

第14章

物联网中的信息 安全与隐私保护

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。

本章将重点讨论**RFID安
全和位置隐私**两大安全
隐私问题。

内容提要

内容回顾

- 第13章介绍了物联网的智能决策——数据挖掘技术。
 - 数据挖掘的基本流程
 - 典型的数据挖掘算法
 - 物联网中数据挖掘技术的广泛应用
- 本章重点介绍物联网中RFID安全和位置隐私隐患以及典型的安全机制。

本章内容

14.1 概述

14.2 RFID安全和隐私

14.3 RFID安全和隐私保护机制

14.4 位置信息与个人隐私

14.5 保护位置隐私的手段

网络安全的一般性指标有哪些？

网络信息安全的一般性指标

可靠性： 三种测度标准（抗毁、生存、有效）

可用性： 用正常服务时间 和整体工作时间之比衡量

保密性： 常用的保密技术（防侦听、防辐射、加密、物理保密）

完整性： 未经授权不能改变信息；与保密性的区别：保密性要求信息不被泄露给未授权的人，完整性要求信息不受各种原因破坏。

不可抵赖性： 参与者不能抵赖已完成的操作和承诺的特性

可控性： 对信息传播和内容的控制特性

什么是隐私？

隐私权：个人信息的自我决定权，包含个人信息、身体、财产或者自我决定等。

物联网与隐私

- 不当使用会侵害隐私
- 恰当的技术可以保护隐私



本章内容

14.1 概述

14.2 **RFID安全和隐私**

14.3 RFID安全和隐私保护机制

14.4 位置信息与个人隐私

14.5 保护位置隐私的手段

RFID安全的现状如何？有哪些主要安全和隐私隐患？

RFID安全现状概述

RFID安全隐私标准规范和建议

EPC (Electronic Product Code)，即产品电子代码，为每一件产品建立全球的、开放的标识标准，实现全球范围内对单件产品的跟踪与追溯。

•EPCglobal在超高频第一类第二代标签空中接口规范中说明了RFID标签需支持的功能组件，其安全性要求有：

ü物品级标签协议要求文档

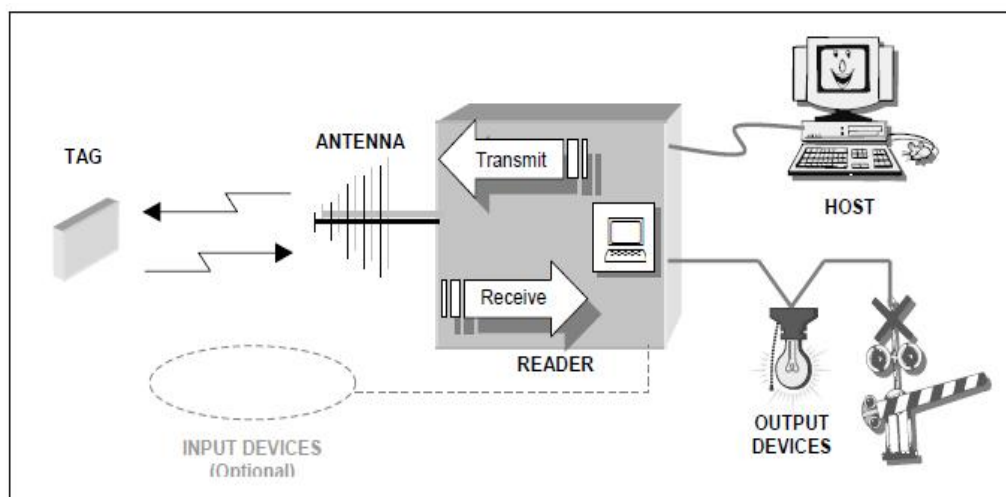
üISO/IEC：RFID数据安全准则

•欧盟：《RFID隐私和数据保护的若干建议》



RFID系统

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系统分为阅读器、天线和标签三大组件，这三大组件一般都可由不同的生厂商生产。**服务器**



RFID标签成本

5000-10000个逻辑门

Hash算法3000-4000个逻辑门

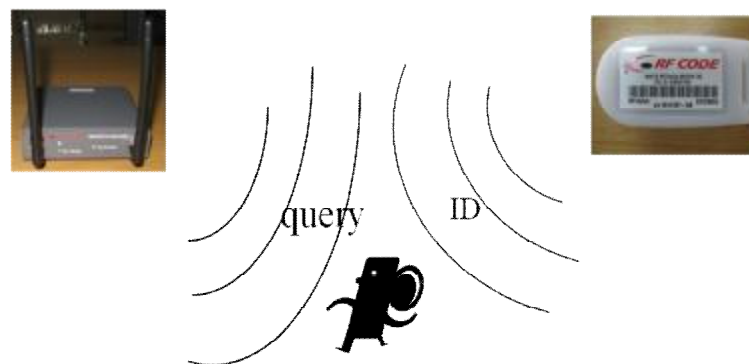
公钥加密算法 很难

阅读器和服务器-支持复杂运算

主要安全隐患

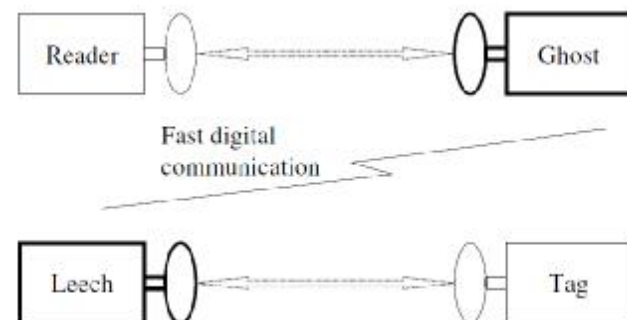
窃听(eavesdropping)

- 标签和阅读器之间通过无线射频广播通信
- 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
- “扒手”系统



主要安全隐患

欺骗、重放、克隆

- 欺骗(spoofing): 基于已掌握的标签数据通过阅读器（超市购物）
- 重放(replaying): 将标签的回复记录并回放
- 克隆(cloning): 形成原来标签的一个副本（门禁系统）

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：
 - ü 产生标签冲突，影响正常读取
 - ü 发起认证消息，消耗系统计算资源
- 对标签的DoS
 - ü 消耗有限的标签内部状态，使之无法被正常识别

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
 - ü 推测此标签之前发送的消息内容
 - ü 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
- 欧洲麦德龙 RFID 系统
自动结算 - EPC 数据区改写

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
 - ü SQL注入
 - ü 缓冲区溢出

其他隐患

- 电子破坏
- 屏蔽、干扰
- 拆除
- ...



主要隐私问题

隐私信息泄露

明文传输

- 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
- 快速验证标签需要知道标签身份，才能找到需要的信息
- **平衡：** 恰当、可用的安全和隐私



Two RFID researchers created a video showing how an RFID reader attached to an improvised explosive device could theoretically identify a U.S. citizen walking past the reader and set off a bomb. They haven't yet tested the theory on a real U.S. passport since the documents have yet to be distributed. The still here shows an attack using a prototype passport with RFID chip placed in the pocket of the victim. As the chip passes the reader, the reader detonates an explosive device placed in the trash can. View Slideshow 

本章内容

14.1 概述

14.2 RFID安全和隐私

14.3 **RFID安全和隐私保护机制**

14.4 位置信息与个人隐私

14.5 保护位置隐私的手段

典型的隐私保护机制有哪些？

14.3 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。

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

哈希锁(hash-lock) MIT&AutoID 阅读器 $\text{metaID} = \text{hash}(\text{key})$ 写入标签 锁定

解锁



数据库

← metaID
→ (key, ID)



阅读器

—— 查询 ——→
← metaID ——

—— key ——→
← ID ——



标签

优点：初步访问控制

威胁：偷听（key明文），跟踪

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

随机哈希锁(randomized hash-lock) 标签及阅读器 哈希函数+伪随机数



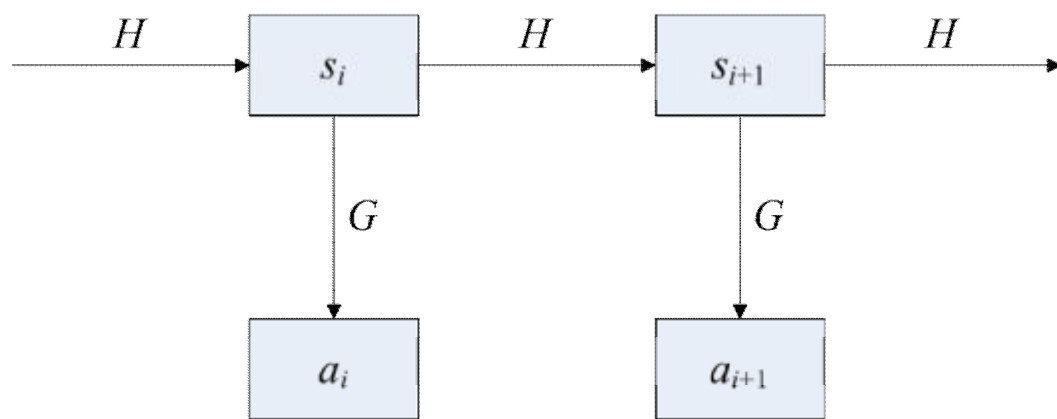
线性复杂度key-search: $O(M)$ 耗时

优点: 增强的安全和隐私 防跟踪, 不防重放攻击

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

哈希链(hash chain) 标签及阅读器 G - 响应 H - 更新 初始化标识符s



穷举

优点: 前向安全性

威胁: DoS 同步

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

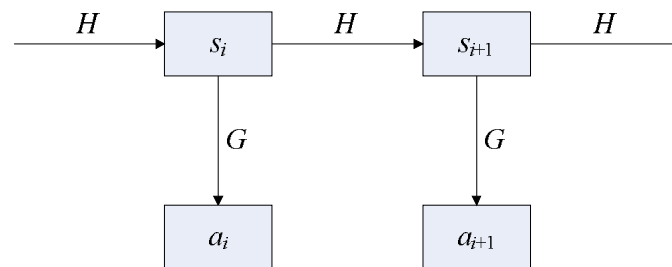
同步方法(synchronization approach)

- 预计算并存储标签的可能回复（状态），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



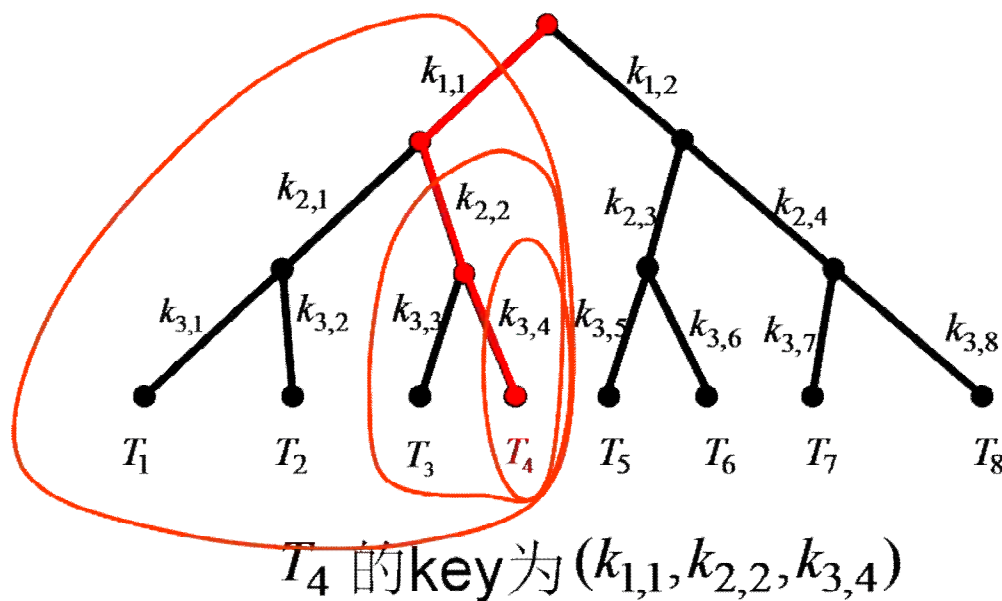
$$s_{i+k} = H^k(s_i), (0 \leq k \leq m-1)$$

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

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

树形协议(tree-based protocol)



标签认证:

1 阅读器 – 查询, 随机数 r_1

2 标签 – 随机数 r_2 ,
 $h(k_1, r_1, r_2), h(k_2, r_1, r_2), h(k_3, r_1, r_2)$

3 阅读器从根开始搜索树

树深

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

树形协议(tree-based protocol)（续） 标签空间 d 个密钥，多次哈希计算
对数复杂度key-search: $O(\log N)$ ，受破解攻击威胁，攻击成功率：

$\delta \backslash K_0$	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)

14.3 RFID安全和隐私保护机制

其他方法

- Physical unclonable function, (PUF): 利用制造过程中必然引入的随机性，用物理特性实现函数。具有容易计算，难以特征化的特点。PUF电路尺寸极小，成本低，可保护密钥。
- 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，（图像处理）
- 可拆卸天线
- 带方向的标签

如何面对安全和隐私挑战？

- 可用性与安全的统一

无需为所有信息提供安全和隐私保护，信息分级别管理。

- 与其他技术结合

- ü 生物识别 指纹等

- ü 近场通信(Near field communication, NFC)

- 法律法规

从法律法规角度增加通过**RFID**技术损害用户安全与隐私的代价，并为如何防范做出明确指导。

近场通讯（NFC）

- 近场通讯（NFC）是Near Field Communication缩写，即近距离无线通讯技术，是由非接触式射频识别(RFID)及互连互通技术整合演变而来，通过在单一芯片上集成阅读器、标签和点对点通信的功能。
- NFC工作在13.56MHz频率范围，作用距离约10-20厘米，兼容ISO 14443、ISO 15693、Felica等射频标准。
- 计算能力比RFID强，界面友好，安全性提高。
- 数据传输速度可以选择106Kb/s、212Kb/s或者 424Kb/s，将来可提高至1Mb左右，不适合音视频流等需要较高带宽的应用。与蓝牙、WiFi等技术在不同的场合、不同的领域起到相互补充的作用。
- 在智能手机等移动终端实现移动支付、电子票务、门禁、移动身份识别、防伪等应用。

NFC工作模式

- 卡模拟模式（**Card emulation mode**）：这个模式其实就是相当于一张采用**RFID**技术的**IC**卡。可以替代现在大量的**IC**卡（包括信用卡）场合商场刷卡、悠游卡、门禁管制，车票，门票等等。此种方式下，有一个极大的优点，那就是卡片通过非接触读卡器的**RF**域来供电，即便是寄主设备（如手机）没电也可以工作。**NFC**设备若要进行**Card Emulation** 相关应用，则必须内置安全组件(**Security Element, SE**)的**NFC**芯片。
- 点对点模式（**P2P mode**）：这个模式和红外线差不多，可用于数据交换，只是传输距离较短，传输创建速度较快，传输速度也快些，功耗低（类似蓝牙）。将两个具备**NFC**功能的设备连接，能实现数据点对点传输，如下载音乐、交换图片或者同步设备地址簿。因此通过**NFC**，多个设备如数码相机、**PDA**、计算机和手机之间都可以交换资料或者服务。
- 读卡器模式（**Reader/Writer mode**）：作为非接触读卡器使用，比如从海报或者展览信息电子标签上读取相关信息。

NFC与RFID区别

- **NFC**将非接触读卡器、非接触卡和点对点功能整合进一块单芯片，而**RFID**必须有阅读器和标签组成。**RFID**只能实现信息的读取以及判定，而**NFC**技术则强调的是信息交互。通俗的说**NFC**就是**RFID**的演进版本，双方可以近距离交换信息。**NFC**手机内置**NFC**芯片，组成**RFID**模块的一部分，可以当作**RFID**无源标签使用进行支付费用；也可以当作**RFID**读写器，用作数据交换与采集，还可以进行**NFC**手机之间的数据通信。
- **NFC**传输范围比**RFID**小，**RFID**的传输范围可以达到几米、甚至几十米，但由于**NFC**采取了独特的信号衰减技术，相对于**RFID**来说**NFC**具有距离近、带宽高、能耗低等特点。
- 应用方向不同。**NFC**看更多的是针对于消费类电子设备相互通讯，有源**RFID**则更擅长在长距离识别。

手机作为互联网最直接的智能终端，**NFC**将同蓝牙、**USB**、**GPS**一样成为标配，通过**NFC**技术，手机支付、看电影、坐地铁都能实现，将在我们的日常生活中发挥更大的作用。

与蓝牙的比较

- **NFC**和蓝牙都是短程通信技术，而且都被集成到移动电话。但**NFC**不需要复杂的设置程序。**NFC**也可以简化蓝牙连接，省去配对过程。
- **NFC**略胜蓝牙的地方在于设置程序较短，但无法达到低功率蓝牙（**Bluetooth Low Energy**）的传输速率。在两台**NFC**设备相互连接的设备识别过程中，使用**NFC**来替代人工设置会使创建连接的速度大大加快：少于十分之一秒。**NFC**的最大数据传输量**424 kbit/s**远小于**Bluetooth V2.1 (2.1 Mbit/s)**。虽然**NFC**在传输速度与距离比不上蓝牙（小于**20 cm**），但相应可以减少不必要的干扰。这让**NFC**特别适用于设备密集而传输变得困难的时候。
- 相对于蓝牙，**NFC**兼容于现有的被动**RFID (13.56 MHz ISO/IEC 18000-3)**设施。**NFC**的能量需求更低，与蓝牙**V4.0**低能协议类似。当**NFC**在一台无动力的设备（比如一台关机的手机，非接触式智能信用卡，或是智能海报）上工作时，**NFC**的能量消耗会大于低功率蓝牙**V4.0**。
- 对于移动电话或是行动消费性电子产品来说，**NFC**的使用比较方便。**NFC**的短距离通信特性正是其优点，由于耗电量低、一次只和一台机器连接，拥有较高的保密性与安全性，**NFC**有利于信用卡交易时避免被盗用。**NFC**的目标并非是取代蓝牙等其他无线技术，而是在不同的场合、不同的领域起到相互补充的作用

支持NFC通信的操作系统与软件

- Android
- Windows Phone 8
- Windows 8

NFC手机一卡通、智能钱包

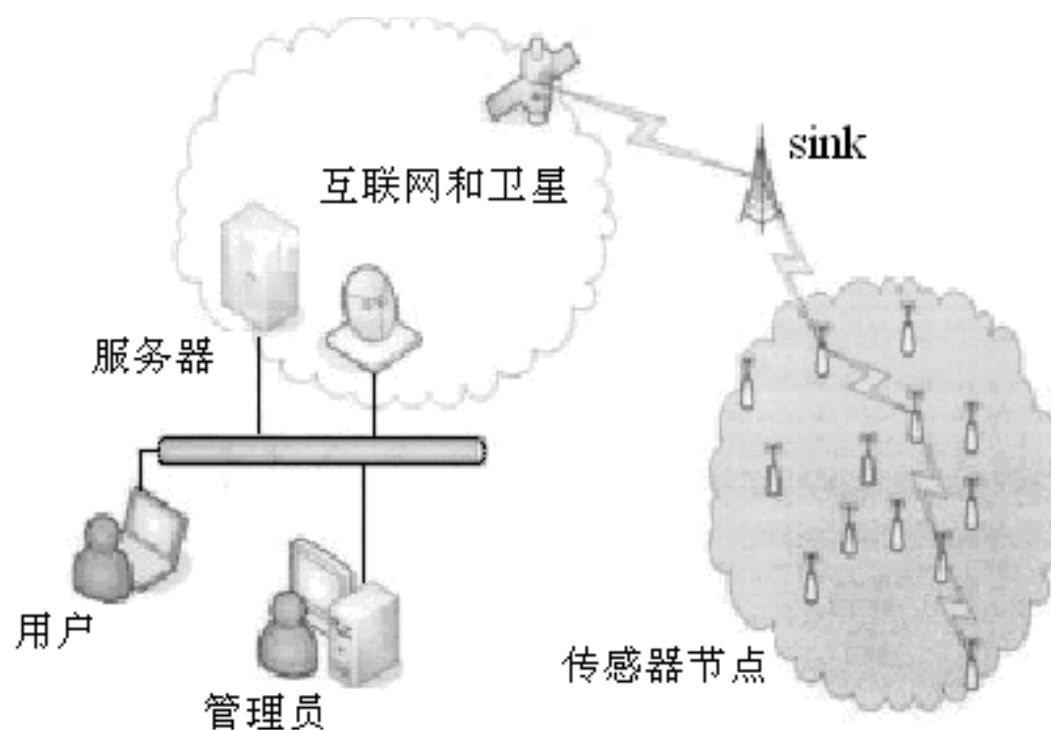
- 内置NFC的设备
手机、笔记本电脑、平板电脑
HTC、三星、诺基亚、索尼、LG
- iPhone 5不支持 NFC， iPhone 6的NFC功能只在ApplePay运用。

传感器网络安全

- 1 传感器网络结构
- 2 传感器网络安全威胁分析
- 3 传感器网络安全防护主要手段
- 4 传感器网络典型安全技术

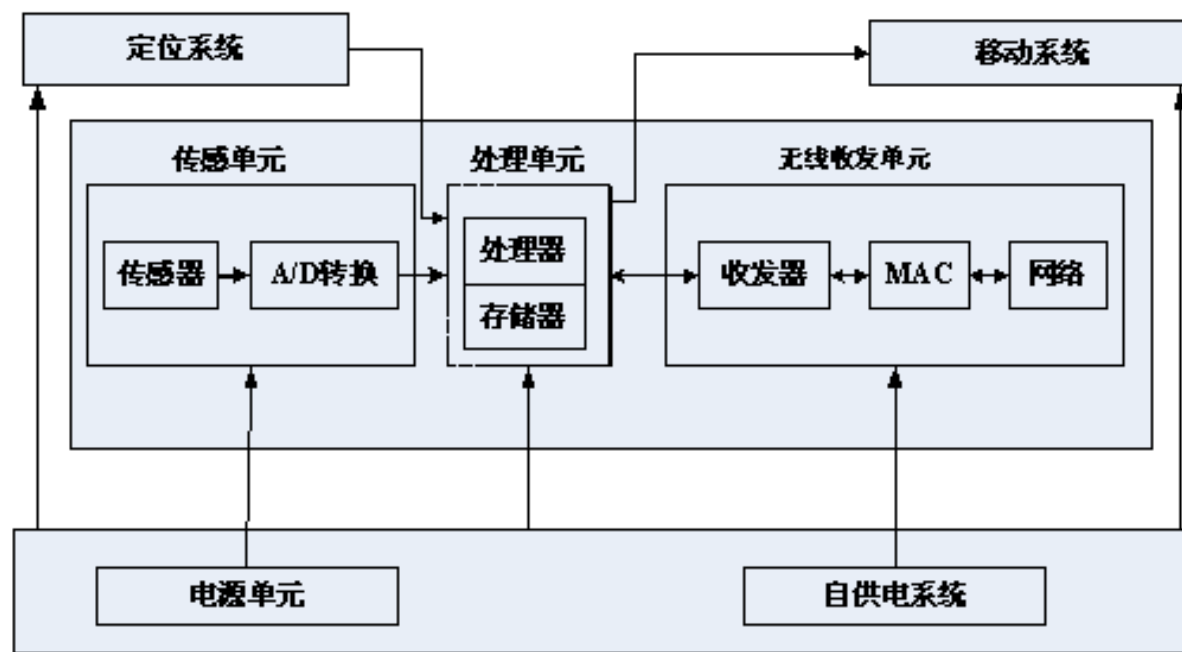
1 传感器网络结构

在实际应用中，无线传感器网络结构如图所示：监控区域内的节点，对感兴趣的数据进行采集、处理、融合，并通过汇聚节点(Sink)路由到基站，用户可以通过卫星或互联网进行查看、控制整个网络。



传感器节点结构

传感器节点由传感器模块、处理器模块、无线通信模块和能量供应模块四部分组成



传感器网络安全威胁分析

1) 外部攻击

外部攻击是攻击者未被授权的加入传感器网络中的攻击方式。由于传感器网络的通信采用无线信道，一个被动攻击者可以在网络的无线频率范围内轻易的窃听信道上传送的数据，从而获取隐私或者机密信息。

2) 内部攻击

节点被俘获是无线传感器网络所面临的一个最大的安全威胁。如果网络中的一个节点一旦被敌手俘获，攻击者就可以利用这个叛逆节点发起内部攻击。

技术分类

物理层攻击

(1) 信号干扰和窃听攻击 (2) 篡改和物理破坏攻击 (3) 仿冒节点攻击

链路层安全威胁

(1) 链路层碰撞攻击 (2) 资源消耗攻击 (3) 不公平竞争

网络层的安全威胁

(1) 虚假路由攻击 (2) 选择性地转发 (3) **Sinkhole** 槽洞攻击
(4) **DoS** 拒绝服务攻击 (5) **Sybil** 女巫攻击 (6) **Wormholes** 虫洞攻击
(7) **HELLO** 洪泛攻击 (8) 确认欺骗 (9) 被动窃听

传输层攻击

(1) 洪泛攻击 (2) 重放攻击

1.物理层防护手段

1) 无线干扰攻击

- (1) 单频点的无线干扰攻击，使用宽频和跳频的方法比较有效。
- (2) 全频长期持续无线干扰攻击，唯一有效的方法是转换通信模式。
- (3) 有限时间内的持续干扰攻击，传感器节点可以在被攻击的时候，不断降低自身工作的占空比，并定期检测攻击是否存在，当感知到攻击终止以后，恢复到正常的工作状态。
- (4) 间歇性无线干扰攻击，传感器节点可以利用攻击间歇进行数据转发。

2) 物理篡改攻击

- (1) 增加物理损害感知机制
- (2) 对敏感信息进行加密存储
- (3) 对节点进行物理伪装和隐藏

3) 仿冒节点攻击

2.链路层攻击

1) 链路层碰撞攻击

- (1) 纠错编码。
- (2) 信道监听和重传机制。

2) 资源消耗攻击

- (1) 限制网络发送速度，节点自动抛弃多余数据请求，但会降低网络效率。
- (2) 在协议实现时制定一些策略，对过度频繁的请求不予理睬，或者限制同一个数据包的重传次数等。

3) 非公平竞争

- (1) 短包策略，不使用过长的数据包，缩短每包占用信道的时间。
- (2) 不采用优先级策略或者弱化优先级差异，可以采用时分复用或者竞争的方式进行数据传输。

3.网络层攻击防御手段

1) 外部攻击的防御

- (1) 对于WSN网络层的外部被动窃听攻击，可以采用加密报文头部或假名变换等方法隐藏关键节点的位置和身份，采用延时、填充等匿名变换技术实现信息收发的逻辑隔离，增大攻击者的逻辑推理难度。
- (2) 对于WSN网络层的大部分外部主动攻击，如外部女巫、告知收到欺骗和HELLO洪泛攻击等，可以通过使用链路层加密和认证机制来防御
- (3) 由于虫洞和HELLO洪泛攻击方式不对数据包内部做任何改动。采用单纯应用密码学知识不能完全抵御这类破坏。

2) 内部攻击的防御

对于内部攻击者或妥协节点而言，使用全局共享密钥的链路层安全机制毫无作用，须考虑采用其它机制抵御这些攻击。

4.传输层的安全威胁

1) 洪泛攻击

(1) 限制连接数量和客户端谜题的方法进行抵御。要求客户成功回答服务器的若干问题后再建立连接，它的缺点是要求合法节点进行更多的计算、通讯和消耗更多的能量。

(2) 入侵检测机制。引入入侵检测机制，基站限制这些泛洪攻击报文的发送。如规定在一定时间内，节点发包数量不能超过某个阈值。

2) 重放攻击。可以通过对数据包赋予时效性来抵御重放攻击，在加密的数据包里添加时间戳或者通过报文鉴别码**MAC**对所有报文(传输协议中包头的控制部分)进行鉴别，发现并防止攻击者通过伪造报文来破坏同步机制。

1.传感器网络加密技术

1) 对称密钥加密算法

- (1) TEA加密算法。
- (2) RC5, RC6加密算法。

2) 非对称密钥加密算法

- (1) RSA。
- (2) Diffie-Huffman。
- (3) 椭圆曲线密码算法ECC。

2. 传感器网络密钥管理技术

传感器网络密钥管理研究主要考虑的因素包括：

- ①机制能安全地分发密钥给传感器节点；
- ②共享密钥发现过程是安全的，能防止窃听、仿冒等攻击；
- ③部分密钥泄漏后对网络中其他正常节点的密钥安全威胁不大；
- ④能安全和方便地进行密钥更新和撤销；
- ⑤密钥管理机制对网络的连通性、可扩展性影响小，网络资源消耗少等。

2. 传感器网络密钥管理技术

1) 基于公开密钥的密钥管理

DavidJ. Malan等人提出了基于椭圆曲线的密钥管理机制。在MICA2平台上，它能在34秒内产生公钥和完成私钥分发。RonaldWatro等人在TinyPk中设计实现了基于PKI技术的加密协议，该协议使得第三方加入传感器网络时，可以安全地传输会话密钥给第三方。

2) 基于随机密钥预分配的密钥管理

这种方法的优点是实现了端到端的加密，并且很容易在新节点加入时进行密钥分配。缺点是攻击者能根据窃听到的密钥 和捕获的密钥，构造出一个优化的密钥集合，这就可能造成整个网络的密钥失效。

2. 传感器网络密钥管理技术

3) 基于密钥分类的密钥管理

SeneunZhu等人在LEAP中，根据不同类型的信息交换需要不同的安全要求(如路由信息广播无需加密而传感器送到基站的信息必须加密等)，提出了每个节点应该拥有四种不同类型的密钥：和基站共享的密钥，与其他节点共享的对密钥，和邻居节点共享的簇密钥，及与所有节点共享的密钥。

4) 基于位置的密钥管理

DonggangLiu等提出了一种用于静态传感器网络的基于位置的密钥安全引导方案。该方案是对随机密钥对模型的一个改进方案，它基于位置的对密钥分配中提出了位置最近对密钥预分配机制和基于双变量多项式的位置对密钥分发机制。

2. 传感器网络密钥管理技术

5) 基于多密钥空间的对密钥预分配模型

基于多密钥空间(**Multi-Space**)的对密钥机制能有效提高基于单密钥机制的安全性。它是密钥池机制和单密钥空间机制的结合。配置服务器随机生成一个含有**m**个不同密钥空间的池。如果两个相邻节点有一个以上的密钥空间相同，它们能通过此单个密钥空间机制建立对密钥。

6) 基于多路径密钥加强的密钥管理

Anderson和**Perrig**首先提出了基于多路径密钥加强的密钥管理机制。目的是为了解决节点密钥被捕获时，其他未捕获的节点对如**A**、**B**节点也可能共享着这个密钥，这就导致了**AB**链路通信安全存在着严重的威胁。该机制的基本思想是利用多条路径发送加密相关信息，使得网络窃听和密钥捕获更加困难。

3.安全架构和协议

1) 安全协议SPINS

SPINS安全协议主要由安全加密协议**SNEP**（Secure network encryption）和认证流广播**TESLA**（Microtime deficient striming loss-tolerant）两部分组成。**SNEP**主要考虑加密，双向认证和新鲜数据(freshdata)。而**uTESLA**主要在传感器网络中实现认证流安全广播。

2) 安全链路层架构TinySee

TinySee是一种无线传感器网络的安全链路层架构，它的设计主要集中考虑数据包鉴别，完整性和数据加密等方面。加密方法采用**Skipjack**块加密方法或**RC5**。

3) 基于基站和节点通信的安全架构

Avancha等人假设传感器节点仅仅向计算能力很强且安全的基站报告数据，提出了基站与节点通信的安全架构。该架构使用二种密钥。一是基站和所有传感器共享的**64**位密钥，另一个是基站单独和每个传感器节点j共享的密钥足。

3.安全架构和协议

4) 安全级别分层架构

Slijepcevic等人提出了根据不同安全级别进行不同级别加密的分层模型，目的是为了平衡传感器网络安全和资源消耗。文献认为最重要的是移动应用码，并且这些包通信不频繁，适合采用比较高的安全机制。

5) 安全协议LiSP

TacjoonPark等提出了一种轻量级的安全协议LiSP。LiSP由一个入侵检测系统和临时密钥TK管理机制组成。前者用于检测攻击节点，后者用于对临时密钥TK的更新，防止网络通信被攻击。

6) 基于路由的入侵容忍机制

Deng等人提出了基于路由的无线传感器网络安全机制INSENS。INSENS包含路由发现和数据转发两个阶段。在路由发现阶段，基站通过多跳转发向所有节点发送一个查询报文，相邻节点收到报文后，记录发送者的ID，然后发给那些还没收到报文的相邻节点，以此建立邻居关系。

4.传感器网络安全路由技术

1) DirectedDiffusion协议

DirectedDiffusion是一个典型的以数据为中心的、查询驱动的路由协议，路由机制包含兴趣扩散、梯度建立以及路径加强三个阶段。**DirectedDiffusion**是一个高效的以数据为中心的传感器网络路由协议，虽然维持多条路径的方法极大地增强了**DirectedDiffusion**的健壮性，但是由于缺乏必要的安全防护，**DirectedDiffusion**仍然是比较脆弱的。

2) Rumor协议

Rumor算法适合应用在数据传输量较少的传感器网络中，该协议借鉴了欧氏平面图上任意两条曲线交叉几率很大的思想，**Rumor**算法的基本思想是：事件发生区域的节点创建称为**Agent**的数据包，数据包内包含事件和源节点信息，然后将其按一条路径或多条路径随机在网络中转发，收到**Agent**的节点根据事件和源节点信息建立反向路径，并将**Agent**再次发向相邻节点。

4.传感器网络安全路由技术

3) LEACH协议

LEACH是一种自适应分簇的层次型、低功耗路由算法，该协议的主要特征是：按周期随机选举簇头、动态的形成簇、与数据融合技术相结合。每一个周期(或每一轮)分为簇头选举阶段和稳定阶段。

4) TEEN协议

TEEN也是一个层次型的路由协议，利用门限过滤的方式来减少数据传输量，该协议采用和**LEACH**相同的形成簇的方式，但是**TEEN**不要求节点具有较大的通信能力，簇头根据与**BS**距离的不同形成层次结构。

5) GPSR协议

GPSR是一个典型的基于位置的路由协议，在该协议中，每个节点只需知道邻居节点和自身的位置，即可利用贪心算法转发数据。在贪心算法中，接到数据的节点，搜索它的邻居节点表，如果邻居节点到**BS**的距离小于本节点到**BS**的距离，则转发数据到邻居节点。

4.传感器网络安全路由技术

6) GEAR协议

和GPSR相似，**GEAR**也是一个基于地理位置信息的路由协议，所不同的是，**GEAR**在选择路由节点时还考虑了节点的能量。**GEAR**路由中，汇聚节点发出查询命令，并根据事件区域的地理位置将查询命令传送到事件区域内距离汇聚节点最近的节点，然后从该节点将查询命令传播到事件区域内的其它节点。

7) 多路径路由

多路径路由研究的首要问题是如何建立数据源节点到目的节点的多条路径。**GanesanD**等提出了一种多路径路由机制。其基本思想是：首先建立从数据源节点到目的节点的主路径，然后再建立多条备用路径；数据通过主路径进行传输，同时利用备用路径低速传送数据来维护数据的有效性；当主路径失败时，从备用路径中选择次优路径作为新的主路径。

5.入侵检测技术

无线传感器网络入侵检测系统与传统网络的入侵检测系统区别较大，主要表现在：

（1）无固定网络基础。无线传感器网络没有业务集中点，入侵检测系统不能很好的统计数据，这要求无线传感器网络的入侵检测系统能基于部分的、本地的信息进行。

（2）通信类型。无线传感器网络的通信链路具有低速率、有限带宽、高误码等特征，断链在无线传感器网络数据传输中是非常常见的，常常会导致检测系统误报警。

（3）可用资源(如能量、CPU、内存等)。传统的入侵检测系统需要的计算量大，无线传感器网络由于可用资源极端受限，入侵检测机制的引入所面临的最大问题就是解决其能耗问题，必须设计出一种轻量级的较少计算和通信开销的入侵检测系统。

6.安全数据融合技术

无线传感器网络存在能量约束，减少传输的数据量能够有效地节省能量，因此在从各个传感器节点收集数据的过程中，节点可以将收集到的信息进行融合，去除冗余信息，从而达到节省能量的目的。

安全数据融合技术是保护传感器网络节点在一个开放的环境中安全地进行数据融合，以保证被融合信息的完整性、认证性和机密性。

第一阶段，融合节点从传感器节点收集原始数据并用特定的融合函数在本地生成融合结果，每一个传感器节点都和融合节点共享一个密钥，以便融合节点证实收到的数据是真实的。

第二阶段，融合节点对融合数据做出承诺，生成承诺标识(如基于 **Merkle HASH** 树结构来生成承诺标识)，确保融合器提交数据后就不能再改变它，否则将被发现。融合节点向主服务器提交融合结果和承诺标识。

第三阶段，主服务器与融合节点基于交互式证明协议来证实结果的正确性。

本章内容

14.1 概述

14.2 RFID安全和隐私

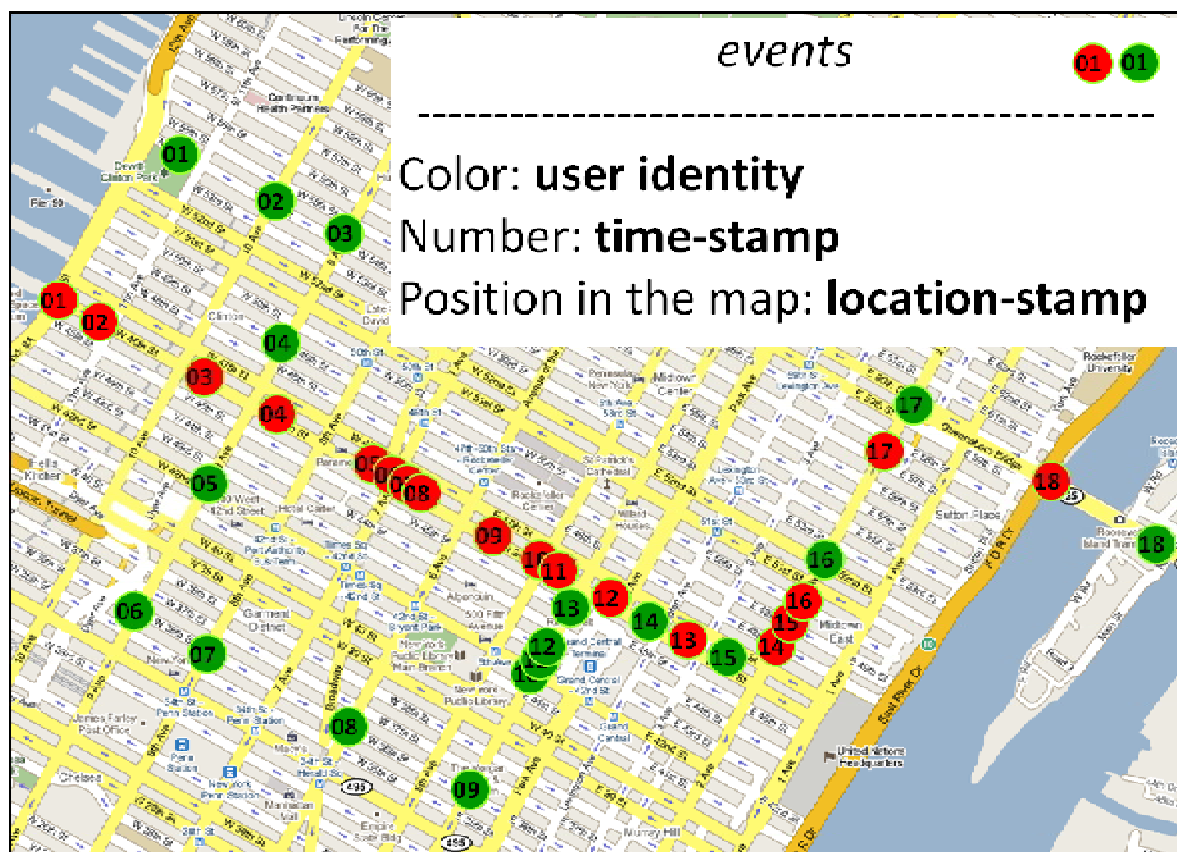
14.3 RFID安全和隐私保护机制

14.4 **位置信息与个人隐私**

14.5 保护位置隐私的手段

什么是位置隐私？

14.4 位置信息与个人隐私



位置信息与基于位置的服务 (LBS)

14.4 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：
 - ü 是否发布
 - ü 发布给谁
 - ü 详细程度

保护位置隐私的重要性

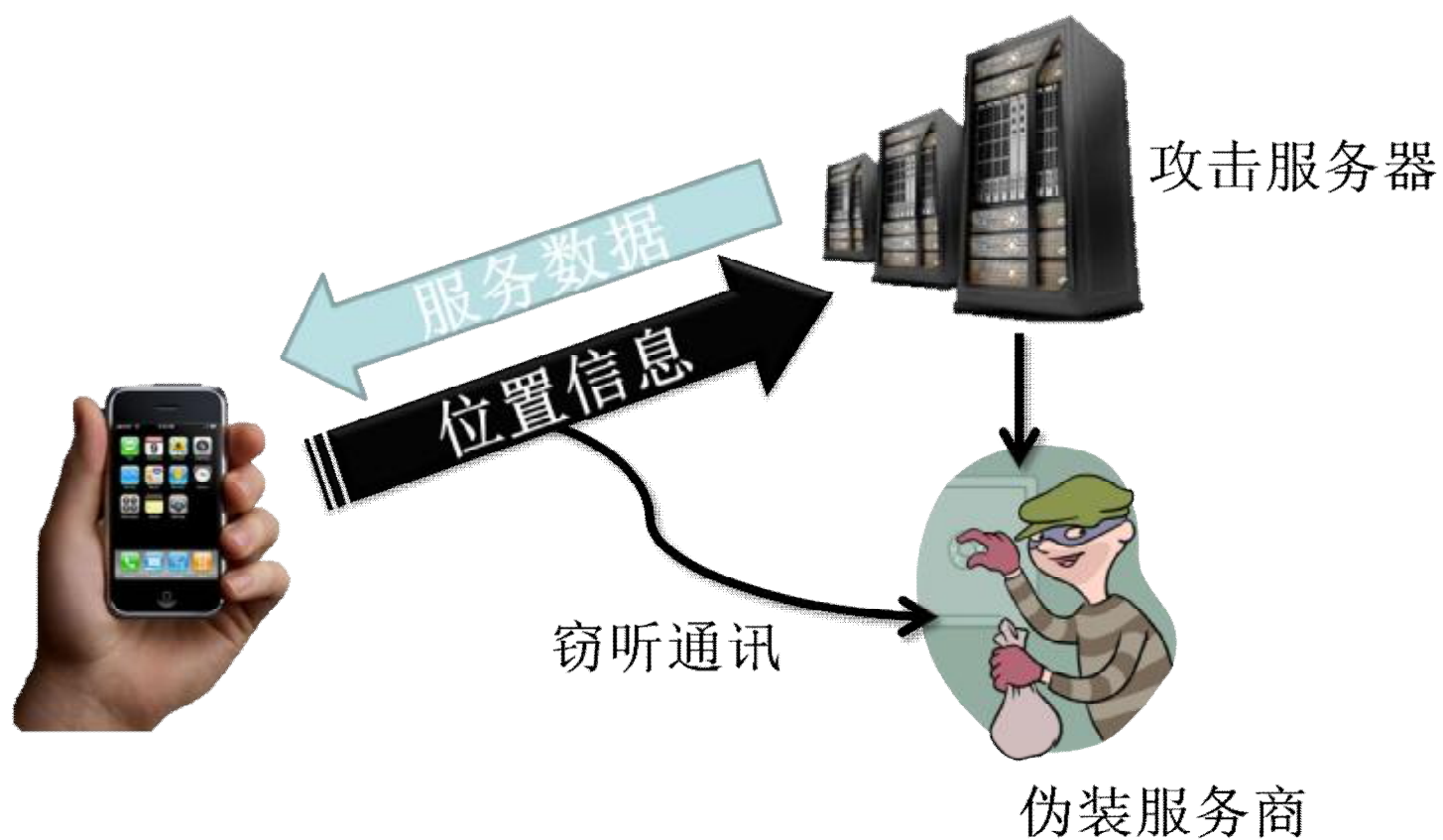
- 三要素：时间、地点、人物
- 人身安全
- 隐私泄露 学生上课、员工跳槽、专科医院、

位置隐私面临的威胁

- 通信 窃听
- 服务商 保护不力
- 攻击者 故意



14.4 位置信息与个人隐私



本章内容

14.1 概述

14.2 RFID安全和隐私

14.3 RFID安全和隐私保护机制

14.4 位置信息与个人隐私

14.5 **保护位置隐私的手段**

保护位置隐私的手段有哪些？

制度约束、隐私方针、身份匿名、数据混淆

14.5 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
 - ü 一切隐私保护的基础
 - ü 有强制力确保实施
- 缺点
 - ü 各国隐私法规不同，为服务跨区域运营造成不便
 - ü 一刀切，难以针对不同人不同的隐私需求进行定制
 - ü 只能在隐私被侵害后发挥作用
 - ü 立法耗时甚久，难以赶上最新的技术进展

14.5 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

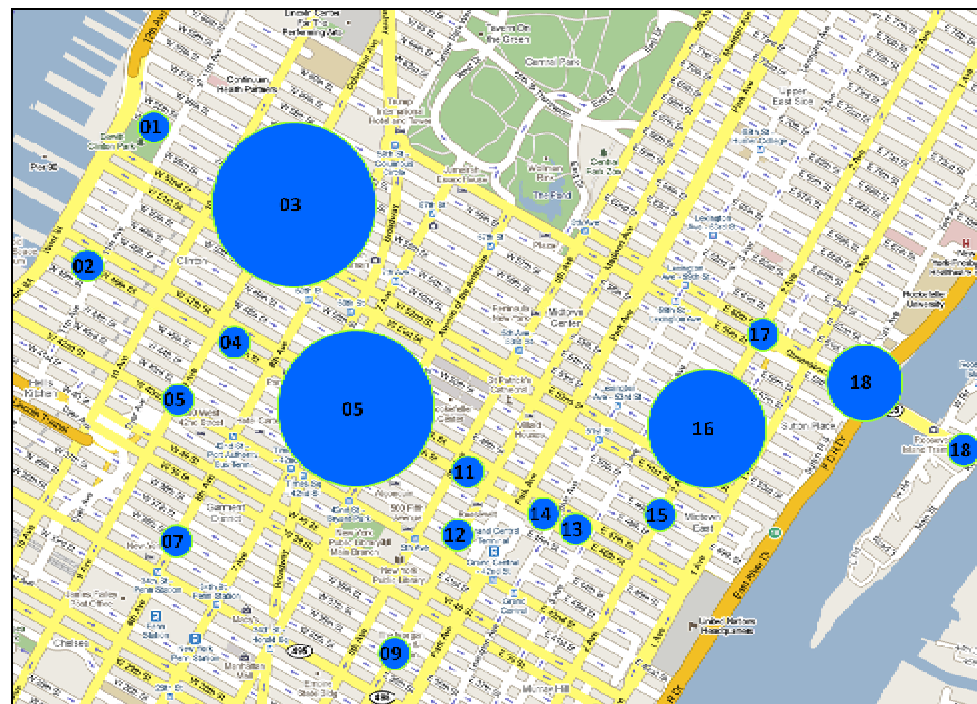
斯诺登--棱镜门事件

- 爱德华·约瑟夫·斯诺登，前美国中央情报局（CIA）雇员，亦担任美国国家安全局（NSA）的美籍技术承包人。
- 2013年，斯诺登向媒体提供机密文件致使包括“棱镜”项目在内美国政府多个秘密情报监视项目“曝光”。斯诺登泄露的文档显示，这一监控项目代号为PRISM，为止尚未对公众披露。通过该项目，美政府直接从包括微软、谷歌、雅虎、Facebook、PalTalk、AOL、Skype、YouTube以及苹果在内的这9个公司服务器收集信息。

14.5 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



14.5 保护位置隐私的手段

身份匿名（续）

- 优点

- ü 不需要强制力保障实施
- ü 对任何服务商均可使用
- ü 在隐私被侵害前保护用户隐私

- 缺点

- ü 牺牲服务质量
- ü 通常需要借助“中间层”保障隐私
- ü 无法应用于需要身份信息的服务

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

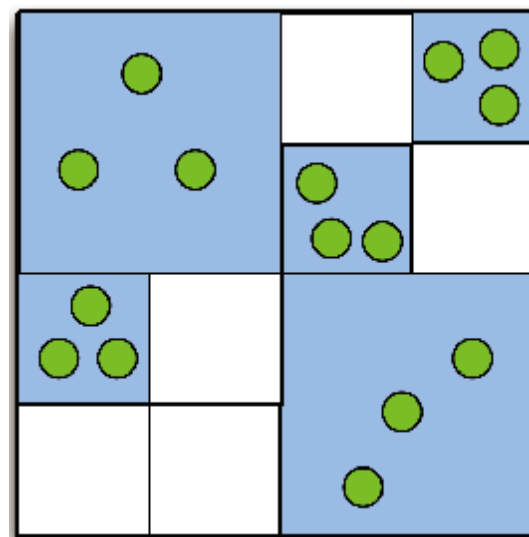
- ü空间上：扩大位置信息的覆盖范围

- ü时间上：延迟位置信息的发布

- 例：3-匿名

- ü绿点：用户精确位置

- ü蓝色方块：向服务商汇报的位置信息



14.5 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

- 三种方法

- ü 模糊范围：精确位置->区域

- ü 声东击西：偏离精确位置

- ü 含糊其辞：引入语义词汇，例如“附近”

- 优点

- ü 服务质量损失相对较小

- ü 不需中间层，可定制性好

- ü 支持需要身份信息的服务

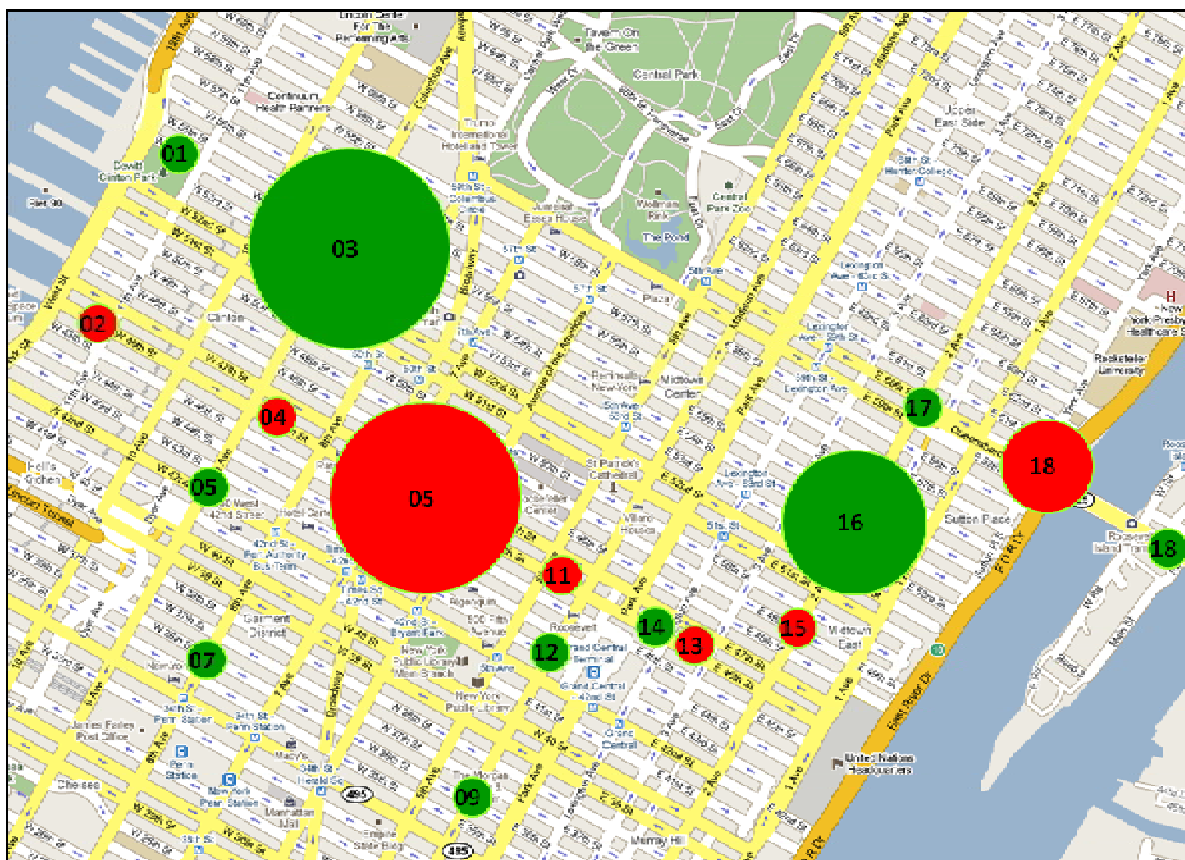
- 缺点

- ü 运行效率低

- ü 支持的服务有限

位置不可分辨与身份不可分辨

数据混淆：模糊范围



本章小结

内容回顾

本章介绍了RFID安全和典型的安全机制，以及位置隐私隐患和相应的保护手段。

重点掌握

- 了解网络信息安全的一般性指标。
- 掌握主要的RFID安全隐患。
- 了解RFID安全保护机制，重点掌握基于密码学的安全机制。
- 理解位置信息的定义，举例说明保护位置信息的手段。