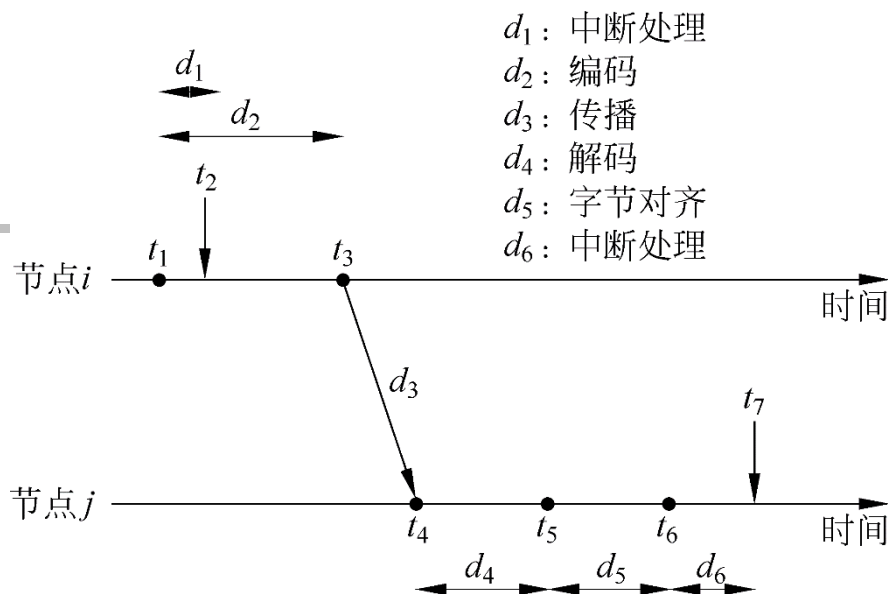




### 3.TPSN传感器网络的时间同步协议

(1)级别探测阶段

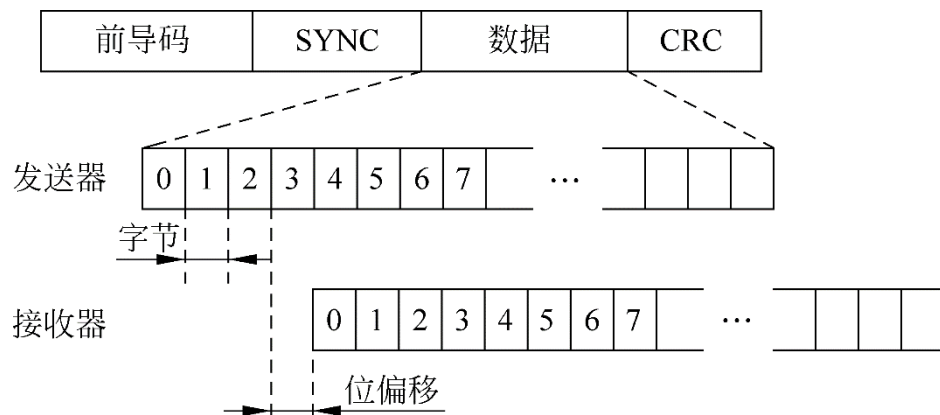
(2)同步阶段



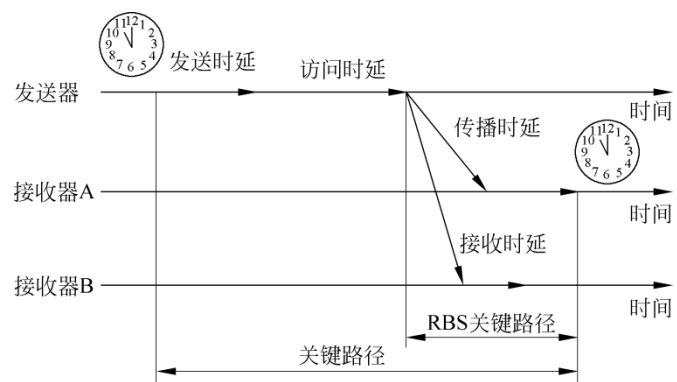
### 4.洪泛时间同步协议

(1) FTSP的时间戳

(2)多跳同步



## 5.参考广播同步



## 6.时间扩散同步协议

# 5.2 定位技术

## 5.2.1 基本描述

### 1、节点定位的基本概念

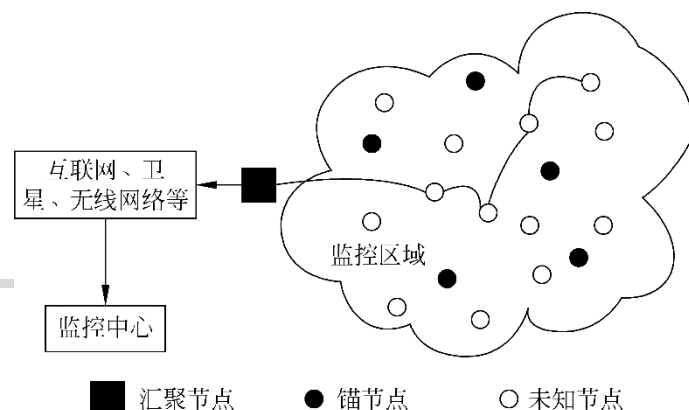
**节点定位**是指根据有限的位置已知的节点来确定无线传感器网络中其他节点的位置，在无线传感器网络的节点之间建立起位置关联关系的定位机制。

在无线传感器网络中，需要定位的节点称为**未知节点(unknown node)**，即不知道自身位置的节点，在一些资料中也称为盲节点(**blind node**)。

而已知位置，并协助未知节点定位的节点称为**锚节点(anchor node)**，部分资料中也称为**参考节点(reference node)**、**信标节点(beacon node)**。

为了描述方便，统-称为**锚节点**，并遵从CC2530数据手册，称位置已知的节点为**参考节点**。锚节点在网络节点中所占的比例很小，可以通过GPS定位系统或根据预先指定等手段获取自身的精确位置。

每个节点通信半径以内的其他节点，称为**邻居节点(neighbor nodes)**。如图5-11所示的典型的无线传感器网络结构，通过锚节点向网络广播信标信息(**beacon**)，或未知节点通过与邻近的锚节点或已经知道位置信息的邻居节点之间通信，未知节点获得与其他节点的距离或跳数信息，然后根据一定的定位算法得到自身的位置信息。





## 2.定位算法的分类

### (1)基于测距的定位和距离无关的定位算法

基于测距(range-Based)的定位(Range-Based)和与距离无关(Range-Free)的定位算法。

### (2)基于锚节点定位和无锚节点辅助的定位算法

基于锚节点的定位算法(Anchor-Based)和无锚节点辅助的定位算法(Anchor-Free)。

### (3)集中式计算定位与分布式计算定位

集中式计算定位需要把信息传送到某个中心节点(例如服务器), 在中心节点完成节点位置的计算。

分布式计算定位也称并发式算法, 依赖节点间的信息交换和协调, 由节点自行计算自身位置。

### (4)紧密耦合定位与松散耦合定位

紧密耦合定位系统是指锚节点不仅被仔细地部署在固定的位置, 并且通过有线介质连接到中心控制器。

松散型定位系统的节点采用无中心控制器的分布式无线协调方式,



# 定位的基本要素

---

信号强度

到达时间

到达时间差

到达角度

.....



### 3.定位算法的性能分析

---

具体分析各个性能指标。

- ① 定位精度
- ② 规模
- ③ 锚节点密度
- ④ 节点密度
- ⑤ 覆盖率
- ⑥ 容错性和自适应性
- ⑦ 功耗
- ⑧ 成本



## 5.2.3 基于测距的定位算法

基于测距的定位机制(rang-based)通过测量相邻节点间的距离或角度信息，然后再使用三边测量、三角测量或最大似然估计定位计算方法来计算节点位置。其常用的测距技术有RSSI，TOA，TDOA和AOA。测距定位过程分为以下三个阶段。

- ①测距阶段，未知节点测量到邻近锚节点的距离或角度。
- ②定位阶段，计算出未知节点与三个或三个以上锚节点的距离或角度后，然后利用三边测量法、三角测量法或极大似然估计法计算未知节点的坐标。
- ③校正阶段，对计算得到的节点的坐标进行循环求精，减少误差，提高定位算法的精度。



# 1.基于RSSI的定位机制

基于RSSI(received signal strength indicator)的定位, 即基于接收信号强度指示的定位, 已知发送节点的发送信号强度, 通过测量接收信号强度, 计算信号的传播损耗, 根据理论或经验信号传播衰减模型将传播损耗转化为距离。得到锚节点与未知节点之间的距离信息后, 采用三边测量法或最大似然估计法可计算出未知节点的位置。

$$p_r(d) = \frac{p_t G_t G_r \lambda^2}{(4\pi)^2 d^2 l}$$

实际应用中的情况要复杂得多, 尤其是在分布密集的无线传感器网络中。

$$p_r(d)[\text{dBm}] = p_0(d_0)[\text{dBm}] - 10n\log_{10}\left(\frac{d}{d_0}\right) + X_s$$

RSSI是一种低功率、廉价的测距技术, 它的**主要误差**来源是环境影响所造成的信号传播模型的建模复杂性, 反射、多径传播、非视距(NLOS)、天线增益等问题都会对相同距离产生显著不同的传播损耗。

因此**这种方法**是一种粗糙的测距技术, 它有可能产生±50%的测距误差。一般只能适用于对误差要求不高的场合。





## 2.基于TOA的定位机制

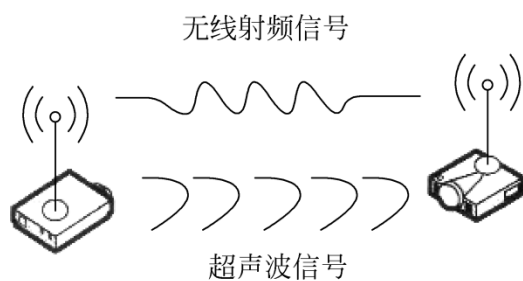
---

**Time of Arrival**

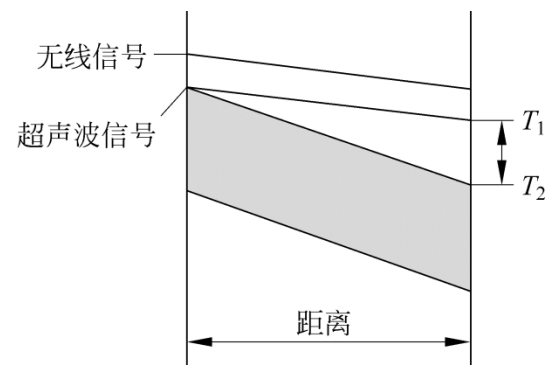
单向传播时间

往返时间差

### 3.基于TDOA的定位机制

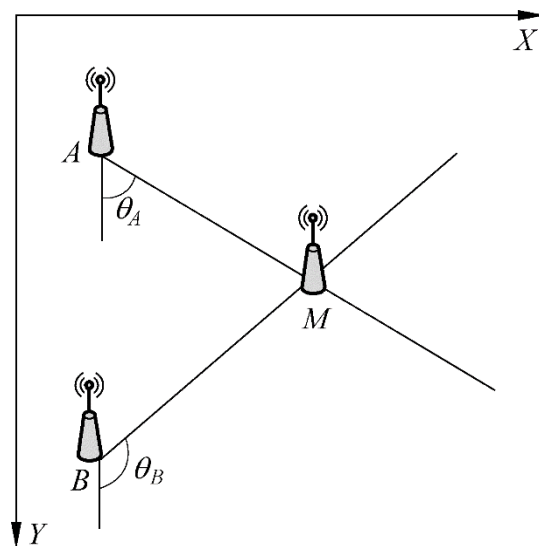


(a) TDOA定位节点示意图



(b) TDOA定位测距原理图

## 4. 基于AOA的定位机制



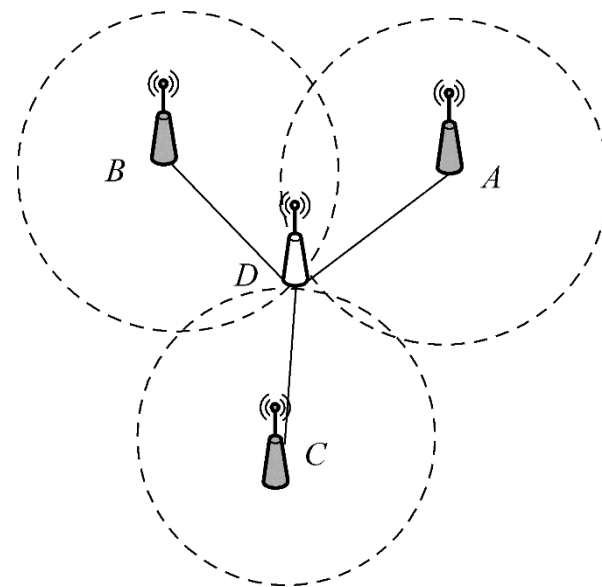
## 5.2.2 节点位置的计算方法

定位计算的基本方法包括：三边测量法、三角测量法、极大似然估计法、最小最大法。

### 1. 三边测量法

当未知节点到至少三个节点的估计距离已知，则可使用三边测量法(trilateration)。三边测量法以三个节点为中心的圆交点作为未知节点的估计位置。

$$\begin{cases} \sqrt{(x-x_1)^2 + (y-y_1)^2} = d_1 \\ \sqrt{(x-x_2)^2 + (y-y_2)^2} = d_2 \\ \sqrt{(x-x_3)^2 + (y-y_3)^2} = d_3 \end{cases}$$

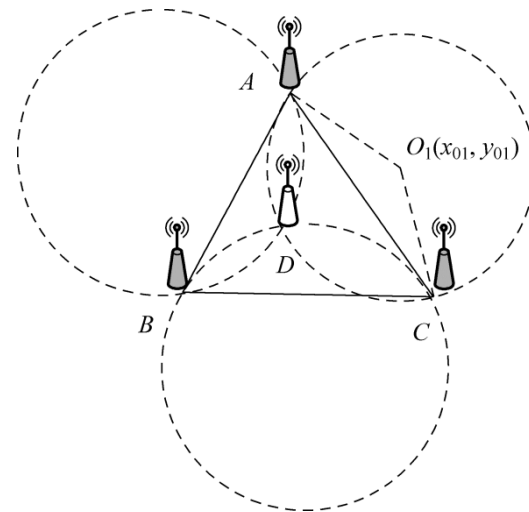


虽然这种方法简单,通常节点间测距误差较大

## 2.三角测量法

三角测量法(triangulation)根据三角形的几何关系进行位置估算。三角测量法首先进行“点在三角形中”的测试，即任意选取三个锚节点组成三角形，以测试未知节点是否落在该三角形内。根据测试结果，如果在三角形内部，就可以采用如下的方法计算节点的位置。

$$\begin{cases} \sqrt{(x_{01} - x_1)^2 + (y_{01} - y_1)^2} = r_1 \\ \sqrt{(x_{01} - x_2)^2 + (y_{01} - y_2)^2} = r_1 \\ (x_1 - x_3)^2 + (y_1 - y_3)^2 = 2r_1^2 - 2r_1^2 \cos \alpha \end{cases}$$



### 3. 极大似然估计法

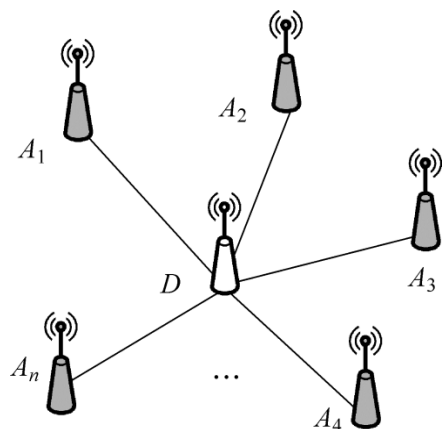
极大似然估计法(multilateration)寻找一个使测距距离与估计距离之间存在最小差异的点，并以该点作为未知节点的位置。

其基本思想为：假如一个节点可以获得足够多的信息来形成一个由多个方程式组成并拥有唯一解的超限制条件或限制条件完整的系统，那么就可以同时定位跨越多跳的一组节点。如图所示。

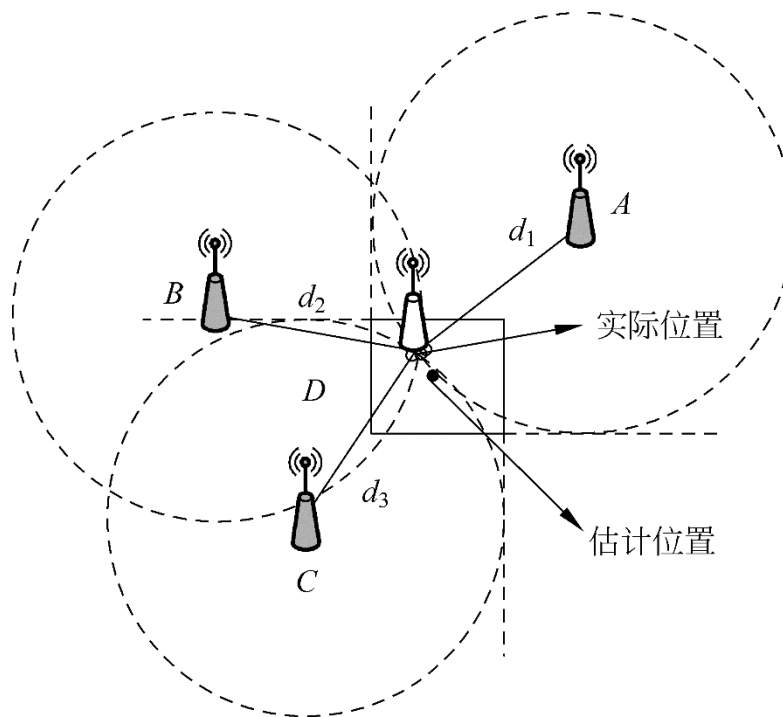
$$\begin{cases} (x_1 - x)^2 + (y_1 - y)^2 = d_1^2 \\ \vdots \\ (x_n - x)^2 + (y_n - y)^2 = d_n^2 \end{cases}$$

将式(5-16)视为线性方程组  $AX=b$ , 解之可得：

$$A = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix}, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}$$
$$b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_n^2 - d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix}$$



## 4.最小最大法



## 5.2.4 距离无关的定位算法

典型的距离无关的定位算法有质心定位算法、凸规划定位算法、APS定位算法、Amorphous定位算法、APIT算法、SeRLOC算法等。

### 1. 质心定位算法

**质心定位算法**首先确定包含未知节点的区域，计算这个区域的质心，并将其作为未知节点的位置。在质心定位算法中，锚节点周期性地向临近节点广播信标分组，信标分组中包含锚节点的标识号和位置信息。当未知节点接收到来自不同锚节点的信标分组数量超过某门限或接收一定时间后，就确定自身位置为这些锚节点所组成的多边形的质心。

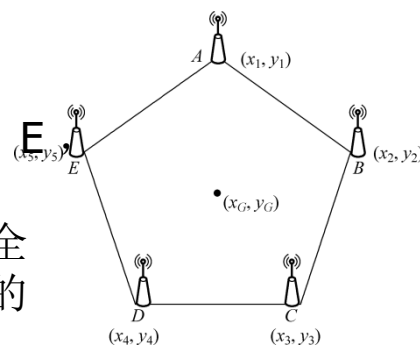
**多边形的几何中心称为质心**，设多边形顶点为  $A_1(x_1, y_1), A_2(x_2, y_2), \dots, A_n(x_n, y_n)$ ，均值就是多边形质心的坐标，

$$(X_G, Y_G) = \left( \frac{\sum_{i=1}^n X_i}{n}, \frac{\sum_{i=1}^n Y_i}{n} \right)$$

例如如图所示的多边形。ABCDE的顶点坐标分别为A, B, C, D, E，其质心坐标为：

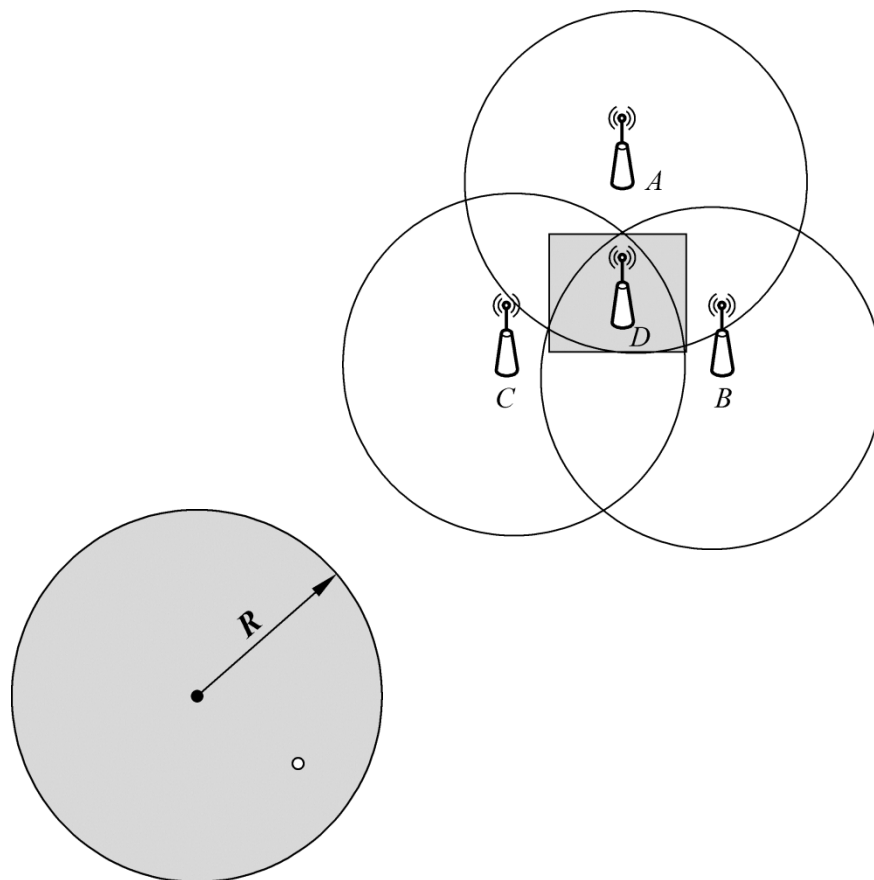
$$(x, y) = \left( \frac{x_1 + x_2 + x_3 + x_4 + x_5}{5}, \frac{y_1 + y_2 + y_3 + y_4 + y_5}{5} \right)$$

质心定位算法的最大优点是无需节点间的协调，但是估计的精确度和锚节点的密度有关，密度越大，定位精度越高。



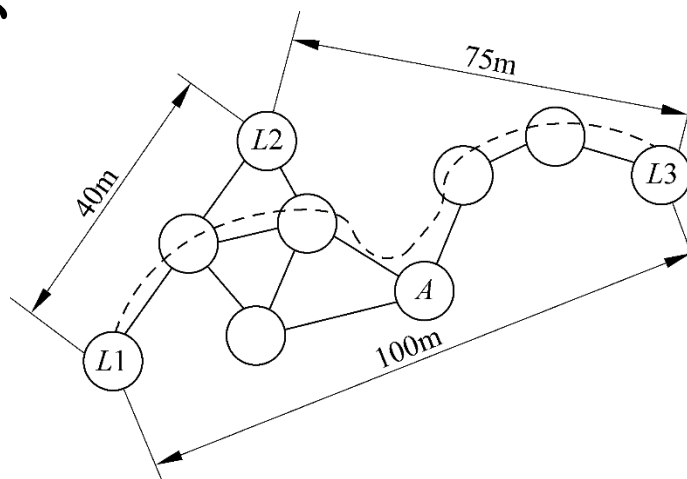
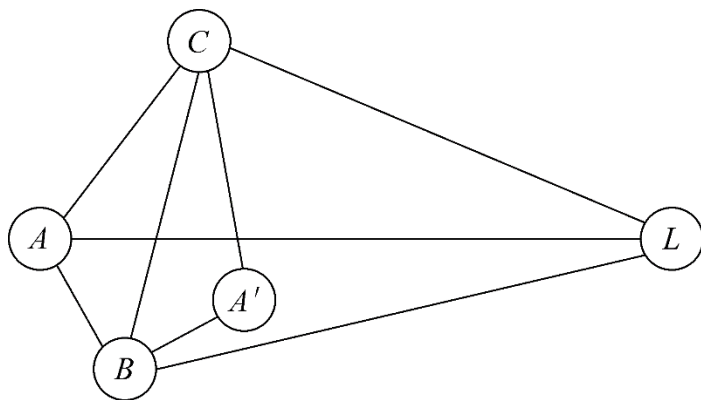


## 2.凸规划定位算法



### 3. APS算法

#### (1)DV-Hop定位算法



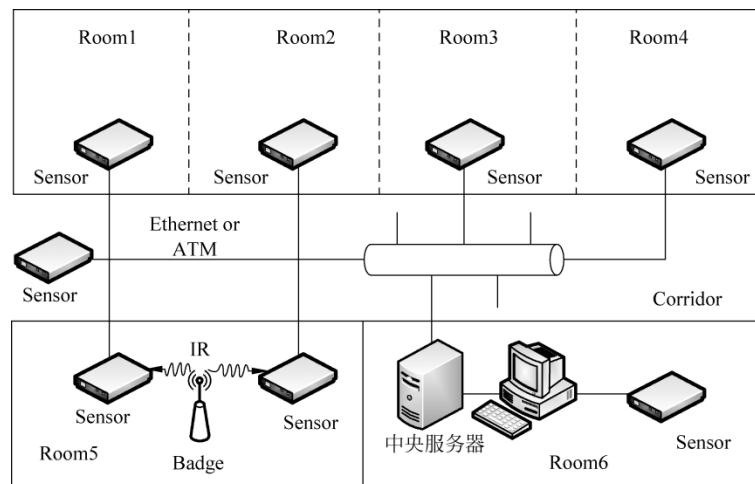


## 5.2.5 典型的定位系统

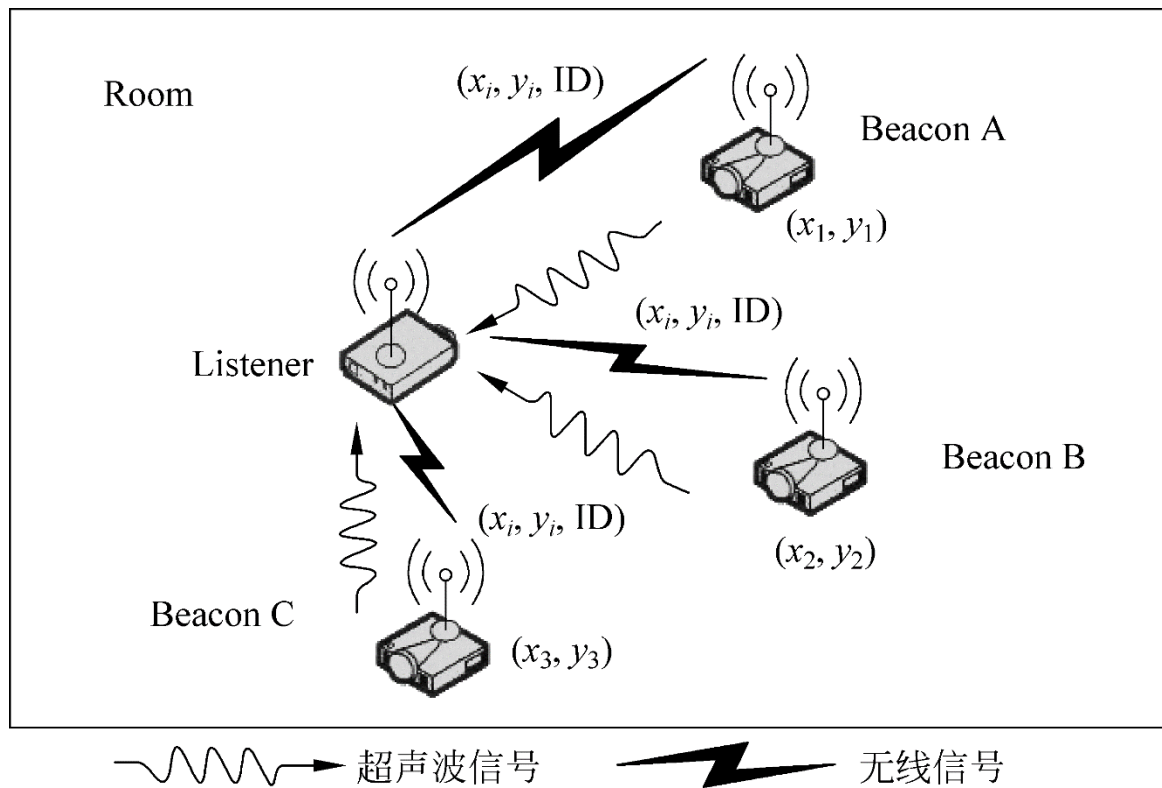
---

面对典型室内定位系统**Active Badge**、**Active Office**、**Cricket**等加以归纳总结。

# 1. Active Office定位系统



## 2. Cricket定位系统



## 5.3 数据融合

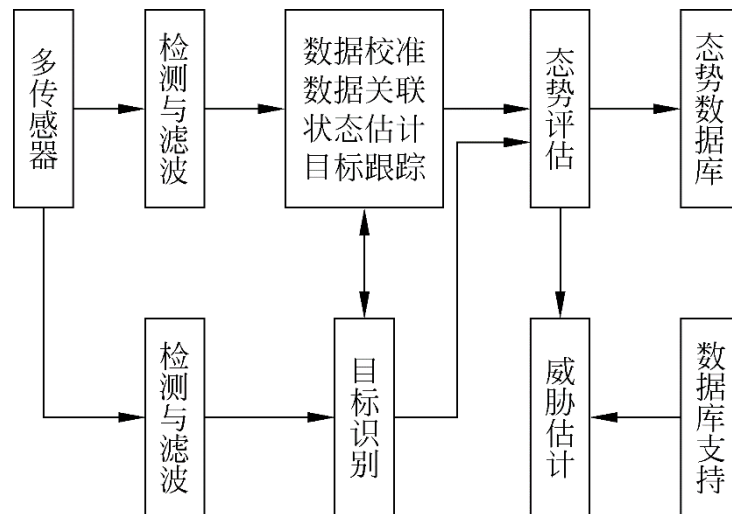
### 5.3.1 数据融合的基本概念

**数据融合**是利用计算机技术对按时序获得的多传感器观测信息在一定的准则下进行多级别、多方面、多层次信息检测、相关估计和综合，以获得目标的状态和特征估计，产生比单一传感器更精确、完整、可靠的信息、更优越的性能，而这种信息是任何单一传感器所无法获得的。

如图所示给出了数据融合的一般处理模型的基本思想。

数据融合技术可以带来的好处有以下六个方面。

- ① 高了信息的可信度。
- ② 扩展系统的空间、时间覆盖能力。
- ③ 减小系统的信息模糊程度。
- ④ 改善系统的检测能力
- ⑤ 提高系统的可靠性
- ⑥ 提高系统决策正确性





## 5.3.2 数据融合技术的分类

根据处理融合信息方法的不同，数据融合系统可分为集中式、分布式和混合式三种。

①集中式:各个传感器的数据都送到融合中心进行融合处理。

②分布式:各个传感器对自己测量的数据单独进行处理，然后将处理结果送到融合中心，由融合中心对各传感器的局部结果进行融合处理。

③混合式:以上两种方式的组合，可以均衡上述两种方式的优缺点，但系统结构同时变得复杂。

根据融合处理的数据种类，数据融合系统可以分为时间融合、空间融合和时空融合。

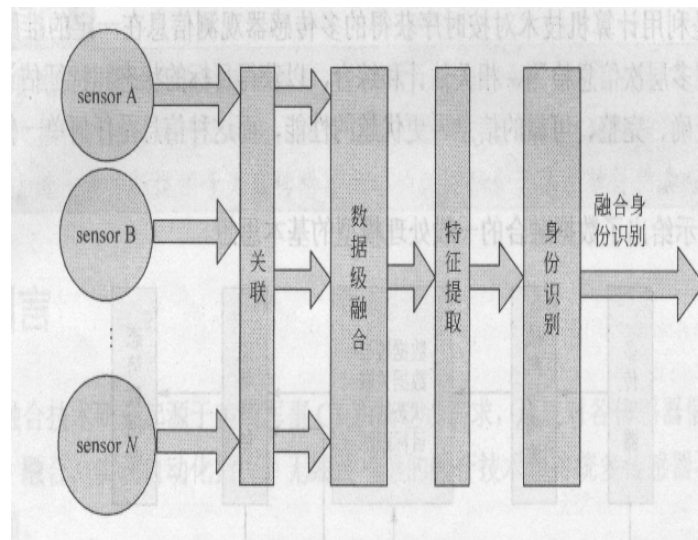
①时间融合:对同一传感器对目标在不同时间的测量值进行融合。

②空间融合:对不同传感器，在同一时刻的测量值进行融合。

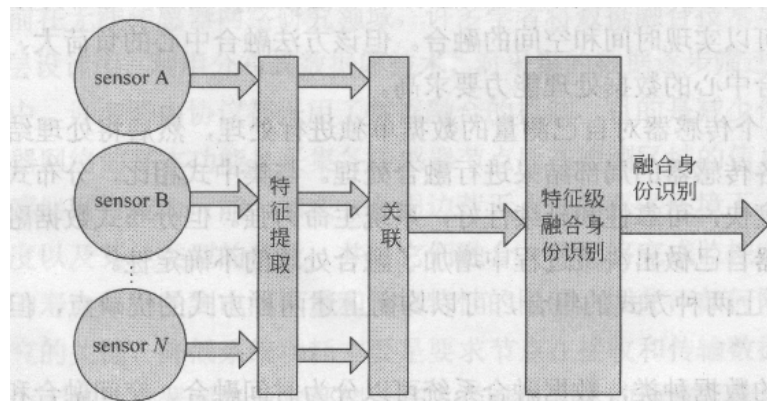
③时空融合:在对不同的传感器，一段时间内的测量值不断地进行融合。

根据信息的**抽象程度**来分，数据融合可分为数据级融合、特征级融合和决策级融合三种。

①数据级融合:如图5-42所示，是直接在采集到的原始数据层上进行的融合，在传感器采集的原始数据未经处理之前就对数据进行分析 and 综合。这是最低层次的数据融合。



②特征级融合:如图5-43所示属于中间层次，它先对来自传感器的原始数据提取特征信息。然后按特征信息对多传感器数据进行分类、汇集和综合。



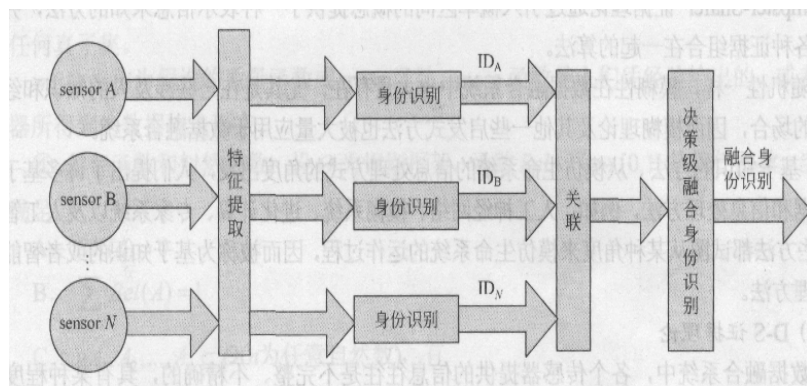


③决策级融合:如图5-44所示,是在最高级层进行的融合。决策级融合是一种高层次融合,融合之前,每种传感器的信号处理装置已完成决策或分类任务。

决策级融合的结果是为决策提供依据,

决策级融合的主要优点有:

- ①具有很高的灵活性;
- ②系统对信息传送的带宽要求较低;
- ③能有效反映环境或目标各个侧面的不同类型信息;
- ④当一个或几个传感器出现错误时,通过适当融合,系统还能获得正确的结果,所以具有容错性;
- ⑤通信量小,抗干扰能力强;
- ⑥对传感器的依赖性小,传感器可以是同质的,也可以是异质的;
- ⑦融合中心处理代价低。





## 5.3.3 常用的数据融合算法

### 1. 数据融合算法类型

①检测和决策理论该理论是通过把被测对象的测量值与被选假设进行比较，以确定哪个假设能最佳地描述观测值。这种方法的代表为贝叶斯概率理论、**Dempster-Shafer (D-S)**证据理论、马尔可夫随机域理论等。

②估计理论一个参数的估计要使用多个观测变量的测量值，而这些观测量又直接与该参量相关。估计理论利用与被估计参数有关的变量的多次观测值对该参数进行估计。代表方法有最小二乘法、最大似然法、维纳滤波、卡尔曼滤波等。

③数据关联技术对于多传感器数据源在进行分类或估计之前，可以将测量值按来源不同分成不同的集合实现数据关联。常用的关联技术包括匹配滤波器、卡尔曼滤波器等。

④不确定性管理系统复杂性的增加不可避免地导致各种不确定因素的产生。

贝叶斯概率模型是最常用的描述测量(证据)不确定性的方法，它用概率来表示假设(或命题)的置信度。

**Dempster-Shafer**证据理论通过引入概率区间的概念提供了一种表示信息未知的方法，并给出了将各种证据组合在一起的算法。

⑤基于知识的方法从模仿生命系统的信息处理方式的角度出发，人们提出了许多基于知识的数据和信息处理方法，例如：人工神经网络、模糊系统、进化计算、专家系统以及人工智能等。



## 2 D-S证据推理法

D-S证据理论是不确定性推理的一种重要方法。

①证据理论基础不确定性推理是处理那些具有不完全、不确定、不清晰的信息或数据的基础，是目标识别和属性信息融合的基础。

②识别框架

③概率分配

④信任函数和似然函数，

⑤D-S合成规则

$l_1, l_2, \dots, l_n$   
其算术平均值为:

### 3 算术平均数据融合方法

在相同的观测条件下，对某量进行多次重复观测，根据偶然误差特性，可取其算术平均值作为最终观测结果。设对某量进行了 $n$ 次等精度观测，观测值分别为：

$$L = \frac{l_1, l_2, \dots, l_n}{n}$$

设观测量的真值为 $X$ ，观测值为 $l_i$ ，则观测值的真误差为：

$$\begin{cases} \Delta_1 = l_1 - X \\ \Delta_2 = l_2 - X \\ \vdots \\ \Delta_n = l_n - X \end{cases}$$

将上式内各式两边相加，并除以 $n$ ，得：

$$\frac{\Delta_1 + \Delta_2 + \dots + \Delta_n}{n} = X - \frac{l_1, l_2, \dots, l_n}{n}$$

进一步可得：

$$L = X + \frac{\Delta_1 + \Delta_2 + \dots + \Delta_n}{n}$$

根据偶然误差的特性，当观测次数 $n$ 无限增大时，则有  
那么同时可得：

$$\lim_{n \rightarrow \infty} \frac{\Delta_1 + \Delta_2 + \dots + \Delta_n}{n} = 0, \vdots$$

$$\lim_{n \rightarrow \infty} L = X$$

由上式可知，当观测次数 $n$ 无限增大时，算术平均值趋近于真值。  
但在实际测量工作中，观测次数总是有限的，因此，  
算术平均值较观测值更接近于真值。



## 5.4 能量管理

### 5.4.1 能量管理的意义

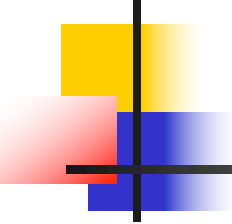
传感器网络存在着能量约束问题，它的一个重要设计目标就是高效使用传感器结点的能量，在完成应用要求任务的前提下，尽量延长整个网络系统的生存期。

(1)传感器结点采用电池供电，

(2)传感器结点中消耗能量的模块，

(3)网络协议控制了传感器网络各结点之间的通信机制，决定无线通信模块的工作过程。

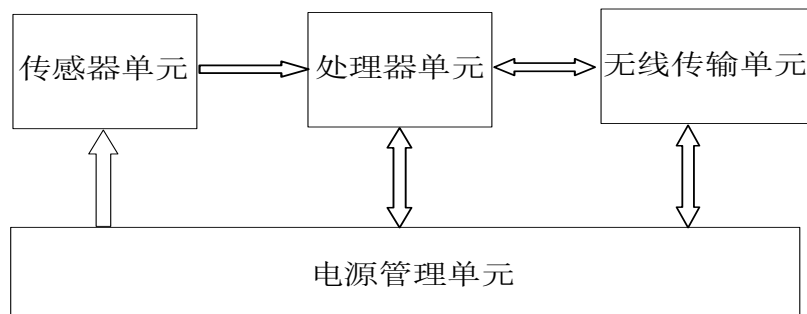
(4)无线传感器网络的能量管理(**Energy Management, EM**)主要体现在传感器结点电源管理(**Power Management, PM**)和有效的节能通信协议设计。



传感器节点通常由四个部分组成：处理器单元、无线传输单元、传感器单元和电源管理单元。其中传感器单元能耗与应用特征相关，采样周期越短、采样精度越高，则传感器单元的能耗越大。

由于传感器单元的能耗要比处理器单元和无线传输单元的能耗低得多，几乎可以忽略，因此通常只讨论处理器单元和无线传输单元的能耗问题。

- (1) 处理器单元能耗；
- (2) 无线传输能耗。





## 5.4.2 电源节能方法

---

目前人们采用的节能策略主要有**休眠机制**、**数据融合**等，它们应用在计算单元和通信单元的各个环节。

### 1、休眠机制

**休眠机制**的主要思想是，当节点周围没有感兴趣的事件发生时，计算与通信单元处于空闲状态，把这些组件**关掉或调到更低能耗**的状态，即休眠状态。



## (1) 硬件支持

现有的无线收发器也支持休眠，而且可以通过唤醒装置唤醒休眠中的节点，从而实现在全负载周期运行时的低能耗。

无线收发器有四种操作模式：发送、接收、空闲和休眠。

表4-1给出了一种无线收发器的能耗都很大，空闲状态的能耗接近于接收状态能耗情况，除了休眠状态外，其他三种状态的，所以如果传感器节点不再收发数据时，最好把无线收发器关掉或进入休眠状态以降低能耗。

表4-1 无线收发器各个状态的能耗

无线收发器状态	能耗/mW
发送	14.88
接收	12.50
空闲	12.36
睡眠	0.016





## (2)采用休眠机制的网络协议

通常无线传感器网络的MAC协议都采用**休眠机制**，例如**S-MAC**协议。在**S-MAC**协议中，在数据发送时，如果结点既不是数据的发送者，也不是数据的接收者，就**转入休眠状态**，在醒来后有数据发送就**竞争**无线信道，无数据发送就侦听其是否为下一个数据接收者。S-MAC协议通过建立周期性的**侦听**和**休眠机制**，减少侦听时间，从而实现节能。



### (3) 专门的节点功率管理机制

#### ① 动态电源管理

动态电源管理(DPM)的工作原理是, 当节点周围没有感兴趣的事件发生时, 部分模块处于空闲状态, 应该把这些组件关掉或调到更低能耗的状态(即休眠状态), 从而节省能量。

这种事件驱动式能量管理对于延长传感器节点的生存期十分必要。在动态电源管理中, 由于状态转换需要消耗一定的能量, 并且带有时延, 所以状态转换策略非常重要。如果状态转换过程的策略不合适, 不仅无法节能, 反而会导致能耗的增加。



## ②动态电压调度

对于大多数传感器节点来说，计算负荷的大小是随时间变化的，因而并不需要节点的微处理器在所有时刻都保持**峰值**性能。

根据**CMOS**电路设计的理论，微处理器执行单条指令所消耗的能量 $E_{op}$ 与工作电压**V**的平方成正比，即： $E_{op} \propto V^2$ 。

动态电压调节(DVS)技术就是利用了这一特点，**动态改变微处理器的工作电压和频率**，使得刚好满足当时的运行需求，从而在性能和功耗之间取得平稳。

动态电压调节要解决的**核心问题**是实现微处理器**计算负荷**与**工作电压及频率**之间的匹配。



## 2、数据融合

数据融合的**节能效果**主要体现在路由协议的实现上。路由过程的**中间节点**并不是简单的转发所收到的数据，由于同一区域内的节点发送的数据具有很大的**冗余性**，中间节点需要对这些数据进行数据融合，将经过本地融合处理后的数据路由到**汇聚点**，只转发**有用**的信息。数据融合有效地降低了整个网络的**数据流量**。

**LEACH**路由协议就具有这种功能，它是一种自组织的在节点之间随机分布能量负载的**分层路由**协议。



## 5.4.3 动态能量管理

### 1. 空闲能量管理

#### (1) 多种关闭状态

具有多种能量模式的设备有很多，例如，Strong ARM SA-1100处理器有3种能量模式：“运行”、“空闲”和“睡眠”。每种模式对应于较低水平的耗能情况。

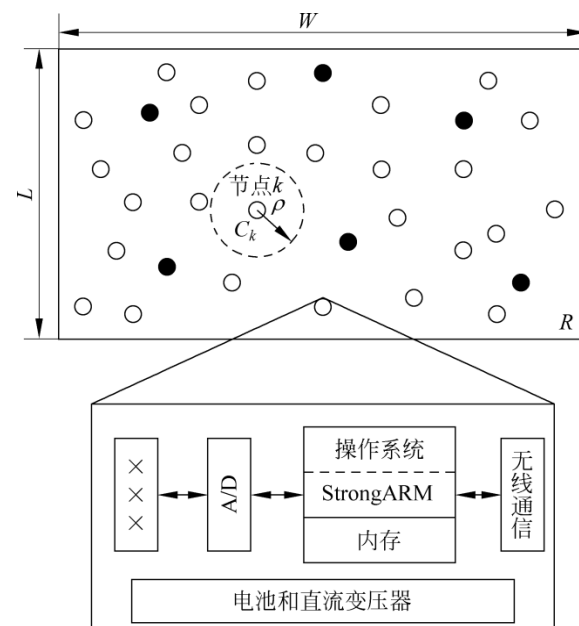
**运行模式**是处理器的一般工作模式，所有能量供应激活，所有时钟均运行，且所有资源均工作。

**空闲模式**允许软件暂停未使用的CPU，而继续侦听中断服务请求。CPU时钟停止，并保存所有处理器的相关指令。中断产生时，处理器返回运行模式，并继续从暂停点开始工作。

**睡眠状态**节省的能量最多，提供的功能最少，大部分电路的能量供应被切断，睡眠状态守候预排程序的唤醒事件，这与蓝牙无线装置中的4种不同的能耗模式：“激活”、“保持”、“嗅探”和“暂停”相类似。

## (2) 传感节点的构成

如图表示基本传感节点的构成。各节点由嵌入式、传感器、A/D转换器，带有存储器的处理器(此情形下为StrongARM SA-11x0处理器)，以及RF电路组成。每个部分通过基本设备驱动受OS控制。OS的一个重要功能是能量管理(PM, Power Management)。OS根据事件统计情况决定设备的开启和关闭。传感网络由分布在矩形区域  $R$  上的类传感节点组成，区域尺寸为，各节点可见度半径为  $p$ 。





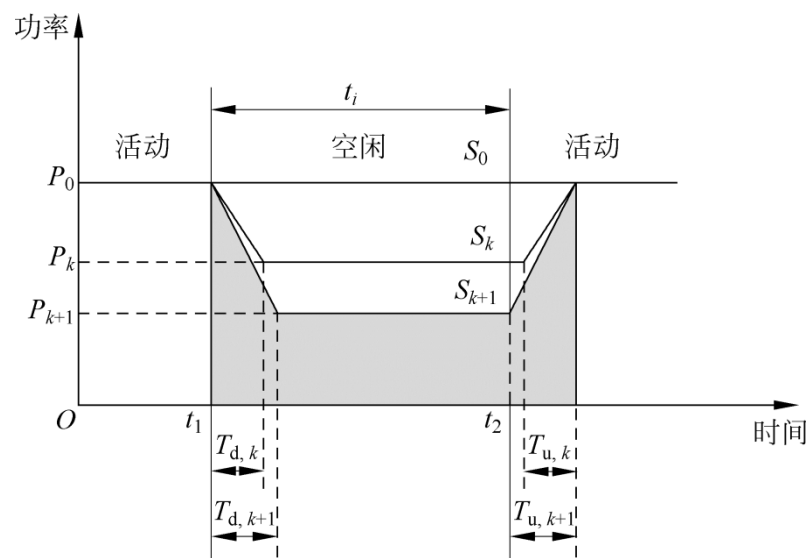
对于传感节点，表4-2列举了与5种不同的有用睡眠状态相关的各部分能量模式。

表 4-2 传感节点有用睡眠状态


状态	StrongARM	存储器	传感器, A/D	无线电
S <sub>0</sub>	激活	激活	开	发送, 接收
S <sub>1</sub>	空闲	睡眠	开	接收
S <sub>2</sub>	睡眠	睡眠	开	接收
S <sub>3</sub>	睡眠	睡眠	开	关
S <sub>4</sub>	睡眠	睡眠	关	关

### (3) 睡眠状态转换策略

假设传感节点在某时刻 探测到一个事件，在时刻 结束处理，下一事件在时刻 发生，在时刻 ，节点决定从激活状态 转换到睡眠状态 ，如图所示。各状态 的能耗为 ，而且 转换到此状态和恢复时间分别为 和 。假设节点睡眠状态中，对于任意  $i > j$ ， $P_i > P_j$ ， $t_{i,j} > t_{j,i}$ ，且，睡眠模式间的能耗可采用状态间线性变化的模型。

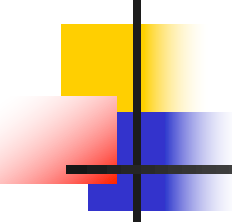






各节点睡眠模式对应于越来越深的睡眠状态，因而其特征描述为渐增的延迟和渐减的能耗。需要根据传感节点的工作条件选择这些睡眠状态，例如，在激活状态中关闭存储器，或关闭其他任何部分是没有意义的：

- ①状态  $s_1$  是节点的完全激活状态，节点可传感、处理、发送和接收数据；
- ②状态  $s_2$  中，节点处于传感和接收模式，而处理器处于待命状态；
- ③状态  $s_3$  与状态  $s_2$  类似，不同点在于处理器断电，当传感器或无线电接收到数据时会被唤醒；
- ④状态  $s_4$  是仅传感的模式，其中除了传感前端外均关闭；
- ⑤状态  $s_5$  表示设备的全关闭的状态。



现在获得一组与状态  $\{S_k\}$  相应的睡眠时间 **阈值**  $\{T_{th,k}\}$ 。若空闲时间  $t_i > T_{th,k}$ ，由于存在转换能量管理花费，从状态  $S_k$  转换到睡眠状态  $S_0$  将造成网络能量损失。假设在转换阶段无需完成其他工作(例如当处理器醒来时，转换时间包括 **PLL** 锁定、时钟稳定和处理器相关指令恢复的时间)。上图中，图线下方区域表示状态转换节省的能量，可用下式计算：

$$E_{save,k} = (P_0 - P_k)t_i - \left(\frac{P_0 - P_k}{2}\right)\tau_{d,k} - \left(\frac{P_0 + P_k}{2}\right)\tau_{u,k}$$

仅当  $E_{save,k} > 0$  时这种转换是合理的。于是，可得到下面的

$$T_{th,k} = \frac{1}{2} \left[ \tau_{d,k} + \left( \frac{P_0 + P_k}{P_0 - P_k} \right) \tau_{u,k} \right]$$

这意味着转换的延迟花费越**大**，能量增益**阈值**越**高**，而且  $P_0$  与  $P_k$  间的区别越**大**，**阈值**越**小**。

表4-3列出了上图所描述传感节点的能耗，说明了现有组件在不同能量模式下相应的能量增益阈值。由此可见，阈值处于微秒量级。OS关闭策略以事件执行间隔统计和能量增益阈值为基础，可视为一个优化问题。若事件采用泊松过程模型，时刻至少发生一个事件的概率可由下式获得：

$$P_E(t) = 1 - e^{-\lambda_i t}$$

此时，采用简单算法更新每单位时间的平均事件数，计算阈值内的事件发生概率  $\{T_{th}, k\}$  并根据有效的最小概率阈值选择最深的睡眠状态。

表 4-3 睡眠状态能量、延迟和阈值

状态	$P_k/\text{mW}$	$\tau_k/\text{ms}$	$T_{th,k}$		状态	$P_k/\text{mW}$	$\tau_k/\text{ms}$	$T_{th,k}$
$s_0$	1040	—	—	↕	$s_3$	200	20	25
$s_1$	400	5	5		$s_4$	10	50	50
$s_2$	270	15	15					

## 4. 动态能量管理实验

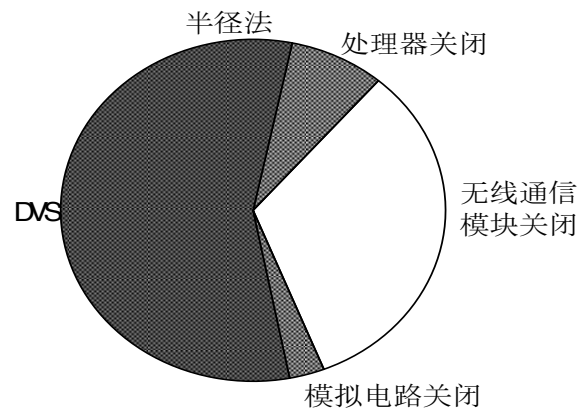
表4-4列出了测得的各种工作模式下传感节点的能耗。

表 4-4 各种传感器工作模式的能耗

	系统模式	成分模式			功率/mW
		处理器	无线电	模拟	
激活状态	激活	最高频率	开	开	975.6
	弱激活	最低频率	开	开	457.2
	空闲	空闲	开	开	443.0
睡眠状态	接收	空闲	开	关	403.0
	传感	空闲	关	关	103.0
	睡眠	睡眠	关	关	28.0



下图表示传感节点电池寿命采用能量管理技术而获得提高的因子，这里电池寿命是工作量和周期需求的函数。





## 5.5容错技术

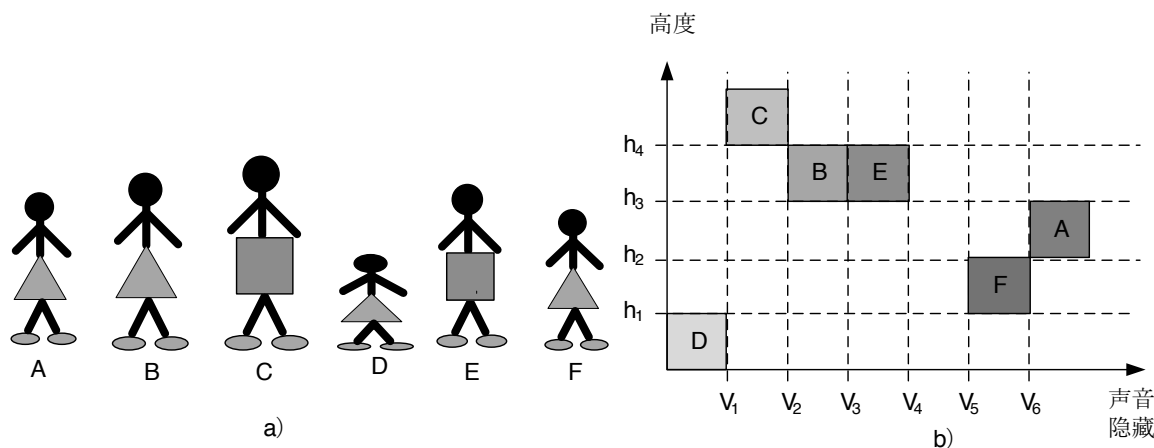
---

### 5.5.1概述

容错领域有几个基本概念：失效(failure)、故障(fault)、差错(error)。

失效是指某个设备中止了它完成所要求功能的能力。故障是指一个设备、元件或组件的一种物理状态，在此状态下它们不能按照所要求的方式工作。差错是指一个不正确的步骤、过程或结果。故障只有在某些条件下才能在其输出端产生差错，这些差错由于在系统内部，不是很容易就能观测到。只有这种差错积累到一定程度或者在某种系统环境下，才能使系统失效。所以，失效是面向用户的，而故障和差错是面向制造和维修的。

无线传感器网络**容错**是指网络中某个节点或节点的某些部件发生故障时，网络仍然能够完成指定的任务。容错的要求在不同的应用中有所不同。例如，一个办公室有六个人，分别标记为**A**、**B**、**C**、**D**、**E**、**F**。在办公室门口布设一个无线传感器网络，要求能识别出这六个人。





## 2. 容错的重要性

---

无线传感器网络的出现给容错设计技术带来了新的挑战，因为无线传感器网络需要考虑如下情况：

(1)技术和实现因素。

(2)无线传感器网络的应用模式。

(3)无线传感器网络是一个新兴的研究和工程领域，处理特定问题的最优方法还不明确。



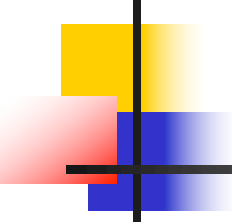
## 5.5.2故障模型

无线传感器网络容错设计需要考虑三个方面：**故障模型、故障检测与诊断、修复机制。**

从整体上考虑，无线传感器网络中的故障可以分为**三个层面**，即**部件级、节点级和网络级**，如表4-5所示。由于**网络、节点、部件**间的包含关系，所以**高层故障本质**也是由**低层故障**所造成。

表 4-5 故障模型的层次

故障级别	故障表征	故障检测	修复机制
部件	故障节点能够正常通信，但是测量数据是错误的	检测出错误的测量数据	舍弃或校正出错的测量数据
节点	故障节点不能与其他节点进行通信	通过询问或重新路由等方法检测故障节点	通过移动冗余节点弥补形成的连接和覆盖问题



设某个节点所在地的真实值为  $\gamma(t)$ ，记测量误差符合正态分布  $N(0, \sigma^2)$ 。

传感器发生故障时，测量值将可以形式化为  $f(t) = \beta_0(t) + \beta_1\gamma(t) + \varepsilon(t)$ ，其中  $\beta_0$  是偏移值， $\beta_1$  是缩放倍数， $\varepsilon$  是测量噪声，由此可以得到下面几种故障模型：

### 故障模型：

- (1) 固定故障, 它可以形式化为  $f(t) = \beta_0(t)$
- (2) 偏移故障, 形式化为  $f(t) = \beta_0(t) + \gamma(t) + \varepsilon(t)$
- (3) 倍数故障, 形式化为  $f(t) = \beta_1\gamma(t) + \varepsilon(t)$
- (4) 方差下降故障, 形式化为  $f(t) = \gamma(t) + \varepsilon(t)$



## 5.5.3故障检测与诊断

故障检测的**目标**是检测网络中的异常行为。故障检测分为部件检测和节点检测。

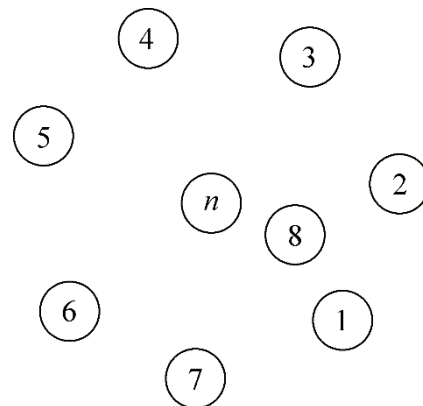
### 1. 部件故障检测

#### (1) 基于**空间相关性的故障检测**

无线传感器网络相邻节点的同类传感器所测量的值通常很相近，称这种特性为**空间相关性**。一个节点通过周围邻居的同类传感器来检测自己的传感器是否发生了故障。根据故障检测时是否需要节点地理位置信息，**可以分为如下两类**：①需要地理位置信息；②不需要地理位置信息

## ①需要地理位置信息

某节点的传感器测量到的结果与周围节点测量到的结果都不相同时，这个节点的传感部件很可能发生了故障。如图5-57所示，节点1～节点8都感应到事件的发生，而节点n没有感应到事件的发生，则认为节点n的传感部件发生了故障。如果节点n及节点1～节点7都感应到事件，则可以判断节点8的传感部件发生了故障。



## ②不需要地理位置信息

- 无线传感器网络中的**正常节点**都能侦听到**邻居发送的消息**。节点可以依据侦听到的邻居数据来**判断自己**测量值是否正确，判断策略可以分为多数投票策略、均值策略和中值策略。
- 设节点  $n_i$  有  $N$  个邻居，邻居测量值分别为  $x_j$  ( $j=1,2,3,\dots,N$ )。判断  $n_i$  的测量值  $x_i$  是否正确的三种策略的详细步骤如表4-8所示。

表 4-8 三种故障检测策略

多数投票策略
1. 得到节点 $n_i$ 的邻居测量值 $x_j$ ( $j=1, 2, \dots, N$ )
2. 比较 $x_i$ 与 $x_j$ ( $j=1, 2, \dots, N$ )，得到与 $x_i$ 相同或在允许差距范围内的 $x_j$ 的个数 $k_i$
3. 如果 $k_i \geq 0.5N$ ，则 $x_i$ 正确；否则 $x_i$ 错误

表 4-9 判断策略比较

+

	识别率	误报率	时间复杂度
多数投票	较高	低	$O(n)$
均值	较高	较低	$O(n)$
中值	高	低	$O(n \log n)$

均值策略
1. 得到节点 $n_i$ 的邻居测量值 $x_j$ ( $j=1, 2, \dots, N$ )
2. 计算出邻居读数的均值 $\bar{x}_i = \frac{\sum_{j=1}^N x_j}{N}$
3. 自身测量值与上述均值比较 $f(x_i, \bar{x}_i) = \begin{cases} 1, & \left  \frac{x_i - \bar{x}_i}{\bar{x}_i} \right  > \xi \\ 0, & \text{其他} \end{cases}$
4. 若 $f(x_i, \bar{x}_i)$ 值为 1，则认为这次测量值有误
中值策略
1. 得到节点 $n_i$ 的邻居测量值 $x_j$ ( $j=1, 2, \dots, N$ )
2. 计算出邻居测量值的中值 $\tilde{x}_i = \text{MED} \left\{ x_j \mid \begin{matrix} N \\ j=1 \end{matrix} \right\}$ ，MED 为求中值的运算
3. 自身测量值与上述中值比较 $f(x_i, \tilde{x}_i) = \begin{cases} 1, & \left  \frac{x_i - \tilde{x}_i}{\tilde{x}_i} \right  > \xi \\ 0, & \text{其他} \end{cases}$
4. 若 $f(x_i, \tilde{x}_i)$ 值为 1，则认为这次测量值有误

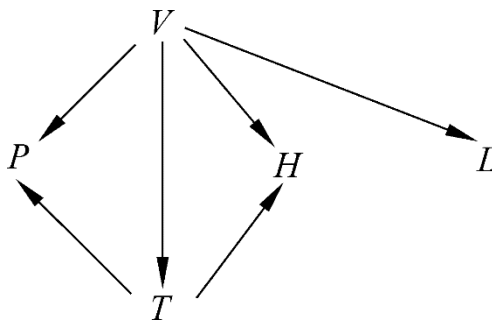
## (2) 基于贝叶斯信任网络故障检测

贝叶斯信任网络包含一个有向图和与之对应的概率表集合。有向图中的顶点表示变量，边表示变量之间的影响关系。贝叶斯信任网络的关键特征是能够模型化并推理出不确定因素。模型化节点间的可靠关系是通过节点概率表实现。

应用贝叶斯信任网络分为构造、学习、推理三个阶段。在构造阶段需要得到所有变量的联合概率分布。

以大鸭岛实验情景来应用贝叶斯信任网络实现传感部件的故障检测。

环境监测中有五个属性：温度(T)、相对湿度(H)、气压(P)、光照强度(L)、节点电压(V)。它们的关系如图4-23所示：气压和相对湿度受温度影响，而电压影响了所有其他属性。





## 2. 节点故障检测

根据检测过程是否集中进行，节点故障检测可分为集中式和分布式两种。

### (1) 集中式故障检测

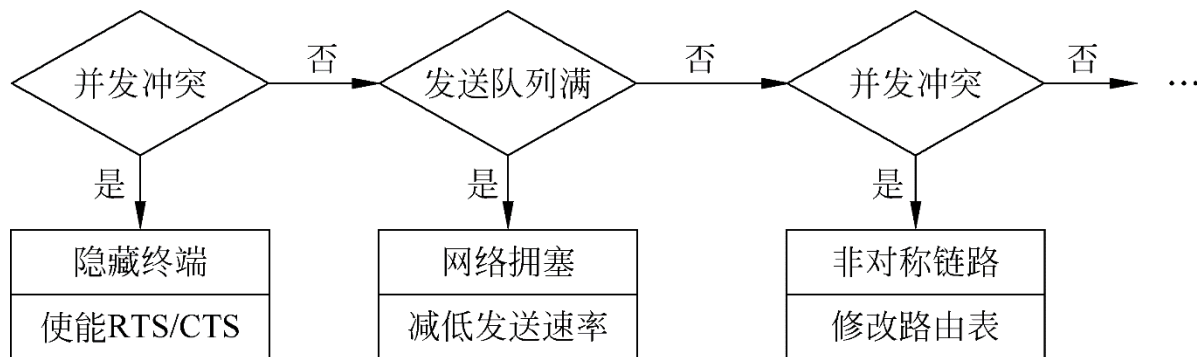
集中式的故障检测通过在Sink节点放置检测程序，实时监测网络状态。Sink节点需要收集的内容如表4-6所示。

表 4-6 需要收集的信息

名称	描述
邻居列表	由邻居 ID 号组成的一个列表
链路质量	用 0（100%丢失）至 100（100%传送）间的一个数来表示
字节数	节点传输和收到的字节数
下一跳（路由表）	路由的下一跳节点
路径丢失（路由表）	从节点到 Sink 节点的链路质量的一种衡量

## (2) 分布式故障检测

分布式故障检测不是由Sink节点统一检测，而是由每个节点分别自行检测。隐藏终端(hidden terminals)、拥塞、链路不对称是几种常见的节点通信故障。





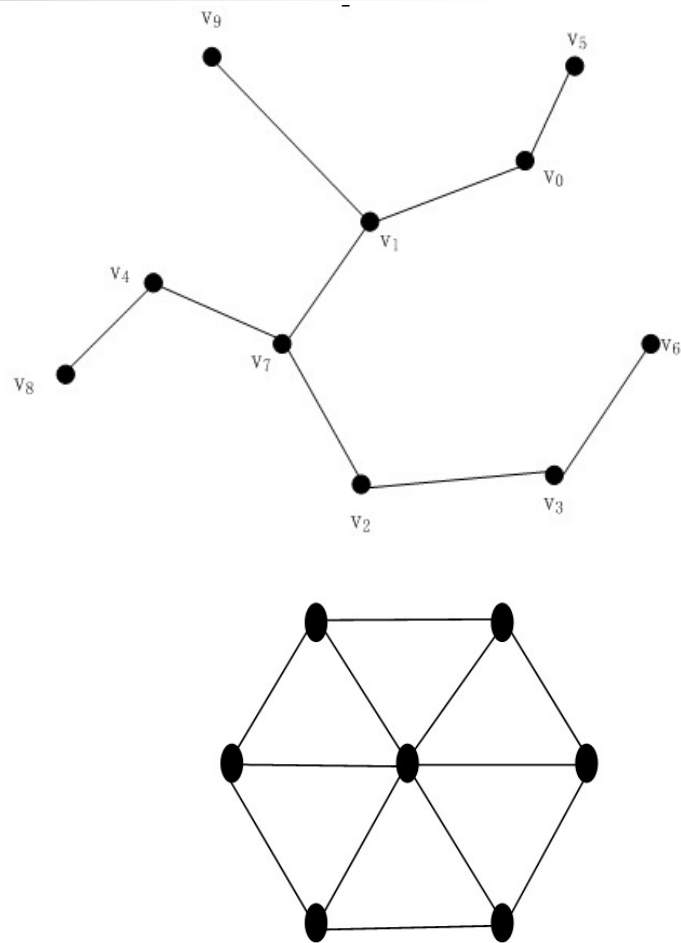
## 5.5.4故障修复

### 1. 基于连接的修复

#### (1) 部署 $k$ 连通拓扑

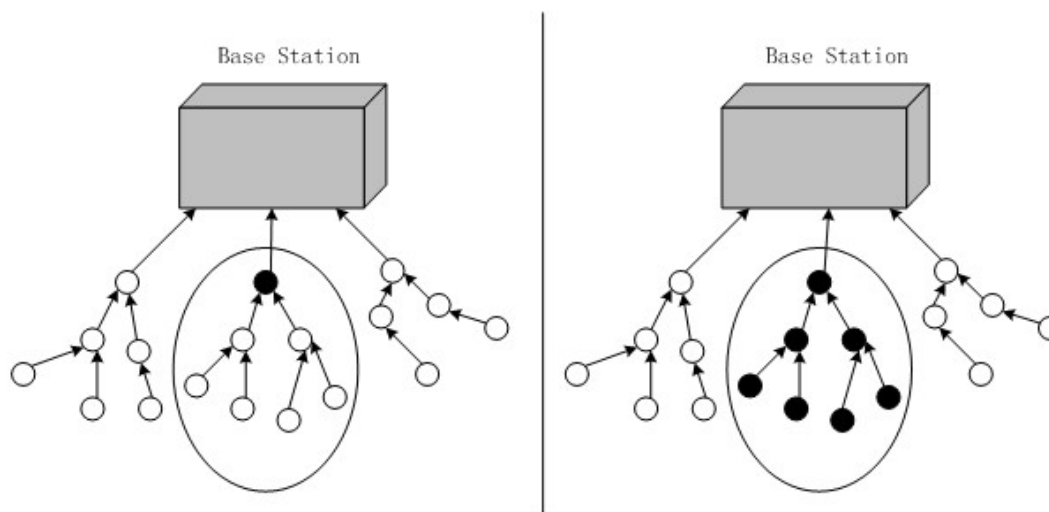
如图如果  $V_1$  或者  $V_7$  发生故障，网络就被划分成3个独立部分。

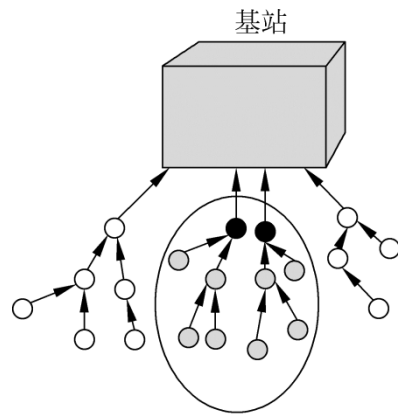
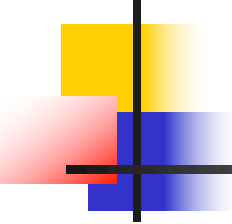
一种建立容错拓扑的方法是构造 $k$ 连通图。 $k$ 连通网络是指网络中任意两点之间都至少有 $k$ 条不相交的路径， $k$ 连通网络中任意 $k-1$ 个节点发生故障时网络仍然保持连通。图4-26是3连通图，它能容忍任意2个节点的故障而保持网络的连通性。



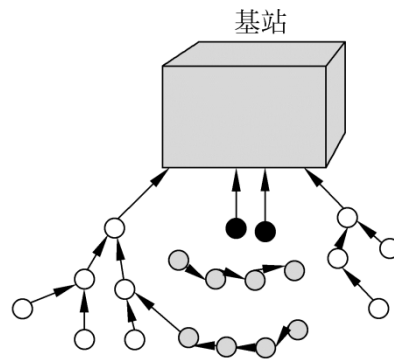
## (2) 非k连通图

如图所示，一个节点或一片节点发生故障时，**基站**将不能收到它们的消息。

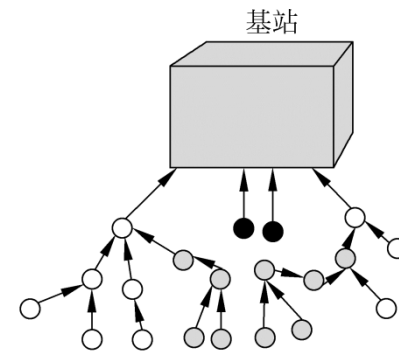




(a) 初始路由拓扑



(b) 最佳路由邻居

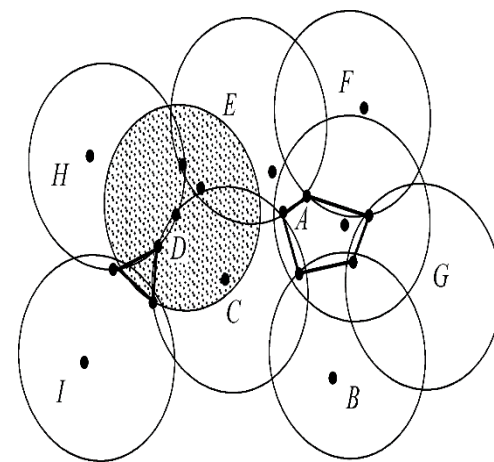


(c) 最佳基站邻居

## 2. 基于覆盖的修复

假设网络中的节点具有**移动能力**，它把覆盖修复过程分为四个阶段：

- (1)**初始化阶段**：节点计算自己的覆盖区域、每个覆盖区域对应的移动区域；
- (2)**恐慌请求阶段**：垂死节点广播求助消息；
- (3)**恐慌回应阶段**：垂死节点的邻居收到求助消息后计算如果自己移动到垂死节点的移动区域，是否会影响到自身的覆盖区域，如果不影响则给求助节点返回消息；
- (4)**决策阶段**：垂死节点根据收到的回应信息，决定让哪个节点移动。





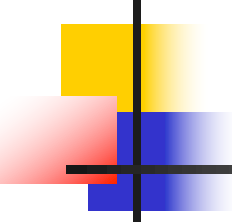
## 5.6 QoS保证

---

### 5.6.1 QoS概述

#### 1. 服务质量(QoS)定义

目前网络界针对如何定义网络QoS并没有一个统一的标准。QoS论坛将QoS定义为网络元素(包括应用、主机或路由器等网络设备)对网络数据的传输承诺的服务保证级别。RFC2386则将QoS看作为网络在从源节点到目的节点传输分组流时需要满足的一系列服务要求。同样在网络分层模型中,不同的层对QoS也有不同的解释。



在应用层，QoS通常是指用户或者应用所获取具体业务的服务质量。而在网络层，QoS则定义为对网络提供给应用及用户的服务质量的度量，网络提供特定QoS的能力依赖于网络自身及其采用的网络协议的特性。

在网络QoS研究中，人们比较关注的服务质量标准主要包括：可用性、吞吐量、时延、时延变化和丢包率等几个参数。



## 2. 服务质量(QoS)支持机制

---

(1) In-tserv 集成业务

(2) Diffserv 区分业务

(3) MPLS 多协议标签交换



## 5.6.2 QoS研究

---

如何合理、有效地利用无线网络的资源，以获取更好的数据传输性能，进而为多媒体业务的服务质量提供保障，是无线自组织网络QoS研究中需要解决的首要问题。

Holger Karl将当前无线传感器网络中的QoS研究总结为三类：

- ①传统端到端QoS支持研究：针对实时性无线传感器网络应用，提供延迟服务保证；
- ②可靠性保证：保证数据包传输的可靠性；
- ③应用相关QoS：包括传感覆盖和如何控制网络活动节点数量等问题。





---

在目前大多数无线传感器网络应用中，人们关注较多的主要有两个问题：

- ① 如何保证网络能够及时可靠地发现所实施应用中相关事件的发生；
- ② 如何保证采集的传感数据在网络中传输时满足应用需求。

这两个问题可以归结为感知服务质量 (传感覆盖) 和网络传输服务质量。



## 5.7 安全性

---

- 5.7.1 WSN安全威胁模型
  - 传感器网络的攻击分成以下几类：
    - ①外部攻击与内部攻击：
    - ②被动攻击与主动攻击：
    - ③传感器类攻击与微型计算机类攻击



## 5.7.2 WSN安全要求

---

- WSN安全服务的目标就是防止信息和网络资源受到攻击和发生异常。
  - 1.数据机密性
  - 2. 数据完整性
  - 3. 数据新鲜度
  - 4. 认证
  - 5.可用性
  - 6.自组织
  - 7. 时间同步
  - 8. 安全定位
  - 9. 其他安全要求



## 7.2 WSN中的安全攻击

- WSN易受各种攻击，根据WSN的安全要求，对WSN的攻击归类如下：
  - ①对秘密和认证的攻击，标准加密技术能够保护通信信道的秘密和认证，使其免受外部攻击(比如偷听、分组重放攻击、分组篡改、分组哄骗)；
  - ②对网络有效性的攻击，对网络有效性的攻击常常称为拒绝服务(Denial of Service, DoS)攻击，可以针对传感器网络任意协议层进行DoS攻击；对服务完整性的秘密攻击：在秘密攻击中，攻击者的目的是使传感器网络接收虚假数据，
- 1.物理层安全攻击
  - 1)人为干扰
  - 2)物理篡改



## 2. 链路层安全攻击

---

- 1)碰撞
- 2)能量消耗
- 3)不公平性
  
- 3. 对WSN网络层(路由)的攻击
- 1)对路由信息的哄骗、篡改、重放
- 2)选择性转发
- 3)污水池攻击 (sinkhole)
- 4)女巫攻击 (Sybil)
- 5)虫洞攻击
- 6)hello泛洪攻击
- 7)确认哄骗



## 4. 对传输层的攻击

---

- 1) 泛洪
- 2) 去同步



end