下一代互联网技术

第四章　物联网技术及应用

本章参考教材

- 《物联网导论》，刘云浩，科学出版社，ISBN 978-7-03-029253-7

检索 978-7-03-029253-7　返回1个结果

[图书] 物联网导论

作 者：　刘云浩编著

出 版 社：科学出版社 2011

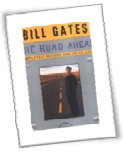
I S B N：978-7-03-029253-7

摘 要：　本书从物联网的感知识别、P

萦绕在物联网这个概念的重重迷雾,引领

物联网思想的起源

- 物联网的理念最早可以追溯到1991年，英国剑桥大学特洛伊计算机实验室的“咖啡壶”。
- 1995年， Bill Gates 的《未来之路》，预测了整个科技产业未来的走势，书中提到了“ 物物互联”的构想
  - 数字音乐、定制广告业务、网上支付、电子钱包、移动支付、电子地图、失物自动发送定位信息等



物联网思想的起源

- 1998年，英国人Kevin Ashton在宝洁公司的一次演讲中首次提出使用RFID（射频识别技术）取代商品条形码，使电子标签成为零售商品的信息发射器，并由此实现供应链管理的透明化和自动化
- 在宝洁和吉列赞助下，Kevin Ashton与MIT的教授Sanjay Sarma、Sunny Siu和研究员David Brock，于199年10月1日，共同创立了一个RFID研究机构——自动识别中心(Auto-ID Center)，Kevin Ashton出任该中心第一任执行主任，2003年，识别中心被EPCglobal更名为自动识别实验室。

Kevin Ashton

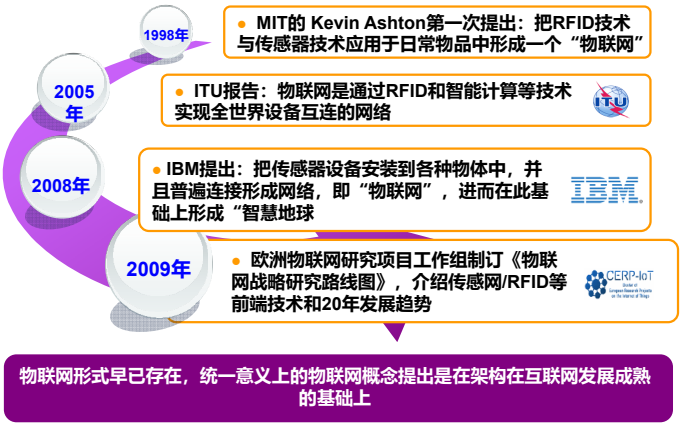
EPCglobal

- EPCglobal是国际物品编码协会EAN和美国统一代码委员会(UCC)的一个合资公司。它是一个受业界委托而成立的非盈利组织，负责 EPC网络的全球化标准，以便更加快速、自动、准确地识别供应链中商品。
- 2003 年10月31日以后，设在麻省理工学院自动识别中心的管理职能正式停止，其研究功能并入自动识别实验室 。
- EPCglobal继续与自动识别实验室密切合作，以改进EPC(电子产品代码）技术使其满足将来自动识别的需要。

物联网思想的起源

- Kevin Ashton对物联网的定义很简单：把所有物品通过射频识别等信息传感设备与因特网连接起来，实现智能化识别和管理。
- Auto-ID Center提出：要在因特网基础上，利用RFID、WSN(传感器网络)、数据通信等技术，构造一个覆盖世界上万事万物的“物联网”——The Internet of Things；在这个网络中，物品能够彼此进行“交流”而无需人的干预。
- Kevin Ashton预测电子产品代码EPC(Electronic Product Code)网络，将使机器能感应到全球任何地方的人造物体，从而创造真正的“物联网”。

物联网概念的发展



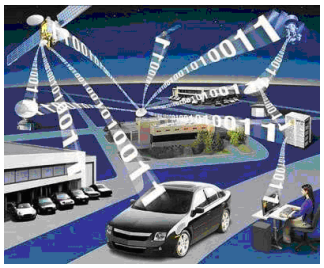
物联网形式早已存在，统一意义上的物联网概念提出是在架构在互联网发展成熟的基础上

ITU眼中的物联网

- 《ITU因特网报告2005：物联网》：From anytime, any place connectivity for anyone, we will now have connectivity for anything.
  - 无所不在的“物联网”通信时代即将来临，世界上所有的物体从轮胎到牙刷、从房屋到纸巾都可以通过因特网主动进行交换。
  - 射频识别技术（RFID）、传感器技术、纳米技术、智能嵌入技术将到更加广泛的应用。

ITU眼中的物联网

- 国际电信联盟（ITU）的报告中描绘了“物联网”时代的情形：
  - 司机出现操作失误时汽车会自动报警；
  - 公文包会提醒主人忘带了什么东西；
  - 衣服会“告诉”洗衣机对颜色和水温的要求；
  - ……



IBM——智慧的地球

- 2008年11月，美国IBM公司总裁彭明盛在纽约对外关系理事会上发表题为《智慧地球：下一代领导人议程》的讲话，正式提出“智慧地球”（Smarter Planet）设想：
  - 将新一代IT、因特网技术充分应用到各行各业，把感应器嵌入装备到全球的医院、电网、铁路、桥梁、隧道、公路、建筑、供水系统、油气管道、大坝等，而后通过基于IBM平台的超级计算机和云计算。使得人智慧的医疗、智慧的城市、智慧的交通、智慧的供应链、智慧的银行

美国：政府积极回应IBM的“智慧地球”

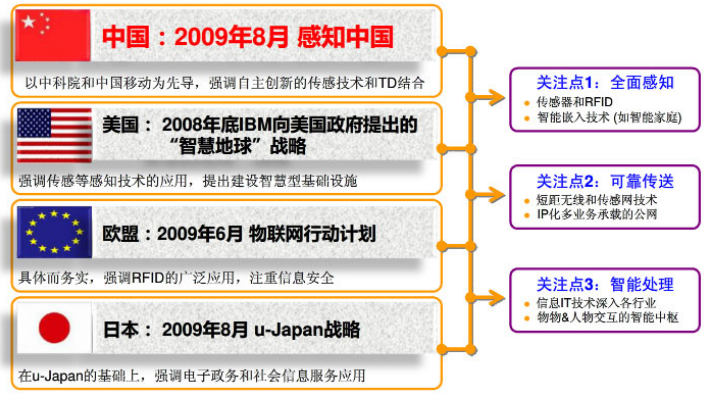
- 1月28日，奥巴马总统与美国工商业领袖举行了一次“圆桌会议”，彭明盛推销“智慧的地球”这一概念，建议新政府投资新一代的智慧型基础设施，阐明其短期和长期效益。
- 奥巴马对此给予了积极的回应。认为“智慧地球”有助于美国的“巧实力”(Smart Power)战略，是继互联网之后国家发展的核心领域。

更透彻的感知
- 利用任何可以随时随地感知、测量、捕获和传递信息的设备、系统或流程。

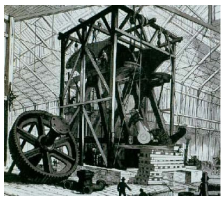
更全面的互联互通
- 先进的系统可按新的方式协同工作

更深入的智能化
- 利用先进技术获取更智能的洞察并付诸实践，进而创造新的价值

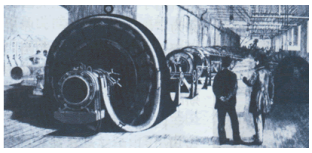
各国对物联网的关注



从科学发展史看物联网



18世纪中期，以蒸汽机为代表的第一次工业革命开创了人类的大机器工业时代



19世纪后期到20世纪中叶，以电机为代表的第二次工业革命使人类进入了电气化时代

物联网在科学发展史的地位

20世纪下半叶，以互联网计算机为代表的第三次工业革命迅速席卷全球，世界进入信息化时代

21世纪初提出的物联网，能够引发第四次工业革命吗?

各国对物联网的关注

中国：2009年8月 感知中国

以中科院和中国移动为先导，强调自主创新的传感技术和

美国：2008年底IBM向美国政府提出的“智慧地球”战略

强调传感等感知技术的应用，提出建设智慧型基础设施

欧盟：2009年6月 物联网行动计划

具体而务实，强调RFID的广泛应用，注重信息安全

日本：2009年8月 u-Japan战略

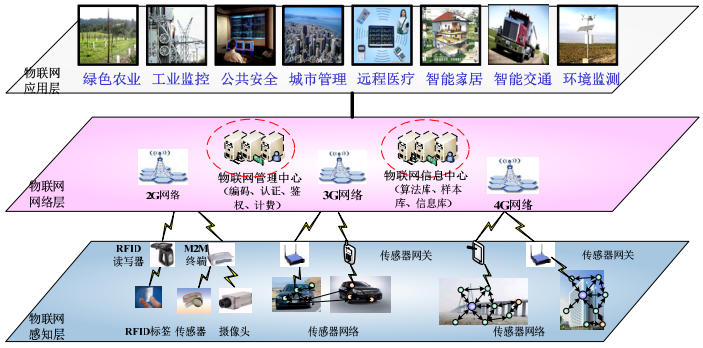
在u-Japan的基础上，强调电子政务和社会信息服务应用

关注点1：全面感知
- 传感器和RFID
- 智能嵌入技术(智能家庭)

关注点2：可靠传送
- 短距无线和传感网技术
- IP化多业务承载的公网

关注点3：智能处理
- 信息IT技术深入各行业
- 物物&人物交互的智能中枢

物联网体系架构:感知层/网络层/应用层



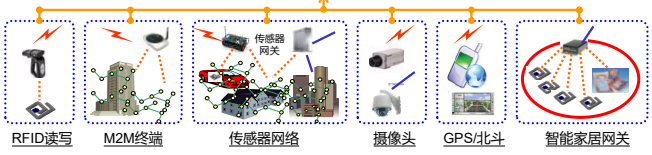
全面感知、可靠传送、智能处理是物联网的三大特征。

感知层是物联网全面感知的基础

物联网感知层

感知层作用	感知层实现方式	感知层突破方向
• 感知和识别物体 • 采集和捕获信息	• RFID标签和读写器 • M2M终端和传感器 • 传感器网络和网关 • 摄像头和监控 • GPS/北斗定位授时 • 智能家居网关	• 更敏感和更全面的感知能力 • 解决低功耗的问题 • 解决小型化和低成本问题

无线上连 & 有线上连



感知层是实现物的世界连接和感知的基础，必须考虑感知层的全面布局和发展重点产品策略

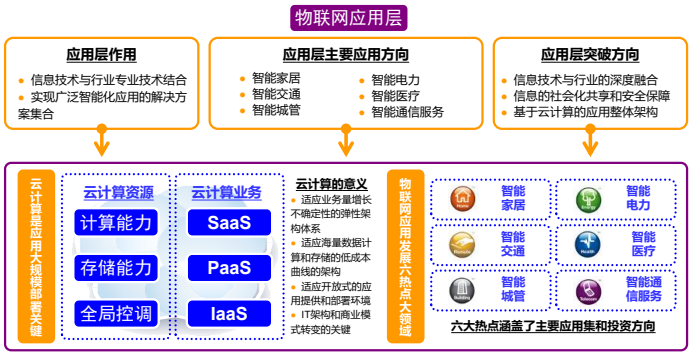
网络层是物联网无处不在的前提

物联网网络层

网络层作用	网络层主要层次	网络层突破方向
• 连接感知层和应用层 • 随时随地的连接实现 • 当前最成熟的部分	• 接入网：无线/光纤各种类型的接入形式 • 核心网：统一IP协议上的大带宽的可靠网络 • 业务支撑平台：业务统一管理部署和运营支撑	• 扩展规模，以实现无处不在 • 业务可扩展的管理运营能力 • 简化结构，上下层面融合

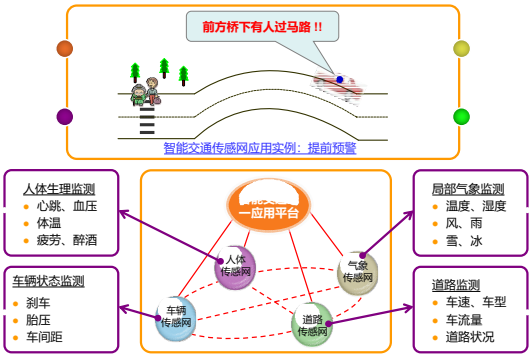
网络层是物联网成为普遍服务前提，必须关注规模扩展机遇，重点是接入网络和业务支撑平台

应用层是物联网智能处理的中枢



应用层是物联网的智能中枢，必须关注云计算新架构应用和聚焦方向的应用方案集合的提供

物联网的应用：智能交通

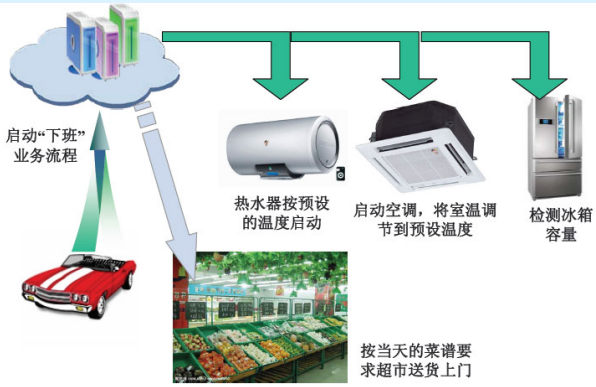


智能交通实现的前提：全面的感知，及时可靠的传送，智能应用平台的信息聚合处理和应用

物联网应用示例——智能家庭

- 智能家庭是各类消费电子产品、通信产品、信息家电及智能家居等通过物联网进行通信及数据交换,实现家庭网络中各类电子产品之间的“互联互通”,并实现随时随地对智能设备的控制。

在智能家居的应用场景中，用户在下班回家的路上即可用手机启动“下班”业务流程，将热水器和空调调节到预订的温度，并检测冰箱内的食物容量，如不足则通过网络下订单要求超市按照当天的菜谱送货。



小结：物联网概念最关注以人为中心

统一的物联网概念核心关注点是：以人为中心，建立为人服务的物的基础架构和

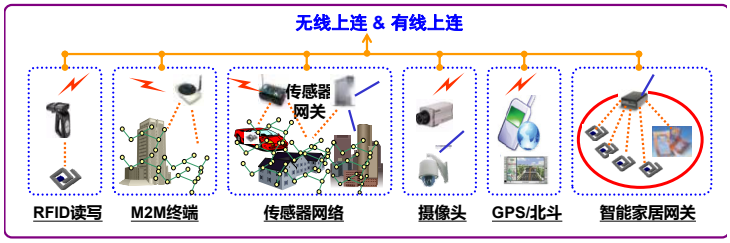
E社会模型
- 强调以人为中心的任意可达的网络
- 强调以人为中心的按需可用的服务

智慧地球模型
- 强调为人服务的生产生活各个方面
- 强调为人服务的智能处理能力提升

物联网不是包含一切的连接物的网络，其核心是以人为中心的物的网络和为人服务的应用

物联网的感知层

- 感知层包括:条码和扫描器、RFID标签和读写器、摄像头、GPS、传感器、传感器网络等
- 其中条码和RFID标签用来识别和显示物品身份和信息。



条形码——物联网的第一代身份证

- 条码技术是在计算机应用发展过程中，为消除数据录入的“瓶颈”问题而产生的，可以说是最“古老”的自动识别技术。
- 条形码是由一组规则排列的条、空以及对应的字符组成的标记。当使用专门的条形码识别设备如手持式条码扫描器扫描这些条码时，条码中包含的信息就转化为计算机可识别的数据。
- 目前市场上常见的是一维条形码，信息量约几十位数据和字符；二维条形码相对复杂，但信息量可达几千字符。

一维条码的基本概念

- 一维条码是由一组规则排列的条、空以及对应的字符组成的标记。普通的一维条码在使用过程中仅作为识别信息，它的意义是通过在计算机系统的数据库中提取相应的信息而实现的。
- 一个完整的条码的组成次序依次为：静区（前）、起始符、数据符、（中间分割符，主要用于EAN码）、(校验符)、终止符、静区（后）。

一维条码的基本概念

- 模块：构成条码的基本单位是模块，模块是指条码中最窄的条或空，模块的宽度通常以mm或mil（千分之一英寸）为单位。
- 构成条码的一个条或空称为一个单元，一个单元包含的模块数是由编码方式决定的
  - 如EAN码，所有单元由一个或多个模块组成；
  - 而如39码中，所有单元只有两种宽度，即宽单元和窄单元，其中的窄单元即为一个模块。

一维条码的基本概念

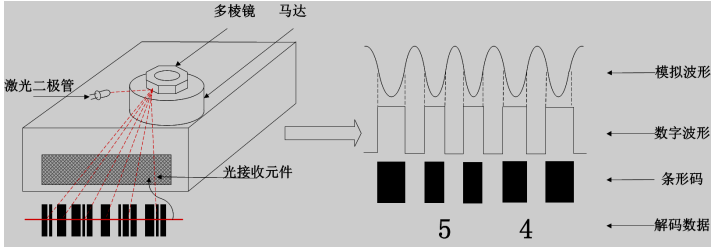
- 密度（Density）：条码的密度指单位长度的条码所表示的字符个数。模块尺寸越小，密度越大，所以密度值通常以模块尺寸的值来表示（如5mil）。通常7.5mil以下的条码称为高密度条码，15mil以上的条码称为低密度条码。
- 宽窄比：对于只有两种宽度单元的码制，宽单元与窄单元的比值称为宽窄比，一般为2-3左右（常用的有2：1，3：1）。宽窄比较大时，阅读设备更容易分辨宽单元和窄单元，因此比较容易阅读。

一维条码的基本概念

- 条码密度:单位长度的条码所表示的字符个数
- 双向条码：条码的两段都可以作为扫描起点的。
- 中间分隔符：在条码符号中，位于两个相邻的条码符号之间且不代表任何信息的空。
- 连续性条码：在条码字符中，两个相邻的条码字符之间没有中间分隔符的条码。
- 非连续性条码：在条码字符中，两个相邻的条码字符之间存在中间分隔符的条码。

一维条形码的译码原理

- 激光扫描仪通过一个激光二极管发出一束光线，照射到一个旋转的棱镜或来回摆动的镜子上，反射后的光线穿过阅读窗照射到条码表面，光线经过条或空的反射后返回阅读器，由一个镜子进行采集、聚焦，通过光电转换器转换成电信号，该信号将通过扫描期或终端上的译码软件进行译码。



一维条形码的缺点

- 一维条码为了保证局部损坏的条码仍可正确辨识，且使得扫描容易完成，它只在一个方向（水平方向）上表达信息，垂直方向不携带信息，因此信息密度偏低。
- 一维条码受限于信息容量，通常只能标识商品，而无法对商品信息进行更详细描述，因此对计算机网络和数据库系统相当依赖。
- 二维条码具有高信息密度、大容量、抗磨损的特点，其信息存储量是一维码的几十到几百倍，获得广泛应用。

一维码与二维码的比较

一维条形码特点：

1. 可直接显示内容为英文、数字、简单符号；
2. 贮存数据不多，主要依靠计算机中的关联数据库；
3. 保密性能不高；
4. 损污后可读性差。

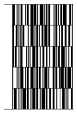
二维条形码特点：

1. 可直接显示英文、中文、数字、符号、图型；
2. 贮存数据量大，可存放1K字符，扫描仪直接读取内容，无需另接数据库；
3. 保密性高（可加密），
4. 安全级别最高时，损污50%仍可读取完整信息。

二维条形码

- 要提高信息密度，同时又要在一个固定面积上印出所需要的信息，可用两种方法来解决：
  - 堆叠式二维条码

PDF417



Code 16K

  - 矩阵式二维条码

Aztec Code

QR Code

DataMatrix

堆叠式二维条码的编码原理

- 将一维条码的高度变窄，再根据需要堆成多行
  - 在编码设计、检查原理、识读方式等方面均继承了一维条码的特点
  - 由于行数增加，对行的识别、解码算法设计上和一维条码不同
- 目前应用最广泛的堆叠式二维码是Symbol公司的华裔王寅敬博士发明的PDF417码。

矩阵式条码的编码原理

- 是建立在计算机图像处理技术，组合编码原理等基础上的图形符号自动识别的码制
- 以矩阵形式构成，在矩阵相应元素位置上，用点的出现表示二进制的1，没有点则表示0
- 点的排列组合确定了矩阵式二维码所代表的意义。
- 2006年，具有我国自主知识产权的紧密矩阵码(CM码)和网格矩阵码(GM码)，成为国家电子行业标准。

RFID射频识别技术——电子标签

- RFID是射频识别技术（Radio Frequency Identification）的英文缩写，利用射频信号通过交变磁场或电磁场，实现电子标签和阅读器之间无接触信息传递，并通过所传递的信息达到识别目的。
- 它是上世纪90年代兴起的自动识别技术，首先在欧洲市场上得以使用，随后在世界范围内普及。
- 射频识别技术改变了条形码依靠"有形"的一维或二维几何图案来提供信息的方式，通过芯片来提供存储在其中的数量巨大的"无形"信息。

RFID的历史与现状

年代	事件
1941-1950	雷达技术催生了RFID技术，1948年奠定了RFID技术的理论基础
1951-1960	早期RFID技术的探索阶段，仍处于实验室实验研究。
1961-1970	RFID技术的理论得到进一步发展，人们开始尝试一些新应用。
1971-1980	RFID技术与产品研发处于高潮期，各种RFID技术测试得到加速出现了最早的商业应用。
1981-1990	RFID技术及产品进入商业应用阶段，各种规模应用开始出现。
1991-2000	RFID技术标准化问题日趋得到重视，RFID应用更加丰富，已经成为人们生活中的一部分。
2000-至今	RFID产品种类更加丰富，各类标签得到大发展，标签的成本也不断降低，规模应用行业开始扩张。

RFID与条形码技术的比较（1）

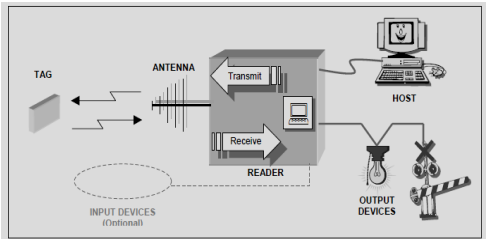
- RFID的优势在于：
  - **体积小且形状多样**：RFID标签在读取上并不受尺寸大小与形状限制，不需要为了读取精度而配合纸张的固定尺寸和印刷品质。
  - **耐环境性**：纸张容易被污染而影响识别。但RFID对水、油等物质却有极强的抗污性。另外，即使在黑暗的环境中，RFID标签也能够被读取。
  - **可重复使用**：标签具有读写功能，电子数据可被反复覆盖，因此可以被回收而重复使用。

RFID与条形码技术的比较（2）

- RFID的优势在于：
  - **唯一标识性**：一个标签唯一标识一件物品
  - **数据存储容量大**：一维条码容量约50字节；二维码最大存储2~3000字符；RFID容量达数百万字节
  - **穿透性强**：标签在被纸张、木材和塑料等非金属或非透明的材质包裹的情况下也可以进行穿透性通讯。
  - **数据安全性**：标签内的数据通过循环冗余校验的方法来保证标签发送的数据准确性；数据由密码保护，不易伪造及变更。

RFID系统构成

- RFID系统由五个组件构成，包括：传送器、接收器、微处理器、天线、标签。
- 传送器、接收器和微处理器通常都被封装在一起，又统称为阅读器(Reader)，所以工业界经常将RFID系统分为为阅读器、天线和标签三大组件。



RFID技术分析——阅读器

- 阅读器是RFID系统最重要也是最复杂的一个组件。工作模式一般是主动向标签询问标识信息
- 阅读器可以通过标准网口、RS232串口或USB接口同主机相连，通过天线同RFID标签通信。有时为了方便，阅读器和天线以及智能终端设备会集成在一起形成可移动的手持式阅读器。

RFID技术分析——天线

- 天线同阅读器相连，用于在标签和阅读器之间传递射频信号。
- 阅读器可以连接一个或多个天线，但每次使用时只能激活一个天线。RFID系统的工作频率从低频到微波，这使得天线与标签芯片之间的匹配问题变得很复杂。

RFID技术分析——标签

- 标签（Tag）是由耦合元件、芯片及微型天线组成，每个标签内部存有唯一的电子编码，用来标识目标对象。
- 标签进入RFID阅读器扫描场以后，接收到阅读器发出的射频信号，凭借感应电流获得的能量发送出存储在芯片中的电子编码（被动式标签），或者主动发送某一频率的信号（主动式标签）。阅读器解码后，送到中央信息系统进行处理

标签的存储方式

- 电可擦可编程只读存储器（EEPROM）：一般射频识别系统主要采用EEPROM方式。这种方式的缺点是写入过程中的功耗消耗很大，使用寿命一般为100,000次
- 铁电随机存取存储器（FRAM）：与EEPROM相比，FRAM的写入功耗消耗减小100倍，写入时间甚至缩短1000倍。FRAM属于非易失类存储器。然而，FRAM由于生产方面的问题至今未获得广泛应用。
- 静态随机存取存储器（SRAM）：SRAM能快速写入数据，适用于微波系统，但SRAM需要辅助电池不间断供电，才能保存数据。

标签的分类（1）

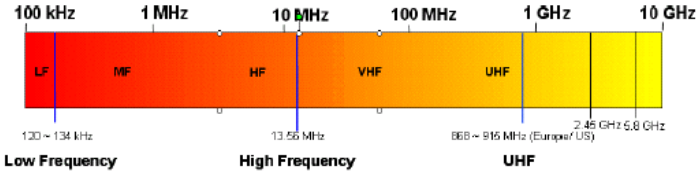
- 被动式标签（Passive Tag）：
  - 因内部没有电源设备又被称为无源标签。
  - 标签内部的集成电路通过接收由阅读器发出的电磁波进行驱动，向阅读器发送数据。
- 主动标签（Active Tag）：
  - 因标签内部携带电源又被称为有源标签。
  - 电源设备和与其相关的电路决定了主动式标签要比被动式标签体积大、价格昂贵。
  - 主动标签通信距离更远，可达上百米远。

标签的分类（2）

- 半主动标签（Semi-active Tag）：
  - 标签内部携带电池，能够为标签内部计算提供电源。
  - 标签可以携带传感器，用于检测环境参数，如温度、湿度、是否移动等。
  - 和主动式标签不同是它们的通信并不需要电池提供能量，而是像被动式标签一样通过阅读器发射的电磁波获取通信能量。

RFID技术分析——频率

- RFID频率是RFID系统的一个很重要的指标，它决定了工作原理、通信距离、设备成本、天线形状和应用领域等因素。
- RFID典型的工作频率有125KHz、133KHz、13.56MHz、27.12MHz、433MHz、860-960MHz、2.45GHz、5.8GHz等。
- 按照工作频率的不同，RFID系统集中在低频、高频和超高频三个区域



RFID技术分析——频率

- 低频（LF）：
  - 范围为30kHz-300kHz，典型低频工作频率有125kHz和133kHz两个，该频段的波长大约为2500m，通信范围一般小于1米。
  - 低频标签一般都为无源标签，其工作能量通过电感耦合的方式从阅读器耦合线圈的辐射场中获得。
  - 除金属材料影响外，低频信号一般能够穿过任意材料的物品而不降低它的读取距离。

RFID技术分析——频率

- 高频（HF）：
  - 范围为3 MHz -30 MHz，典型工作频率为13.56MHz，该频率的波长大概为22米，通信距离一般也小于1米。
  - 该频率的标签不再需要线圈绕制，可以通过腐蚀活字印刷的方式制作标签内的天线，采用电感耦合的方式从阅读器辐射场获取能量。

RFID技术分析——频率

- 超高频（UHF）：
  - 范围为300MHz-3GHz，3GHz以上为微波范围。
  - 采用超高频和微波的RFID系统一般统称为超高频RFID系统，典型的工作频率为：433MHz，860-960MHz，2.45GHz，5.8GHz，频率波长大概在30厘米左右(严格意义上，2.45GHz和5.8GHz属于微波范围)。
  - 超高频标签可以是有源标签与无源标签两种，通过电磁耦合方式同阅读器通信。
  - 通信距离一般大于1米，典型情况为4-6米，最大可超过10米。

RFID标签冲突

- 随着阅读器通信距离的增加，其识别区域的面积也逐渐增大，这常常会导致多个标签同时处于阅读器的识别范围之内。
- 由于阅读器与所有标签共用一个无线通道，当两个以上的标签位于阅读器的可读范围内，且同一时刻向阅读器发送标识信号时，信号将产生叠加，导致阅读器不能正常解析标签发送的信号。
- 这个问题通常被称为标签信号冲突问题（或碰撞问题）
- 解决标签冲突问题的方法被称为标签防冲突算法（或防碰撞算法，反冲突算法）。

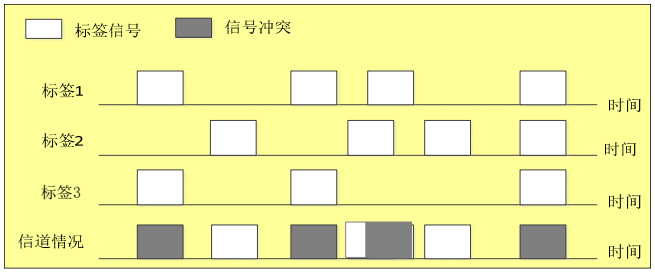
RFID标签冲突

- 现有的基于时分多址标签防冲突算法可以分为：
  - 基于ALOHA机制的算法
  - 基于二进制树算法

PS:上述这两种类型又包括若干种变体。

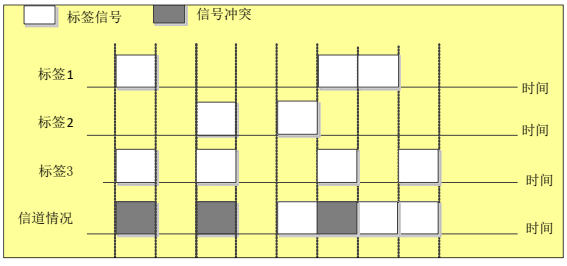
纯ALOHA的防冲突算法

- 是一种随机接入方法。标签在收到阅读器广播的识别命令后，立即发送标识符。
- 纯ALOHA防冲突算法简单，易于实现，但信道利用率仅为18.4%，性能非常不理想。



分时隙的ALOHA防冲突算法（S-ALOHA）

- S-ALOHA算法将纯ALOHA算法的时间分为若干时隙，每个时隙≥标签标识符发送的时间长度，并且每个标签只能在时隙开始时刻发送标识符。
- 需要系统进行时间同步，S-ALOHA协议的信道利用率达到36.8%，是纯ALOHA的两倍。



基于帧的分时隙ALOHA防冲突算法（FSA）

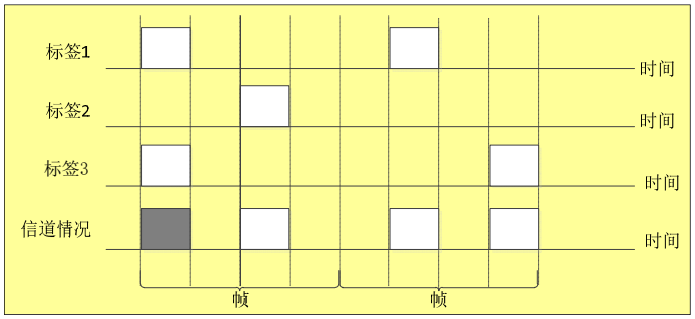
- 在S-ALOHA基础上，将若干个时隙组织为一帧，时隙个数即为帧长度*f*；每个时隙长度足够一个标签应答完阅读器的读取命令。阅读器按照帧为单元进行识别：
- 算法原理：
  - Step1：每一帧开始时，阅读器广播帧的长度*f*，激活所有标签。
  - Step2：每个非休眠状态的标签随机独立的在0~*f-1*中选择一个整数做为各自时隙序号，并将时隙序号存于自己的寄存器SN中。
    - ps:已成功应答阅读器命令的标签将处于休眠状态

基于帧的分时隙ALOHA防冲突算法（FSA）

- 算法原理（续）：
  - Step3:在一帧中，阅读器启动新时隙直到/时隙为止
    - 如果标签的时隙序号SN=0，立即发送自己标识符
      - 无冲突发生：该标签进入休眠状态不再活动
      - 发生冲突：标签进入等待状态，在阅读器下一帧周期中再次等待发送
    - 如果标签的时隙序号SN≠0，仅将时隙序号减1
  - Step4:重复Step1~Step3，直到阅读器在某一帧中没有收到任何来自标签的应答信号

基于帧的分时隙ALOHA防冲突算法（FSA）

- FSA成为RFID系统中最常用的一种基于ALOHA的防冲突算



基于帧的分时隙ALOHA防冲突算法（FSA）

- FSA算法的优点：
  - 逻辑简单，电路设计简单，所需内存少，且在帧内只随机发送一次能够更进一步降低了冲突的概率。
- FSA的缺点：
  - 标签数量远大于时隙个数时，读取标签的时间大大增加；
  - 当标签个数远小于时隙个数时，会造成时隙浪费。
- 只有当时隙个数=阅读器识别范围内的标签数时，FSA性能达到最优。
- 实际应用中标签数未知，如何确定合理帧长?

时隙随机算法SR

- 动态自适应设置帧长度的算法可以解决FSA算法固定帧的局限性(P36)。
- 流行的方法有两种：
  - 1、根据前一帧通信获取的空的时隙数目、发生碰撞的时隙数目、成功识别标签的时隙数目的数量，估计当前的标签数，并设置下一帧的最优的长度；
  - 2、根据前一时隙的反馈动态调整时隙周期
    - 时隙随机算法SR
    - EPCglobal Gen2标准中设计的Q算法

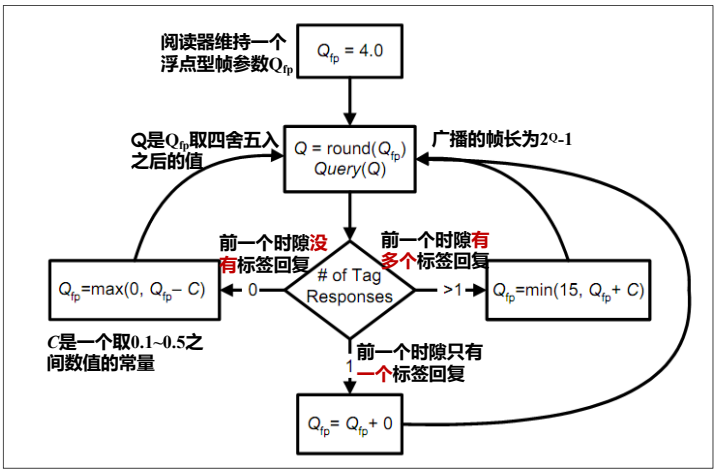
时隙随机算法SR

- step1:阅读器发送含有时隙参数Q的QueryAdjust命令，未休眠标签从0-2^Q-1中随机选择一个做为自己的时隙序号,置入自己的时隙计数器：
- step2:
  - 计数器 = 0的标签立即应答阅读器，转移到应答状态；若此时未发生标签冲突，则此标签进入休眠状态，退出识别；
  - 计数器不等于0的标签，计数器值 - 1，转移到仲裁状态，并等待下一条QueryAdjust或QueryRep命令

时隙随机算法SR

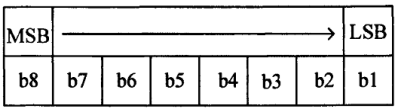
- step3:
  - 1、如果阅读器认为无需更改参数Q，则在下一时隙发送QueryRep命令：
    - 处于仲裁状态的标签收到QueryRep命令时，时隙计数器值 - 1，转step2
    - 处于应答状态的标签，计数器值被置为7FFFFH，转step2
  - 2、如果阅读器认为冲突过多需要更改参数Q，则重新设定Q值，在下一时隙转step1

EPCglobal Gen2标准的Q算法



基于二进制树的防冲突算法

- 算法执行过程中，阅读器要多次发送命令给标签，每次命令都把标签分成两组，在分组过程中，将对应的命令参数以节点的形式存储起来，就可以得到一个数据的二叉树，标签位于叶结点，而所有的这些数据节点又是以二进制的形式出现的，所以称为“二进制树”。
- 每个标签都有唯一标识自身的序号，称为SN(SerialNumber)，序号的长度，格式，以及编码方式因标准而异，为了说明的便利，统一定义为8位长度的二进制码。

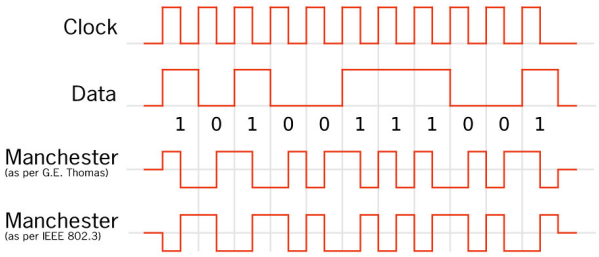


基于二进制树的防冲突算法

- 为了实现二进制搜索算法，RFID标签通常采用曼彻斯特编码，因为这种编码自带时钟同步，而且可以检测出碰撞位。
- 目前曼彻斯特编码存在两种相反的数据表示约定。
  - 第一种是由G. E. Thomas, Andrew S. Tanenbaum等人在1949年提出的，规定0是由低-高的电平跳变表示，1是高-低的电平跳变。
  - 第二种约定则是在IEEE 802.4(令牌总线)和低速版的IEEE 802.3(以太网)中规定，低-高电平跳变表示1，高-低的电平跳变表示0。

基于二进制树的防冲突算法

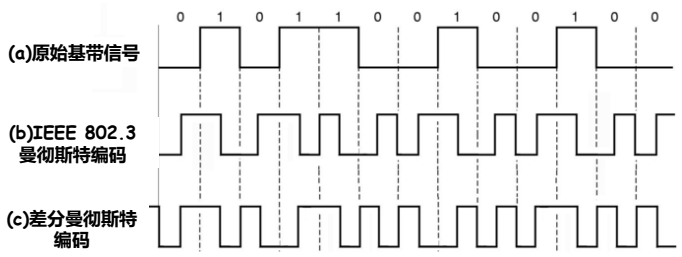
- 两种曼彻斯特编码图例



- 由于有以上两种不同的表示方法，所以应用时会出现歧异。使用差分曼彻斯特编码(Differential Manchester encoding)可以解决上述问题

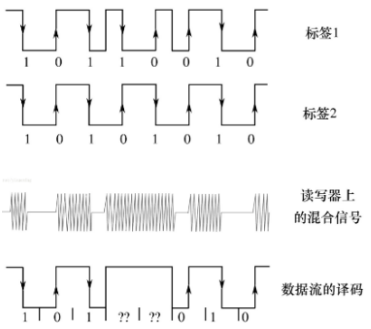
基于二进制树的防冲突算法

- 曼彻斯特编码和差分曼彻斯特编码对比图例



基于二进制树的防冲突算法

- 何为碰撞位检测?
  - 如果两个或多个电子标签同时发送，因为其发送的数位有不同值，则接收的上升沿和下降沿互相抵消，“没有变化”的状态是不允许的，将作为错误被识别。用这种方法可以按位追溯碰撞的出现。



曼彻斯特编码

基于二进制树的防冲突算法

- 基本思想：按照递归的工作方式，将冲突的标签集合分为两个标签子集，直到集合中只剩下一个标签为止。
- 如何划分子集?
  - 基本二进制树算法
  - 随机二进制树算法
    - 让标签随机选择所属集合
  - 查询二进制树算法
    - 按照标签的标识符号进行划分

基本二进制树

- step1：标签进入阅读器工作范围，阅读器发出一个最大序列号S_{max}，（最初所有标签的序列号均小于S_{max}）
- step2：当前没有未识别标签，结束；否则，所有序列号≤S_{max}的标签都将自身序列号应答给阅读器。
- step3：
  - 若阅读器检测到标签的应答信号发生碰撞，则将S_{max}中对应的碰撞起始位设置为0，低于该位者设置为1，高于该位者保持不变，阅读器将处理后的S_{max}发送给标签，转step2；
  - 若无碰撞发生，则必然只有一个标签应答阅读器，待标签与阅读器通信结束后，此标签进入休眠状态，不再响应阅读器的请求命令，转step2。
- 重复上述算法，即可按序列号从小到大依次识别出各个标签。

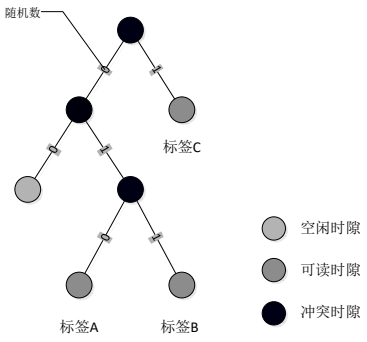
基本二进制树实例分析

假设四个电子标签的序列号分别为标签1：10110010；标签2：10100011；标签3：10110011；标签4：11100011，识别过程如下：

- 1）读写器设置筛选条件（11111111），向标签发送请求。
- 2）阅读范围内的所有标签均符合条件，响应请求，发送自身ID。
- 3）读写器检查到第0，4，6位发生碰撞，即1x1x001x，读写器将碰撞的最高位置0，其余低位置1，重新设定筛选条件（10111111），向标签发送请求。
- 4）标签10110010，10100011，10110011响应读写器请求，发送自身ID。
- 5）读写器检测到第0，4位发生碰撞，即101x001x，读写器将最高位置0，其余低位置1，重新设定筛选条件（10101111），向标签发送请求。
- 6）标签10101111响应读写器的请求，发送自身ID。
- 7）读写器没有检测到碰撞的发生，成功识别出标签10100011，选择该标签，完成对标签的读写后，令该标签进入“无声”状态。
- 8）读写器重新设定筛选条件（11111111），重复以上识别过程

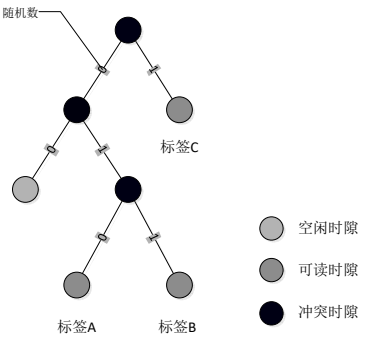
随机二进制树

- Step1：每个标签维持一个初值为0的计数器。
- Step2：每一个时隙开始时
  - 如果标签的计数器为零，立即发送自己的标识符号；否则，标签在该时隙不回复。
    - 显然，第一个时隙时，所有标签都会回复



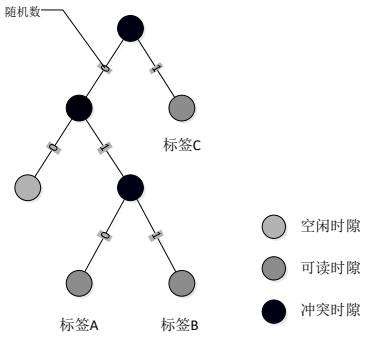
随机二进制树

- Step3：每个时隙结束时，阅读器会将接收结果反馈给标签；标签根据反馈结果调整计数器：
  - 如果该时隙有冲突发生
    - 发送标识符号的标签从0或1两个数字中，随机选择一个，加到计数器上
    - 没有发送标识符号的标签，计数器+1



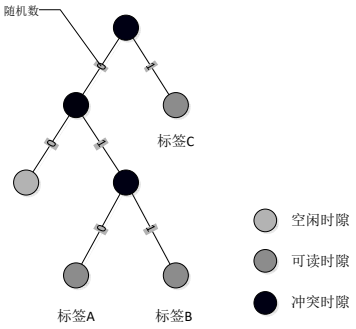
随机二进制树

- 如果该时隙没有冲突发生
  - 表示该时隙内没有标签发送标识符号；或者仅有一个标签成功发送标识符号
  - 成功发送标识的标签，在以后的时隙均不再回复阅读器的命令
  - 其它标签，将自己计数器减1



随机二进制树

- 重复Step2~Step3，直到所有标签均成功发送自己的标识符号为止
- 上述步骤类似对二叉树的中序遍历过程，图中每个结点代表一个时隙

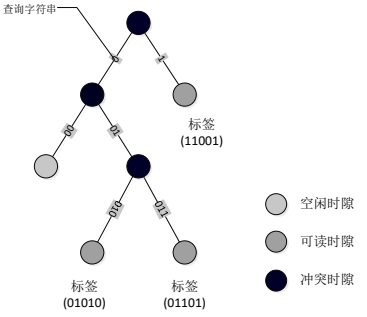


查询二进制树

- 算法思路：
  - 阅读器内部维持一个二进制前缀，初始值为0。每一个时隙开始时，阅读器广播该二进制前缀，标签将自己的标识符号的前缀与此二进制前缀进行比较，若相同则立即发送标识符号。
  - 如果阅读器探测到冲突发生，则在下次查询中在原来的二进制前缀后面增加0或1，重新查询，如此循环直到识别完所有的标签。

查询二进制树

- 总结：查询二进制树算法是无状态协议，不需标签内部维持任何状态，标签只需根据阅读器广播的标识符前缀作比较即可。

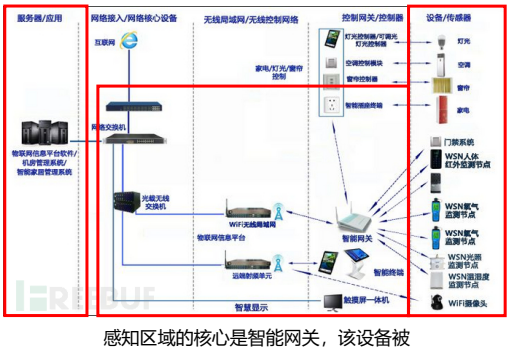


物联网安全和隐私概述

- 从信息安全和隐私保护的角度讲，物联网终端（RFID,传感器，智能信息设备）的广泛引入在提供更丰富信息的同时也增加了暴露这些信息的危险。
- 案例之一：2007年10月，台湾高校学生举行抵制含有RFID芯片的多功能学生证的活动。
- 案例之二：2008年8月，麻省理工3名学生宣布成功破解波士顿地铁资费卡，世界各地公交系统都采用几乎相同的智能卡技术
- 案例之三：2018年物联网安全大事件
  - https://www.freebuf.com/column/193277.html

一个智能家居的常见IoT网络拓扑

信息业务平台集中管理区，有公网的业务系统和ip，容易成为黑客攻击的目标，并且入侵后能获取大量敏感数据。

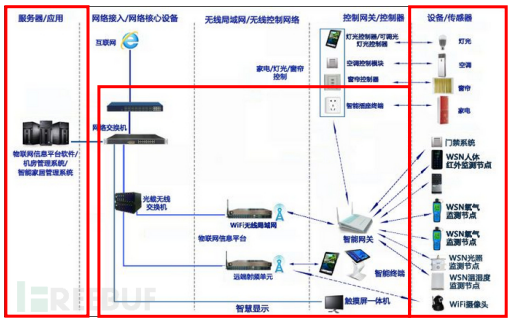


感知区域的核心是智能网关，该设备被入侵会导致全部物联网设备，传输区域需要保证各个传输设备的安全（尤其是口令安全）。

安全主要靠出场的设置，黑客接触利用必须经过智能网关，本身存在安全隐患低，风险小，在该网络构架中本身安全系数最高。

黑客对智能家居IoT网络的入侵途径

- 通过公网，入侵业务平台管理器
- 通过无线网络，入侵同属局域网内的不同设备
- 通过入侵个人终端，渗透同属局域网内的不同设备



黑客如何利用智能家居IoT网络的漏洞

- IOT设备本身存在的安全问题（串口安全漏洞，默认证书(密码)，硬编码问题，不安全的移动和WEB应用，缺乏完整性和签名的校验等）
- 网络问题（不安全的网络通信（伪造各类指令，中间人攻击实现控制整个系统），不安全的无线通信）
- 业务应用安全问题（命令执行，弱口令，SQL注入，任意文件上传等等）

常见的IoT的威胁

- 僵尸网络和DDoS攻击（更多作为分布式节点攻击服务器）
- 远程拍录（所有带摄像功能的末端设备都有可能）
- 垃圾邮件（作为垃圾邮件的一个节点，难以溯源）
- 高级持续性威胁(针对电网，工控等)
- 勒索病毒（通过控制室内温度，控制家电启动来进行勒索）
- 数据窃取（窃取有关用户信息，比如信用卡等信息）
- 入侵住宅（打开住宅智能锁，打开监控等等）
- 遥控车辆（入侵车辆智能系统，自动启停等）

IoT的隐私权

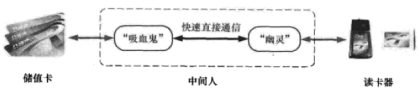
- 物联网与隐私
  - 不当使用会造成信息泄露、篡改以及侵害隐私
  - 恰当的安全和隐私保护技术，可以有效降低使用物联网的安全风险
- RFID及更多的物联网感知识别设备，是物联网重要的信息获取手段。
  - 感知识别设备产品是否有相关的安全和隐私的标准?
  - 这些标准能否为感知识别设备提供保护?

RFID标签的不安全性

- 实际应用背景：
  - RFID标签使用量大，必须控制单个标签的成本
  - 受限于现有技术和芯片制造水平，目前造价约为10美分的被动式标签，包含5000~10000个逻辑门，主要只用于实现最基本的标签功能
  - 在标签芯片中实现SHA-1等成熟的HASH算法，大约还需要3000~4000个逻辑门，公钥加密算法需要的逻辑门更多；
  - 因此，单个标签很难支持复杂的密码学计算

RFID标签主要安全隐患

- 窃听(eavesdropping)
  - 标签和阅读器之间通过无线射频通信
  - 攻击者可以在设定通信距离外偷听信息
- 中间人攻击(man-in-the-middle attack, MITM)
  - 对reader(tag)伪装成tag(reader)，传递、截取或修改通信消息
  - 2005年，Ziv Kfir和Avishai Wool发表了如何攻击电子钱包的论文——“扒手”系统



RFID标签主要安全隐患

- 欺骗阅读器
  - 重放(replaying)：将标签的回复记录，待阅读器询问时回放以欺骗阅读器
  - 克隆(cloning)：形成原来标签的一个副本
- 拒绝服务攻击(Denial-of-service attack, DoS)
  - 通过不完整的交互请求消耗系统资源，如：
    - ✓产生标签冲突，影响正常读取
    - ✓发起认证消息，消耗系统计算资源
  - 对标签的DoS
    - ✓消耗有限的标签内部状态，使之无法被正常识别

RFID标签主要安全隐患

- 物理破解(corrupt)
  - 标签容易获取
  - 标签可能被破解：通过逆向工程等技术
  - 破解之后可以发起进一步攻击
    - ✓推测此标签之前发送的消息内容
    - ✓推断其他标签的秘密
- 篡改信息(modification)
  - 非授权的修改或擦除标签数据

RFID标签主要安全隐患

- RFID病毒(virus, malware)
  - 标签中可以写入一定量的代码
  - 读取tag时，代码被注入系统
    - ✓SQL注入
- 其他隐患
  - 电子破坏标签
  - 屏蔽干扰标签的正常访问
  - 拆除标签
  - ...

主要隐私问题

- 隐私信息泄露
  - 姓名、医疗记录等个人信息
- 跟踪
  - 监控，掌握用户行为规律和消费喜好等。
  - 进一步攻击
- 效率和隐私保护的矛盾
  - 标签身份保密，增加了标签检索的代价，影响系统吞吐量
  - 快速验证标签却需要预先知道标签身份
  - 平衡：恰当、可用的安全和隐私

RFID安全和隐私保护机制

- 早期物理安全机制
  - 灭活(kill)：杀死标签，使标签丧失功能，不能响应攻击者的扫描。
  - 法拉第网罩：屏蔽电磁波，阻止标签被扫描。
  - 主动干扰：用户主动广播无线信号阻止或破坏RFID阅读器的读取。
  - 阻止标签(block tag)：通过特殊的标签碰撞算法阻止非授权阅读器读取那些由阻止标签预定保护的标签。
- 物理安全机制通过牺牲标签的部分功能满足隐私保护的要求。

RFID安全和隐私保护机制

- 现代基于阅读器与电子标签之间的非物理安全方案主要有两大类：认证机制和加密机制度
  - 认证机制:在阅读器与电子标签进行通信前实行安全认证机制，确认身份后才能进行正常通信，这样可以防止非授权或非法阅读器对标签信息的读取与标签数据信息的篡改，还能防止欺骗攻击和假冒攻击。
  - 加密机制:对二者之间传输的数据信息加密后再进行传输，这样就算攻击者获取数据后也不能得到需求的信息。

基本的RFID安全协议

- 由于安全问题愈发突出，针对这些安全问题的安全协议也相继而出，这些安全协议主要针对应用层的安全问题。
- 多数安全协议都是基于密码学中的hash函数来展开的
- hash函数通过相应算法的可以将任意长度的消息或者明文映射成一个固定长度的输出摘要。因为hash函数的特性，常常被应用于消息认证和数字签名中，最常用的hash函数有MD5与SHA-1。

基于Hash函数的安全协议

- 基于密码学的安全机制——哈希锁(hash-lock)协议
  - Hash-Lock协议是由Auto-ID Center的Sarma等人提出，使用metaID来代替真实的标签ID，以避免信息的泄漏和被追踪
  - 每个标签拥有自己的访问密钥key，且metaID=Hash（key）
- Hash-Lock协议的锁定过程：
  - 阅读器随机生成一个Key，并计算metaID=Hash（key）
  - 阅读器将metaID写入到标签
  - 标签进入锁定状态
  - 阅读器以metaID为索引，将（metaID，key）存储到后台数据库

基于Hash函数的安全协议

- Hash-Lock协议的解锁过程

- Hash-Lock协议的优点：
  - 让标签回传metaID来代替ID，避免将ID直接传送给未经授权的标签阅读器。
- Hash-Lock协议的缺点：
  - 由于未使用动态刷新机制，metaID保持不变，标签易被跟踪定位
  - （key，ID）以明文形式发送，容易被窃听者获取

基于Hash函数的安全协议

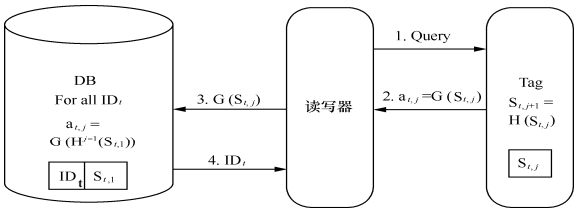
- 基于密码学的安全机制——随机哈希锁(randomized hash-lock)
  - Weis等人提出了随机Hash-Lock协议。该协议中，对于标签读写器的不同询问，标签将回传乱数形态的回传值给读写器，以解决Hash-Lock协议中标签容易被跟踪的问题。

基于Hash函数的安全协议

- Randomized Hash-Lock协议的缺点
  - 无法防止重放攻击，ID_k仍然以明文方式传输，获取了该信息就可以对标签进行假冒。
  - 每次确认一个标签身份，都要穷尽后台数据库存储的所有ID，并进行Hash运算，耗时长，该协议只适合小规模应用

基于Hash函数的安全协议

- 基于密码学的安全机制——哈希链(hash chain)
  - 此协议是基于共享秘密的询问-应答协议，在Hash链协议中，标签在每次认证过程中其密钥值是不断更新的。
  - 在发放标签之前，需要将标签的ID_i和$S_{i,1}$($S_{i,1}$是标签初始密钥值，对每一个标签而言，它的值都是不同的)存于后端数据库中，并将$S_{i,1}$存于标签随机存储器中。

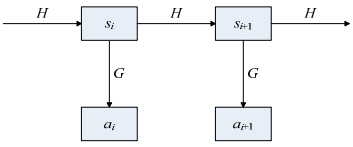


基于Hash函数的安全协议

- **Hash Chain协议的优点：**
  - 标签是个具有自主ID更新能力的主动式标签，避免了标签定位隐私信息的泄漏。又由于单向的Hash函数，不可能从$S_{t,j+1}$获得St_j，具有前向安全性。
- **Hash Chain协议的缺点：**
  - 为了尽量降低标签的制作成本，该协议降低了标签的存储空间和计算能力，只是单向的认证协议，标签未确认读写器的合法性。
  - 协议非常容易受到重传和假冒攻击。只要隐私侵犯者截获了$a_{t,j}$，它就可以进行重传攻击，伪装标签通过后台服务器认证。

其它安全协议

- 基于密码学的安全机制——同步方法(synchronization approach)
  - 预计算并存储标签的可能回复，如：
    - 在哈希链方法中，可以为每个标签存储m个可能的回复，标签响应时直接在数据库中查找
  - 高效key-search: O(1)
  - 威胁：回放，DoS



$s_{i+k} = H^k(s_i)$, (0 ≦ k ≦ m-1)

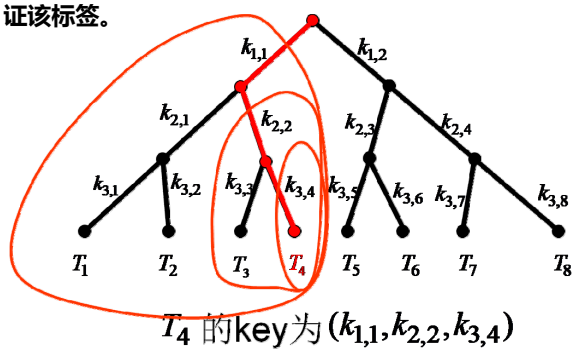
$a_{i+k} = G(H^k(s_i))$, (0 ≦ k ≦ m-1)

其它安全协议

- 基于密码学的安全机制——树形协议(tree-based protocol)
  - 标签中的多个密钥被组织在一个树形结构中，对应于从根结点到标签所在叶结点的路径。
  - 阅读器发起一个带有随机数r_1的查询
  - 标签T_i收到查询后产生随机数r_2，并用r_1,r_2及它所携带的所有密钥，计算所有密钥的Hash值
  - 算出的所有Hash值和r_2发送给阅读器
  - 阅读器使用这些Hash值在树中进行深度优先遍历，进而认证该标签。(P 286)

其它安全协议

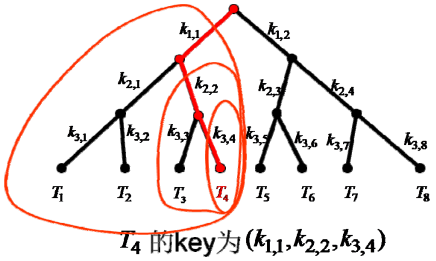
- 基于密码学的安全机制——树形协议(tree-based protocol)
  - 阅读器使用这些Hash值在树中进行深度优先遍历，进而认证该标签。



T_4 的key为 $(k_{1,1}, k_{2,2}, k_{3,4})$

其它安全协议

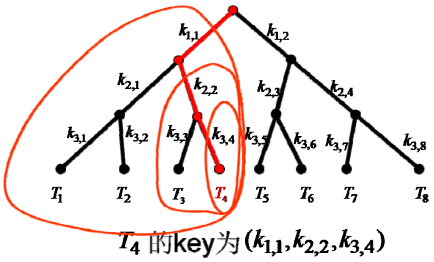
- 树形协议中标签的密钥是结构化存储的，如果树的深度是d，则整个认证过程中，标签和阅读器均需要计算d次$Hash$值
- 树的深度d与标签总数N有关，如果整棵树正好能存放所有标签的密钥，则有：$d=\log_\delta N$，δ 是树的度。



T_4 的key为 $(k_{1,1}, k_{2,2}, k_{3,4})$

其它安全协议

- 标签T_3和T_4共享了2个密钥，只有叶结点密钥不同，因此，如果标签T_3被攻击者破解并获取其中所有密钥，则攻击者可以利用T_3与T_4共享的密钥，跟踪标签T_4的隐私



T_4 的key为 $(k_{1,1}, k_{2,2}, k_{3,4})$

其它安全协议

- Avoine等人在2005年论文中分析，在2^{20}个标签系统中，树的度记为δ时，当攻击者破解K_0个标签后，成功跟踪单个标签的几率如下：

K_0 \ δ	2	20	100	500	1000
1	66.6%	9.5%	1.9%	0.3%	0.1%
20	95.5%	83.9%	32.9%	7.6%	3.9%
50	98.2%	94.9%	63.0%	18.1%	9.5%
100	99.1%	95.4%	85.0%	32.9%	18.1%
200	99.5%	96.2%	97.3%	55.0%	32.9%

2^{20}个tag，δ:分枝数，K_0个tag被破解 (Avoine, SAC'05)

- 此外，由于标签需要存储d个密钥，必然增加标签的存储空间，导致标签成本上升
- 进行标签认证时，需要计算多次Hash函数，使得认证时延增加。

RFID安全和隐私保护机制

- 其他方法
  - Physical unclonable function, (PUF)：利用芯片制造过程中必然引入的随机性，用芯片独有的物理特性实现函数。具有容易计算，难以特征化的特点。
  - 掩码：使用外加设备给阅读器和标签之间的通信加入额外保护。
  - 通过网络编码(network coding)原理得到信息
  - 可拆卸天线
  - 带方向的标签

如何面对安全和隐私挑战?

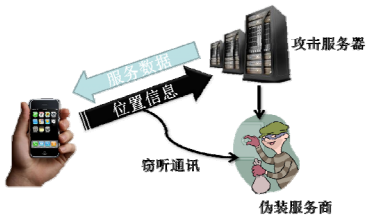
- 与其他技术结合解决RFID安全性问题
  - 生物识别技术
  - 近场通信(Near field communication, NFC)
- 以法律手段明确给出使用RFID技术损害用户安全与隐私必须付出的代价，并为如何防范做出明确指导。

位置信息与个人隐私

- 位置隐私的定义
  - 用户对自己位置信息的掌控能力，包括：
    - ✓是否发布、发布给谁、详细程度
- 保护位置隐私的重要性
  - 三要素：时间、地点、人物
  - 人身安全
  - 隐私泄露

位置信息与个人隐私

- 位置隐私面临的威胁
  - 用户和服务商之间的通信线路受到攻击者的窃听
  - 服务商对用户信息保护不力，攻击者通过攻击服务商的数据库，窃取用户位置隐私信息
  - 攻击者假冒服务商窃取用户隐私信息，或者服务商出卖用户隐私信息



保护位置隐私的手段

- 制度约束
- 隐私方针
- 身份匿名
  - 将位置信息中用户真实身份替换为匿名代号
  - K匿名策略
- 数据混淆
  - 对位置信息的数据进行混淆，不提供精确坐标，而以模糊说明性语句代替

保护位置隐私的手段

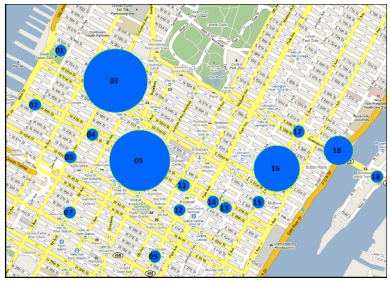
- 制度约束
  - 5条原则（知情权、选择权、参与权、采集者、强制性）
  - 优点
    - ✓一切隐私保护的基础
    - ✓有强制力确保实施
  - 缺点
    - ✓各国隐私法规不同，为服务跨区域运营造成不便
    - ✓一刀切，难以针对不同人不同的隐私需求进行定制
    - ✓只能在隐私被侵害后发挥作用
    - ✓立法耗时甚久，难以赶上最新的技术进展

保护位置隐私的手段

- 隐私方针：定制的针对性隐私保护
  - 分类
    - 用户导向型，如PIDF（Presence Information Data Format）
    - 服务提供商导向型，如P3P（Privacy Preferences Project）
  - 优点
    - 可定制性好，用户可根据自身需要设置不同的隐私级别
  - 缺点
    - 缺乏强制力保障实施
    - 对采用隐私方针机制的服务商有效，对不采用该机制的服务商无效

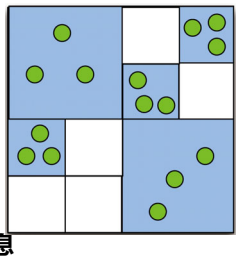
保护位置隐私的手段

- 身份匿名：
  - 认为“一切服务商皆可疑”
  - 隐藏位置信息中的“身份”
  - 服务商能利用位置信息提供服务，但无法根据位置信息推断用户身份
  - 常用技术：K匿名



K匿名

- 基本思想：让K个用户的位置信息不可分辨
- 两种方式
  - ✓空间上：扩大位置信息的覆盖范围
  - ✓时间上：延迟位置信息的发布
- 例：3-匿名
  - ✓绿点：用户精确位置
  - ✓蓝色方块：向服务商汇报的位置信息



保护位置隐私的手段

- 身份匿名（续）
  - 优点
    - ✓不需要强制力保障实施
    - ✓对任何服务商均可使用
    - ✓在隐私被侵害前保护用户隐私
  - 缺点
    - ✓牺牲服务质量
    - ✓通常需要借助“中间层”保障隐私
    - ✓无法应用于需要身份信息的服务

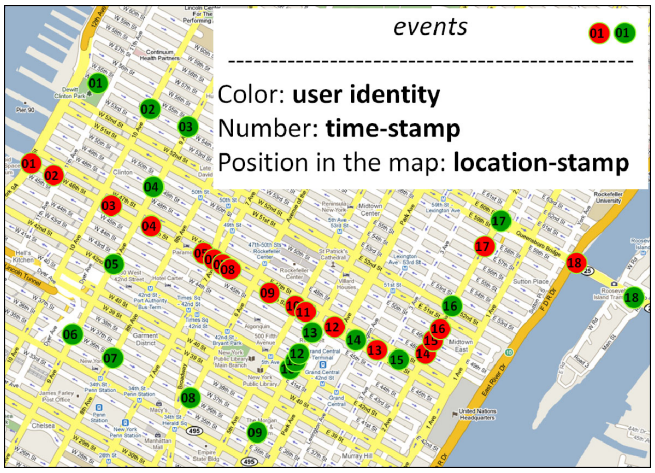
保护位置隐私的手段

- 数据混淆：保留身份，混淆位置信息中的其他部分，让攻击者无法得知用户的确切位置
- 对位置信息的数据进行混淆，不提供精确坐标，而以模糊说明性语句代替：
  - 模糊范围：精确位置->区域
  - 声东击西：偏离精确位置
  - 含糊其辞：引入语义词汇，例如“附近”

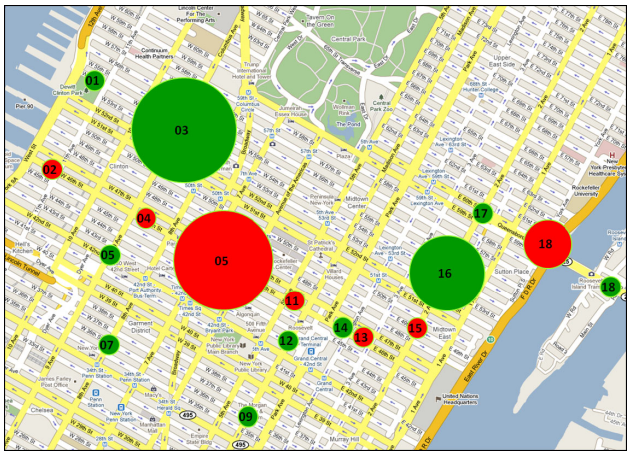
保护位置隐私的手段

- 数据混淆：保留身份，混淆位置信息中的其他部分，让攻击者无法得知用户的确切位置
  - 优点
    - ✓服务质量损失相对较小
    - ✓不需中间层，可定制性好
    - ✓支持需要身份信息的服务
  - 缺点：
    - ✓运行效率低
    - ✓支持的服务有限

用户位置的精确信息



数据混淆：模糊范围



物联网与定位

- 在物联网时代，各种自动服务离不开位置信息的支持，如：
  - 自动导航
  - 搜索周边服务信息
  - 基于位置的社交网络：Four square
- 位置信息不是单纯的“位置”
  - 地理位置（空间坐标）
  - 处在该位置的时刻（时间坐标）
  - 处在该位置的对象（身份信息）

主流的定位系统

- 卫星定位
- 蜂窝基站定位
- 无线室内环境定位
- 新兴定位系统：A-GPS，网络定位

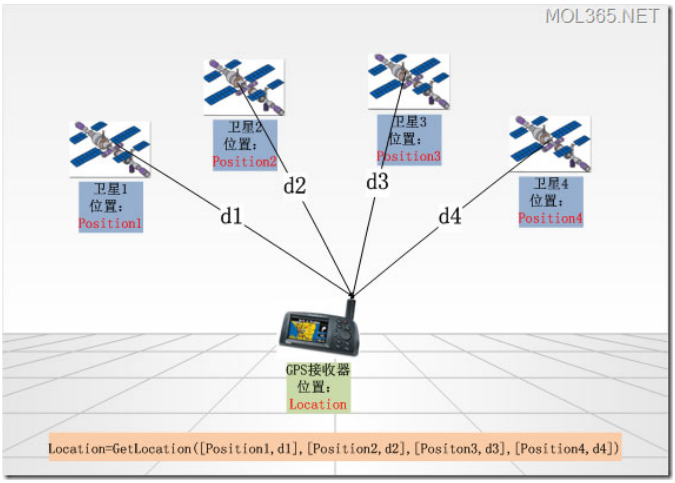
主流的定位系统

- 卫星定位：
  - 美国：GPS，是目前世界上最常用的卫星导航系统
  - 俄罗斯：GLONASS
  - 欧盟：伽利略
  - 中国：北斗一号（区域）、北斗二号（全球）
- 蜂窝基站定位
- 无线室内环境定位
- 新兴定位系统：A-GPS，网络定位

GPS系统结构

- 宇宙空间部分
  - 24颗工作卫星
- 地面监控部分（全部在美国境内）
  - 1个主控中心（另有1个备用）
  - 4个专用地面天线
  - 6个专用监视站
- 用户设备部分
  - GPS接收机

GPS：定位原理

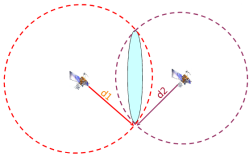


GPS：定位原理

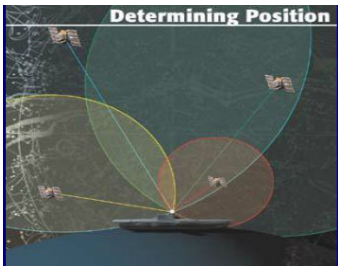
- GPS定位需要用到4颗卫星
- 已知Position1、Position2、Position3、Position4分别为四颗卫星的当前位置（空间坐标）
- 已知 d1、d2、d3、d4分别为四颗卫星到要定位的GPS接收器的距离
- Location 为要定位的GPS接收器的位置，与Position和d的关系，可以表示为如下函数形式：
  - Location=GetLocation([Position1,d1],[Position2,d2],[Position3,d3],[Position4,d4]);

GPS：定位原理

- 两个球面交集是一个圆
- 三个球面交集是两个点



- 时钟的精度影响定位的精度；引入第4颗卫星是为了消除GPS接收机时间精度不够带来的误差



GPS:典型应用

- 优点：精度高、全球覆盖，可用于险恶环境
- 缺点：
  - 启动时间长
  - 室内信号差
  - 需要GPS接收机
- 最初仅能提供位置和周边地图
- 第二代汽车导航系统可根据目的地自动计算“最短”路线
- 物联网时代，汽车导航可从交管部门取得路况咨询，优化路线，找出“最快”路线

主流的定位系统

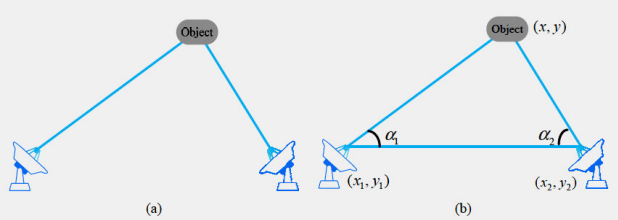
- 卫星定位
- 蜂窝基站定位
  - 通讯区域被分割成蜂窝小区
  - 每个小区对应一个通讯基站
  - 通讯设备连接小区对应基站进行通讯
  - 利用基站位置已知的条件，可对通讯设备进行定位
- 无线室内环境定位
- 新兴定位系统：A-GPS，网络定位

蜂窝基站定位

- COO定位（Cell of Origin）
  - 将移动设备所属基站的位置视为移动设备的位置
  - 精度直接取决于基站覆盖的范围
  - 基站分布疏松地区，一个基站覆盖范围半径可达数公里，误差巨大
- 优点：简单、快速，适用紧急情况

蜂窝基站定位

- ToA/TDoA定位法
  - 需要三个基站才能定位
  - 稀疏地区可能只能收到两个基站的信号，不适用
- AoA定位法



蜂窝基站定位

- 优点
  - 不需要GPS接收机，可通讯即可定位
  - 启动速度慢
  - 信号穿透能力强，室内亦可接收到
- 缺点
  - 定位精度相对较低
  - 基站需要有专门硬件，造价昂贵

蜂窝基站定位

- 典型应用：美国E-911系统
  - 拨打报警电话时，根据基站定位出手机位置，自动接到最近警局
  - 综合了各种定位系统，包括ToA，TDoA，AoA，RSS，A-GPS
  - 使用时尝试各种定位方法，择优而用

主流的定位系统

- 卫星定位
- 蜂窝基站定位
- 无线室内环境定位
  - 采用RSS定位技术
    - 使用信号强度进行定位
    - 短途定位的方法有：红外线、超声波、蓝牙、RFID、蓝牙、Wi-Fi、ZigBee……
- 新兴定位系统：A-GPS，网络定位

无线室内环境定位

- 典型应用：资产管理
  - 在设备上贴上RFID标签
  - 需要使用时通过RFID定位找到标签的位置，从而定位设备的位置
  - 结合感知技术，还可以监控设备的状况
    - ✓ 是否空闲
    - ✓ 是否故障
    - ✓ 是否老化

主流的定位系统

- 卫星定位
- 蜂窝基站定位
- 无线室内环境定位
- 新兴定位系统：A-GPS，无线AP定位、网络定位
  - A-GPS是GPS定位和蜂窝基站定位的结合体
    - ✓利用基站定位确定大致范围
    - ✓基站连接网络查询当前位置可见卫星
    - ✓大大缩短搜索卫星的时间

主流的定位系统

- 卫星定位
- 蜂窝基站定位
- 无线室内环境定位
- 新兴定位系统：A-GPS，无线AP定位，网络定位
  - 无线AP定位
    - ✓类似A-GPS，只是由基站定位改为利用可见的Wi-Fi接入点(AP)来定位
    - ✓在大城市中，无线AP数目多，定位非常精确
    - ✓还可与GPS结合定位，在iPhone中成熟应用

定位技术

- 定位技术的关键：
  - 有一个或多个已知坐标的参考点
  - 得到待定位目标与已知参考点的空间关系
- 定位技术的两个步骤：测量物理量→根据物理量确定目标位置
- 基于测距技术常用的定位方法：
  - 基于距离的定位（ToA）
  - 基于距离差的定位（TDoA）
  - 基于信号特征的定位（RSS）

基于距离的定位（ToA）

- 基本思想：测量目标到多个参考点的距离，然后利用测得的距离和参考点坐标，来计算出目标的距离。
- 第一步：测量距离
  - 距离d = 波速v * 传播时间Δt
  - 传播时间Δt = 收到时刻t – 发出时刻t_0
- 问题：接收端如何得知t_0?

基于距离的定位（ToA）

- 方法1：利用波速差
  - 发送端同时发送一道电磁波和声波，传输速度分别记为v_r和v_s
  - 接收端记录：
    - 电磁波到达时刻 t_r
    - 声波到达时刻 t_s
  - 距离 $d = \dfrac{v_r v_s (t_s - t_r)}{v_r - v_s}$
  - 由于v_r远大于v_s，上式可简化为 $d = v_s (t_s - t_r)$

基于距离的定位（ToA）

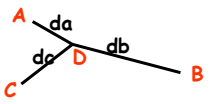
- 方法2：测量波的往返时间 Δt
  - 发送端于时刻 t_0发送波
  - 接收端收到波后，等待时间 t 后返回同样的波
  - 发送端记录收到回复的时间
  - 距离 $d = \dfrac{v(t - t_0 - \Delta t)}{2}$

基于距离的定位（ToA）

- 第二步：位置计算
  - 三边测量
    - 平面上定位，取三个参考点
    - 以每个参考点为圆心，到该参考点的距离为半径画圆，目标必在圆上
    - 平面上三个圆交于一点
  - 实际中取用超过三个参考点，用最小二乘法减少误差

三边测量原理

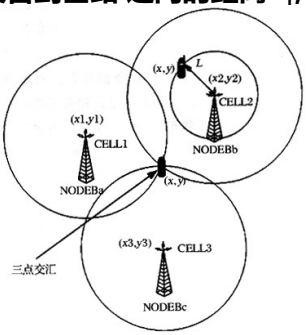
- 已知A，B和C节点的坐标分别为(x_a, y_a)，(x_b, y_b)和(x_c, y_c)，它们到待定位点D的距离分别为d_a，d_b和d_c，假设D的坐标为(x ,y) ,则通过计算可以得到



$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_a - x_c) & 2(y_a - y_c) \\ 2(x_b - x_c) & 2(y_b - y_c) \end{bmatrix}^{-1} * \begin{bmatrix} x_a^2 - x_c^2 + y_a^2 - y_c^2 + d_c^2 - d_a^2 \\ x_b^2 - x_c^2 + y_b^2 - y_c^2 + d_c^2 - d_b^2 \end{bmatrix}$$

基于距离的定位（ToA）

- 例如：三基站定位，得到电波到达时间T_i(i=1,2,3)后，由T_i*c得到设备到基站i之间的距离R_i，然后求得(x,y)。



基于距离差的定位（TDoA）

- ToA的局限
  - 需要参考点和测量目标时钟同步
- 改用TDoA算法
  - 不需要参考点和测量目标时钟同步
  - 参考点之间仍然需要时钟同步

基于距离差的定位（TDoA）

- 第一步：测量距离差
  - 待测目标首先广播一个信号
  - 参考点i，j分别记录信号接收到的时刻t_i，t_j
  - 测量目标到i，j的距离差

$$\Delta d_{ij} = d_i - d_j = v(t_i - t_0) - v(t_j - t_0) = v(t_i - t_j)$$

- 优点：只需要接收端的时钟保持同步即可

基于距离差的定位（TDoA）

- 第二步：计算待测目标的位置
  - 至少两组数据联立方程求解
  - 实际采用多组数据最小二乘法求解
  - 每次测量结果
    - 参考点坐标(x_j, y_j)，(x_i, y_i)
    - 到参考点的距离 Δd_{ij}
    - 构建方程：

$$\left[(x - x_i)^2 + (y - y_i)^2\right] - \left[(x - x_j)^2 + (y - y_j)^2\right] = \Delta d_{ij}^2$$

基于信号特征的定位

- ToA和TDoA都需要接收端特殊装置
- 基于信号特征的定位直接利用无线通信的射频信号定位，不需要额外设备
- 原理：信号强度随传播距离衰减

$$P_r(d)=\left(\frac{\lambda}{4\pi d}\right)^2 P_t G_t G_r$$

- 问题：理想公式实际难以应用

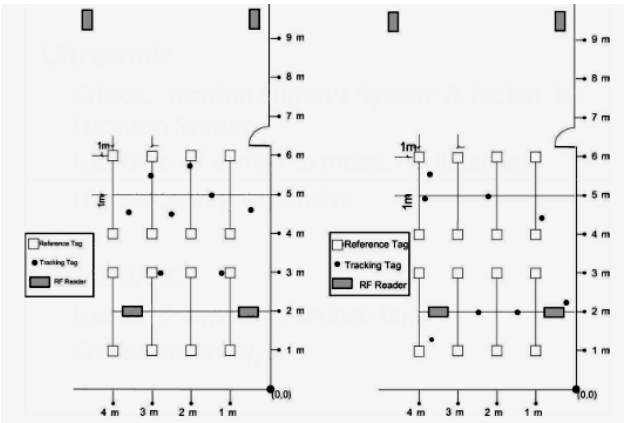
基于信号特征的定位

- 解决方法：
  - 将信号强度看做“特征”
  - 预先布置N个参考节点
  - 测出N个参考节点信号的强度，得到一个N维向量
  - 事先测出区域中每个位置的特征向量
  - 将目标测出的特征向量和事先测量值比对，找出位置
- 缺点：不能应对动态变化

基于信号特征的定位

- LANDMARC：基于信号特征的动态定位方法
  - 除了信号发送源，再布置一系列RFID标签作为参考标志
  - 每个标志随时记录自己收到的RSS信号强度特征向量
  - 将目标测得的信号特征向量与参考标志此时的特征向量进行比对，确定位置，误差在1m范围以内

LANDMARC布局的一个例子



无线网络对物联网的支持

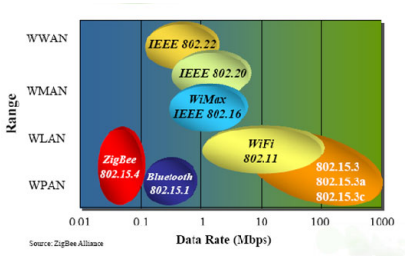
- 如何将数量庞大的轻型移动设备(手机、平板电脑等)稳定、高速的连入因特网？
  - 无线高速宽带网络消除了有限网络队接入设备位置的限制
- 无线宽带网络包括：
  - Wi-Fi：无线局域网
  - WiMAX：无线城域网
  - 3G：无线广域网
  - UWB：超宽带无线个域网

为什么需要无线低速网络?

- 物联网连接的不仅是传统意义上的主机节点，物联网背景下连接的物体，既有智能的也有非智能的，它们很难通过路由器、交换机等设备有组织的级联，因此，适用于互联网的高速无线网络协议不能完全满足物联网的需求。
- 需要对物联网中各种各样的物体进行操作的前提就是先将他们连接起来，低速网络协议是实现全面互联互通的前提。
- 无线低速网络适应物联网中那些能力较低的节点
  - 低速率、低通信半径、低计算能力，低能耗

无线低速网络协议

- 典型的无线低速网络协议：
  - 蓝牙
  - 红外
  - 802.15.4/ZigBee



蓝牙（Bluetooth）

- 蓝牙技术是一种短距离低功耗传输协议，最早始于1994年，由瑞典的爱立信公司研发。
- 采用的是调频技术（frequency-hopping spread spectrum），频段范围是2.402GHz-2.480GHz。
- 通信速率一般能达到1Mbps左右，新的蓝牙标准也支持超过20Mbps的速率。
- 通信半径从几米到100米左右不等，常见为几米左右。

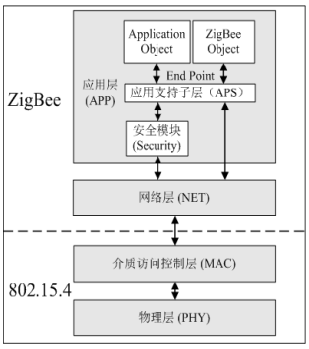
蓝牙和Wi-Fi区别

- Wi-Fi的定位目标是为了取代网络应用中的有线设备，能够真正的实现从有线到无线的转变，他可以用来传送各种文件，视频，音频，实现互联网的各种应用。
- 蓝牙主要是为了替换一些个人用户携带设备的有线，如耳机，键盘等。这些设备对带宽的要求相对较少，或者说不是经常使用，比如手机间的传送小文件，或者说这些设备的资源拥有量（电量，计算资源等等）相对较低。

红外（Infrared）

- 红外通信技术利用红外线传输数据，是一种蓝牙技术出现更早的无线通信技术。
- 特点
  - 红外通信采用的是875nm左右波长的光波通信，通信距离一般为1米左右。
  - 设备体积小、成本低、功耗低、不需要频率申请等优势
- 缺点
  - 设备之间必须互相可见
  - 对障碍物的衍射较差

802.15.4/ZigBee



- 802.15.4/ZigBee
- 是无线传感网领域最为著名的无线通信协议
- ZigBee主要定义了网络层、传输层以及之上的应用层的规范
- 802.15.4主要定义了短距离通信的物理层以及链路层规范

802.15.4 物理层

- 频段：3个频段，均为国际电信联盟电信标准化组定义的用于科研和医疗的开放频段，包括
  - 868.0-868.6MHz，主要为欧洲采用，单信道；
  - 902-928MHz，北美采用，10个信道，支持扩展到30；
  - 2.4-2.4835GHz世界范围内通用，16个频道。
- 传输技术：最早为直接扩频，后来可采用调频、调相等多种技术。

802.15.4介质访问控制层

- 介质访问控制层（MAC）控制和协调节点使用物理层的信道
- 802.15.4采用载波侦听多路访问方式(CSMA/CA)，与802.11（Wi-Fi）类似。
  - 传输之前，先侦听介质中是否有使用同一信道的载波存在，若不存在说明信道空闲，将直接进入数据传输状态
  - 若系统检测到存在载波，则在随机退避一段时间后重新检测信道，退避的时间长短由具体的协议指定。

ZigBee 网络层

- ZigBee网络层采用距离矢量路由协议（AODV）
  - 源节点广播一个路由请求给它的所有邻居
  - 邻居节点在收到消息后，再广播收到的消息给它们的邻居，如此直到消息到达目的节点。
  - 当目的节点收到路由请求消息以后，目的节点返回一个路由回复给源节点。
  - 回复不再以广播方式发送到源节点，而是沿着路由请求数据包从源节点到目的节点的路径，这样源节点就可以按照这条路径发送消息到目的节点了。

ZigBee 网络层以上

- 网络层以及上提供了向终端用户的接口
- 与互联网类似，在网络层以上：
  - 互联网模型中需要提供不同类型的传输服务（比如TCP协议和UDP协议）
  - 在传输协议上还需要提供各种基于不同传输协议的应用（比如FTP，HTTP等等）。

本章结束