物联网信息安全

欧阳元新

2020年10月26日

信息安全的重要性

重要事件

- 2009年6月24日

美国总统奥巴马批准成立美国的网络战司令部。

- 陆地，海洋，天空，网络

信息安全

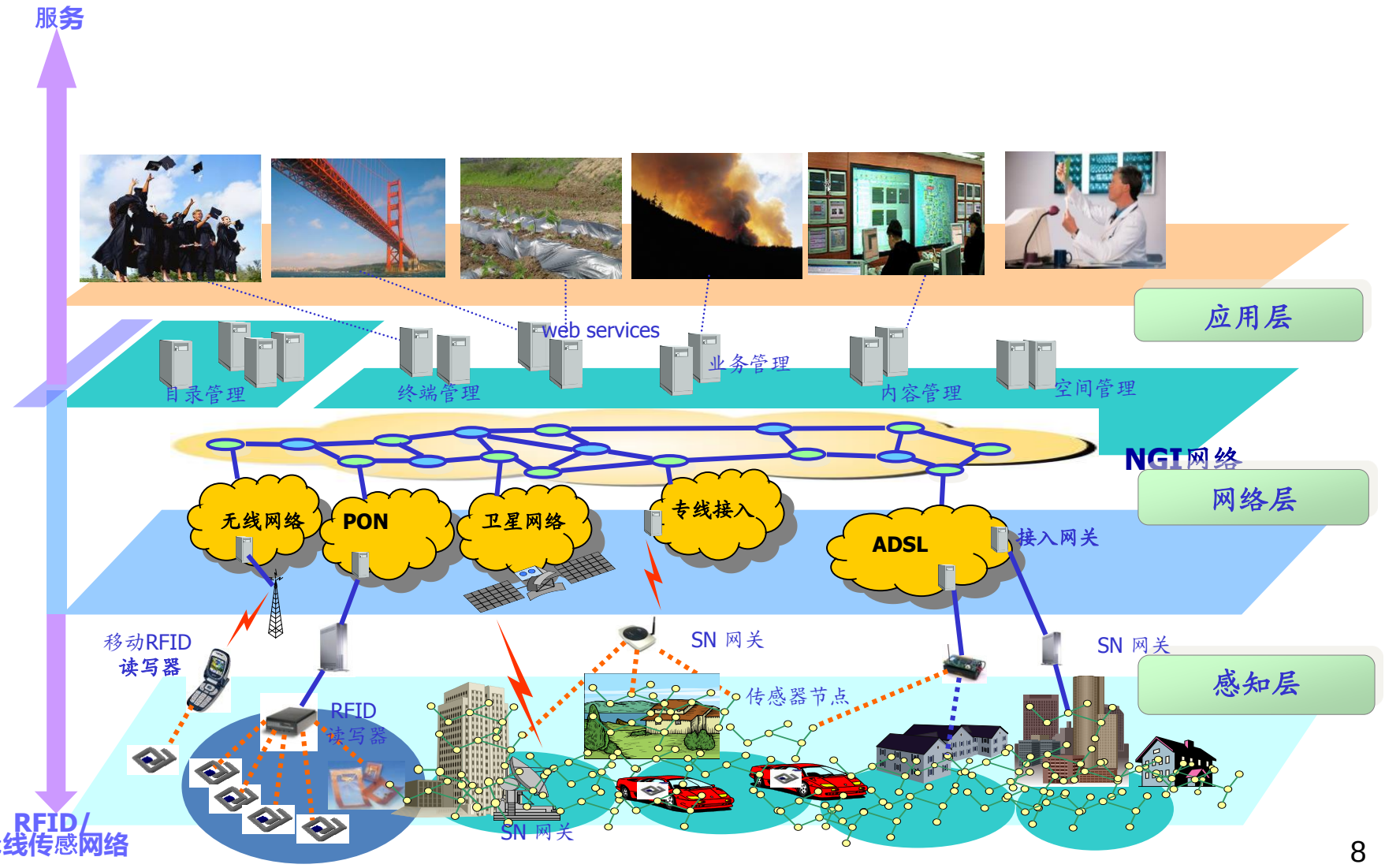
- 广义上，凡是涉及到信息的安全性，完整性，可用性，真实性和可控性的相关理论和技术都是信息安全所要研究的领域。

- 狭义的信息安全是指信息内容的安全性，即保护信息的秘密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗、盗用等有损合法用户利益的行为，保护合法用户的利益和隐私。

信息安全通常被划分为四个层次

- 物理安全：信息系统硬件方面，表现在信息系统电磁特性方面的安全问题
- 运行安全：信息系统软件方面，表现在信息系统代码执行过程中的安全问题
- 数据安全：信息自身的安全问题
- 内容安全：即信息利用方面的安全问题

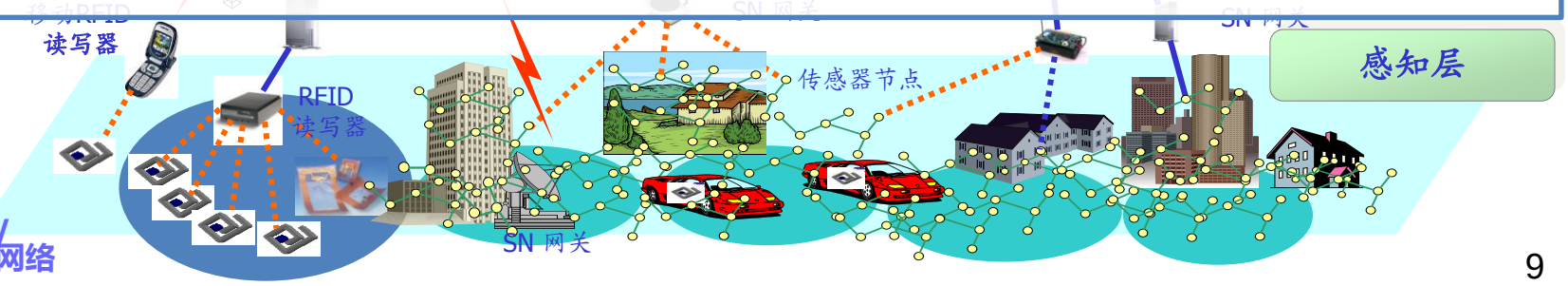
物联网体系框架


服务
应用层
web services
目录管理
终端管理
业务管理
内容管理
空间管理
NGI网络
网络层
无线网络
PON
卫星网络
专线接入
ADSL
接入网关
移动RFID
读写器
RFID
读写器
SN 网关
SN 网关
SN 网关
传感器节点
感知层
RFID/
无线传感网络

物联网体系框架

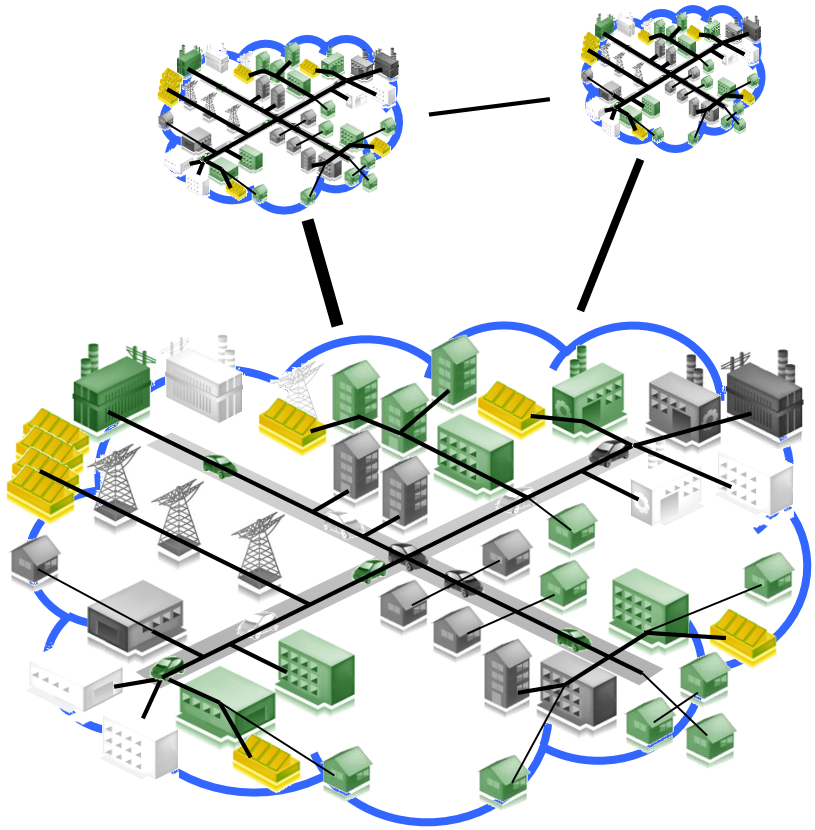
感知层：数据采集与感知

- 主要用于采集物理世界中发生的物理事件和数据，包括各类物理量、标识、音频、视频数据。物联网的数据采集涉及传感器、RFID、多媒体信息采集、二维码和实时定位等技术。
- 传感器网络组网和协同信息处理技术实现传感器、RFID等数据采集技术所获取数据的短距离传输、自组织组网以及多个传感器对数据的协同信息处理过程。



构建物联网的要素:传感器与传动器设备

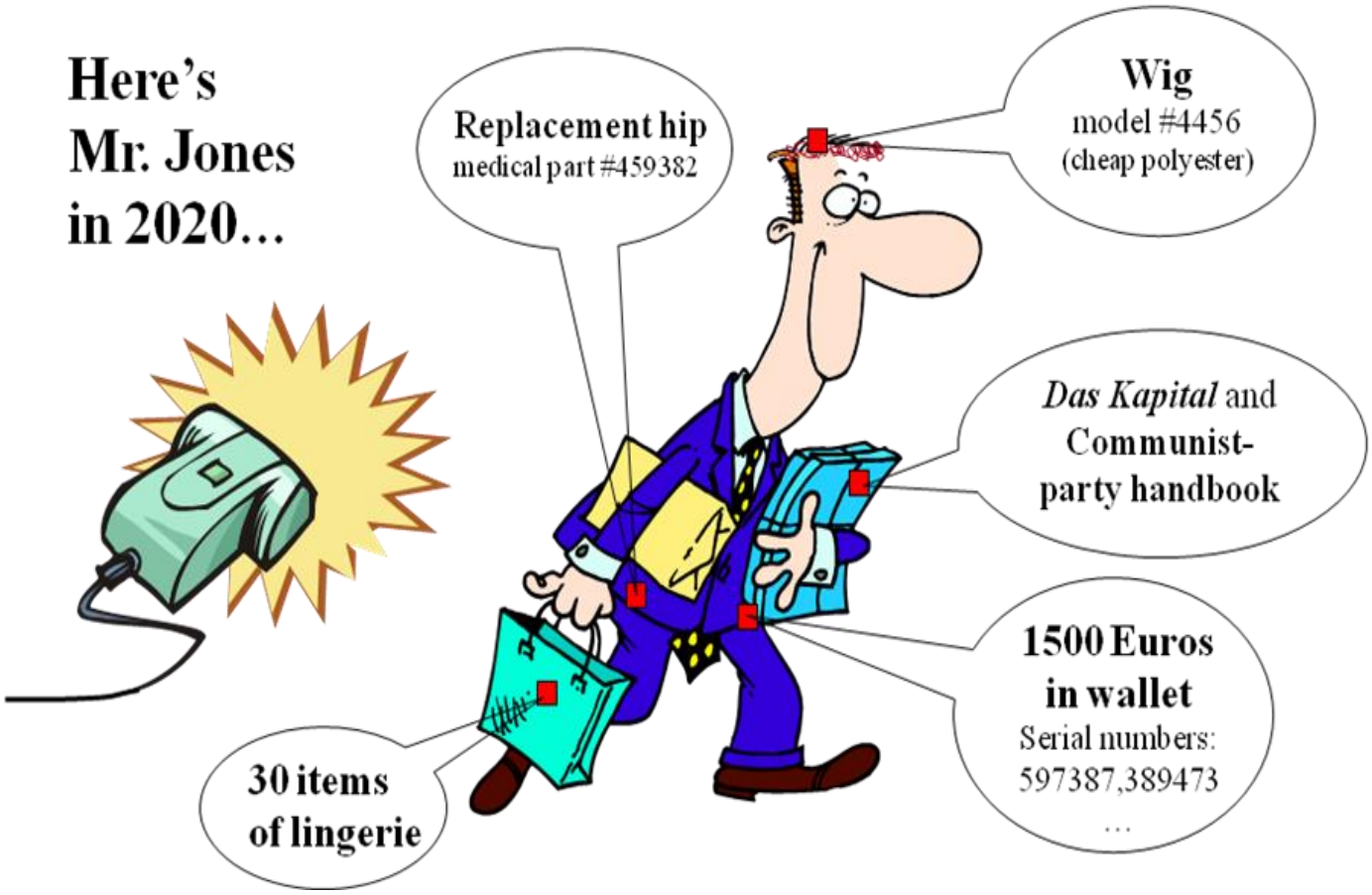
- 物联网基础设施的组件应配备传感器、传动器、标签、读取设备
  - 公共设施
  - 建筑物
  - 固定的运输设施
  - 移动的设施
- 将其全部链接到通用IP设施上
  - 通过已存在于建筑物中的接入设施、手机等



感知层面临的安全问题

	特点	面临的安全风险
RFID	1. 非接触操作，长距离识别，具有穿透性和无屏障阅读功能、无需可见光源； 2. Tag处理能力较弱，应用逻辑较为简单。	1. 隐私泄露：位置被非法跟踪；信息被非法收集 2. 身份认证
传感器节点	1. 部署于无人值守场合； 2. 节点资源严格受限，难以采用复杂的安全机制； 3. 节点处理能力较弱，应用逻辑较为简单。	1. 丢失，连接可能时断时续，物理捕获，窃取节点内部信息； 2. 计算能力有限，节点冒充，发送虚假数据； 3. 传统的安全机制无法应用。
移动终端	1. 处理能力较强； 2. 移动性强，可随时接入网络。	1. 易受病毒入侵，泄露个人隐私数据，也可对网络或其他用户发起攻击。

RFID隐私保护


Here's
Mr. Jones
in 2020...
Replacement hip
medical part #459382
Wig
model #4456
(cheap polyester)
Das Kapital and
Communist-
party handbook
1500 Euros
in wallet
Serial numbers:
597387,389473
...
30 items
of lingerie

主要的安全隐私威胁

- 非法读取
- 位置跟踪
- 窃听
- 拒绝服务
- 伪装哄骗
- 重放

前提与要求

- 阅读器与后台数据库的通信可以在更为安全可靠的有连接信道上进行，与之相比，阅读器与标签之间的无线通信信息易被窃听
- 要普及RFID技术，必须保证RFID标签的低成本实现
- 安全的RFID系统应能抵御各种攻击，且考虑到较坏的情况，即使敌人获得了标签内部的秘密数据，也应保证其无法追踪到跟标签有关的历史活动信息（如：数据库启用安全访问控制）

智能卡操作系统的防护

- 控制数据传送过程，防止非授权访问
- 重要存储内容应用校验和保护
- 应用密钥
- 面向对象的访问条件

RFID隐私保护典型方法

- Kill标签
- 主动干扰
- 访问控制
  - Hash锁
  - 随机Hash锁

Kill 标签

- 商品交付给最终用户时，通过KILL指令杀死标签
- 改进方法：
  - 让标签的唯一逻辑Tag ID由一个Class ID和一个唯一Local ID组成
  - 在收银台处使用一个用户自定义的值替换Class ID，通过消除标签的唯一性来保护用户的隐私
  - 当用户将产品返回维修时，又恢复原来的产品Class ID，使用户能够继续享受特殊的服务

主动干扰—— Blocker tag

- 成本很低，只需一个安装了两个天线的标签，其工作原理是根据防冲突检测的Tree-walking算法
- 设标签的序列号长度为k位，Blocker tag冒充所有可能的2k个标签全集，每次当阅读器询问Tree中给定结点A子树的下一比特位时，Blocker Tag同时发送一个0比特和一个1比特回答询问（故需要两个天线）

访问控制

- Hash锁
- 随机Hash锁
- 基于低成本的单向Hash函数实现

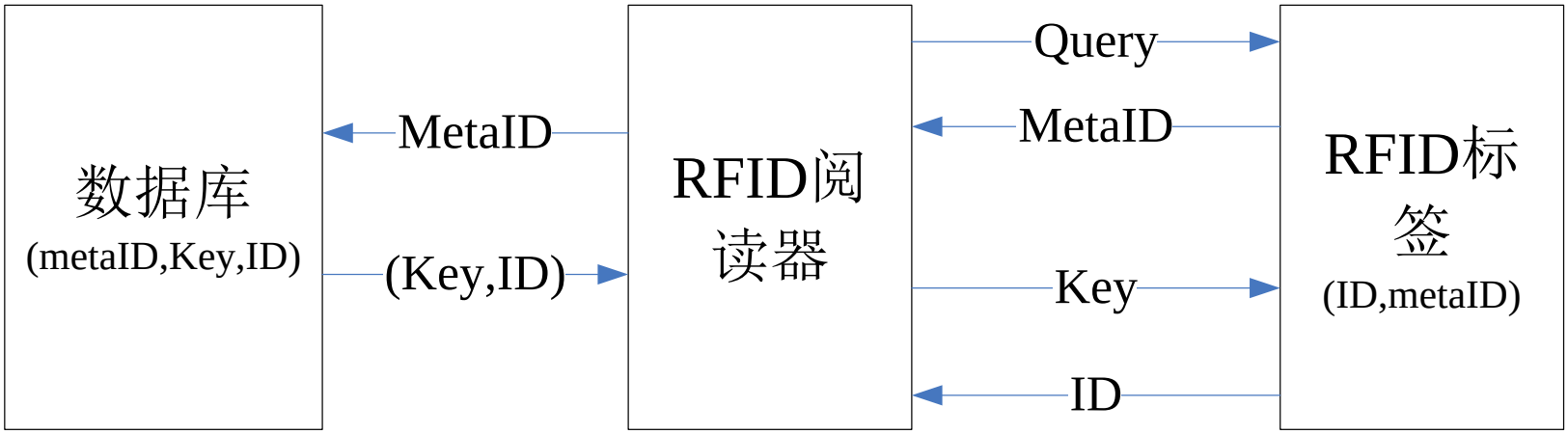
Hash函数

- 输入一个长度不固定的字符串，返回一串定长度的字符串，又称HASH值
- 单向HASH函数用于产生信息摘要
- 主要可以解决，在某一特定的时间内
  - 无法查找经HASH操作后生成特定HASH值的原报文
  - 无法查找两个经HASH操作后生成相同HASH值的不同报文。

Hash锁锁定标签过程

令 metaID = Hash(Key)

Hash锁解锁标签过程



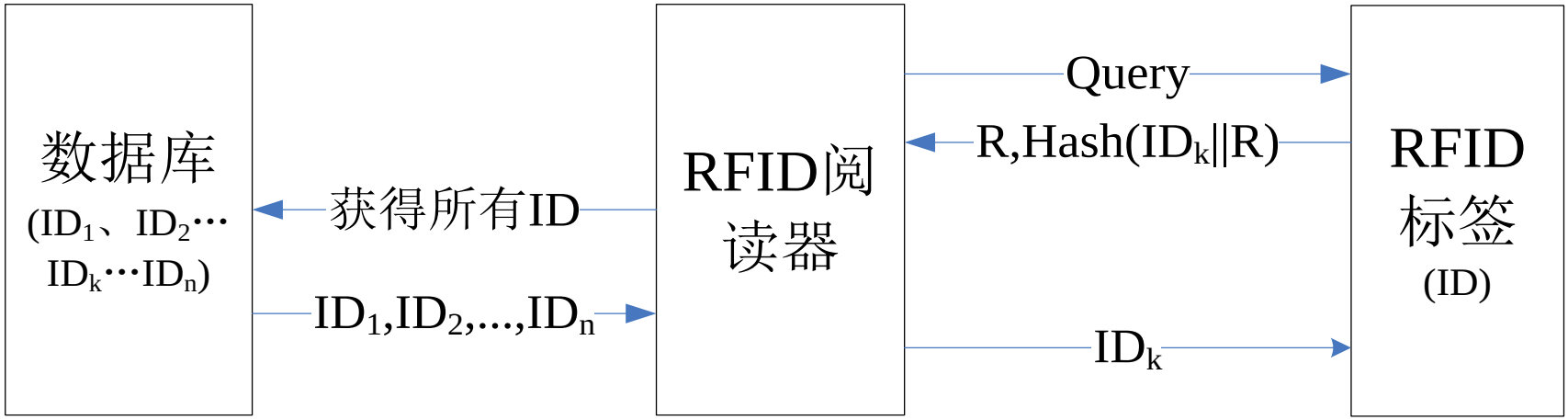
Hash锁优缺点

- 优点：
  - 解密单向Hash函数是较困难的，因此该方法可以阻止未授权的阅读器读取标签信息数据，在一定程度上为标签提供隐私保护；
  - 该方法只需在标签上实现一个Hash函数的计算，以及增加存储metaID值，因此在低成本的标签上容易实现；
  - 设在后台数据库中存储的标签总数为N，执行总时延是1个Hash函数的计算时间加上N个(metaID, Key, ID)记录的线性搜索时间，因此效率较高，延时较短。

Hash锁优缺点

- 缺点：
  - 非授权阅读器先对标签进行询问，获得metaID，然后在合法阅读器前伪装成该标签，从而获得Key值，继而非授权阅读器利用获得的Key值询问标签从而得到标签的ID信息，造成重放攻击；
  - 由于每次询问时标签回答的数据是特定的，因此其不能防止位置跟踪攻击；

随机Hash锁解锁标签过程



随机Hash锁优缺点

- 优点：标签每次回答是随机的，因此可以防止依据特定输出而进行的位置跟踪攻击
- 缺点：阅读器需要搜索所有标签ID，并为每一个标签计算Hash(IDk||R)，因此标签数目很多时，系统延时会很长，效率并不高，其适用于标签数目比较少的情况

感知层面临的安全问题

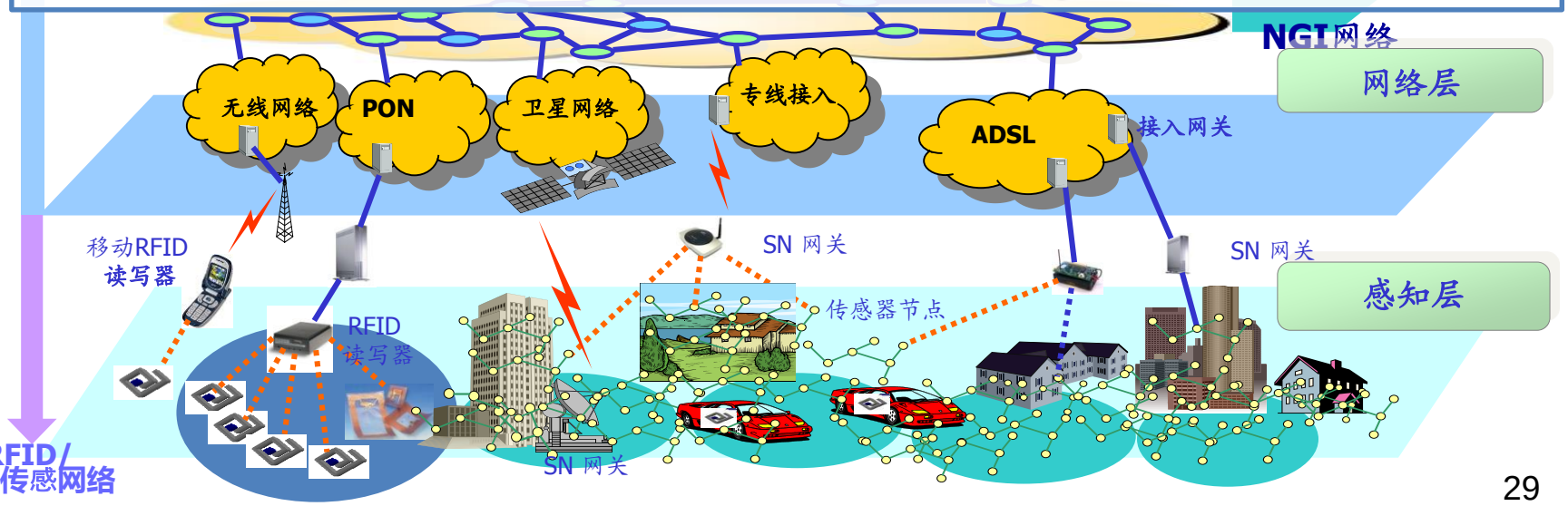
	特点	面临的安全风险
RFID	1. 非接触操作，长距离识别，具有穿透性和无屏障阅读功能、无需可见光源； 2. Tag处理能力较弱，应用逻辑较为简单。	1. 隐私泄露：位置被非法跟踪；信息被非法收集 2. 身份认证
传感器节点	1. 部署于无人值守场合； 2. 节点资源严格受限，难以采用复杂的安全机制； 3. 节点处理能力较弱，应用逻辑较为简单。	1. 丢失，连接可能时断时续，物理捕获，窃取节点内部信息； 2. 计算能力有限，节点冒充，发送虚假数据； 3. 传统的安全机制无法应用。
移动终端	1. 处理能力较强； 2. 移动性强，可随时接入网络。	1. 易受病毒入侵，泄露个人隐私数据，也可对网络或其他用户发起攻击。

物联网体系框架

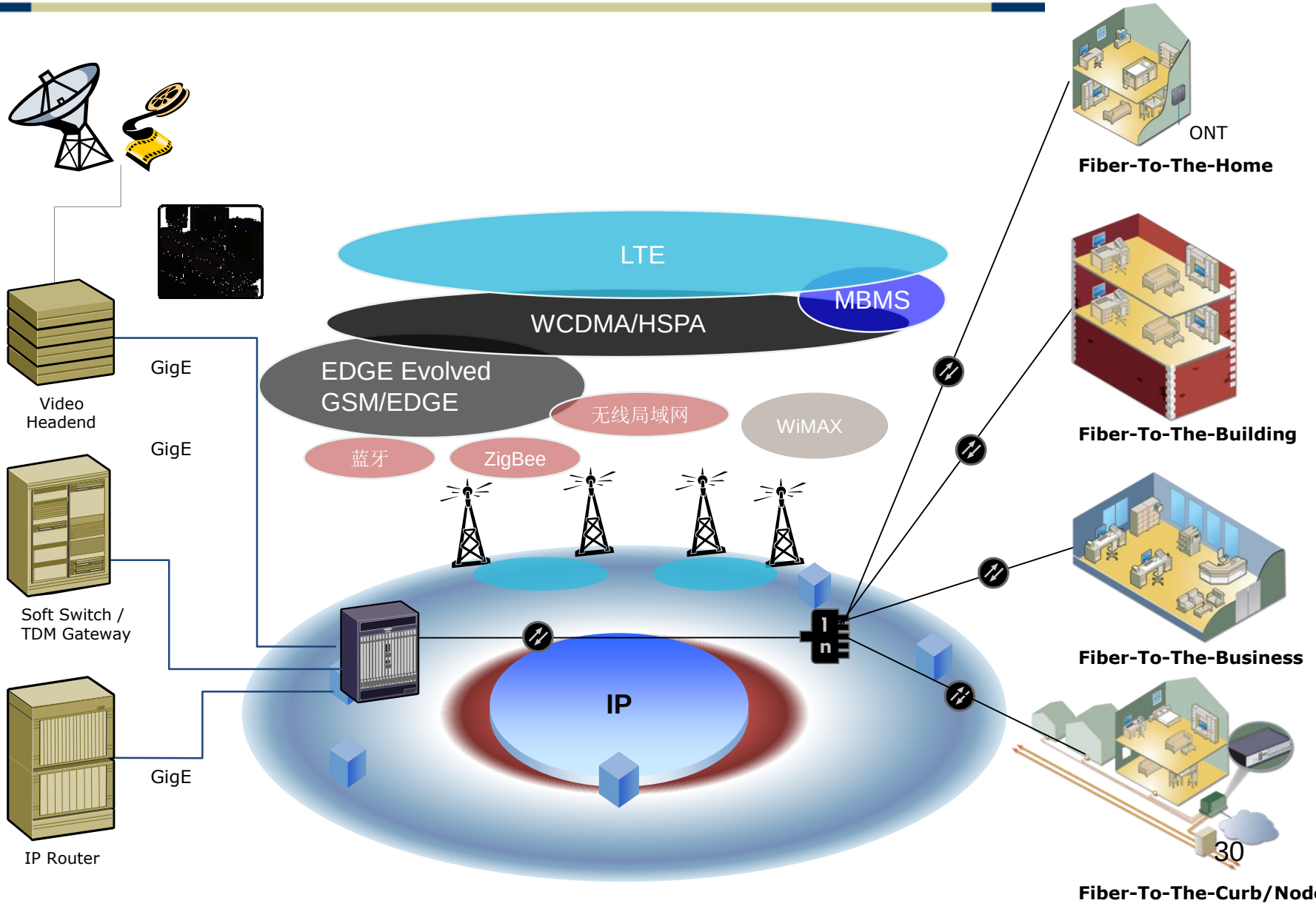
服务

网络层：实现更加广泛的互联功能

- 能够把感知到的信息无障碍、高可靠性、高安全性地进行传送，需要传感器网络与移动通信技术、互联网技术相融合。



构建物联网的要素:高速互联的基础设施



网络层面临的安全问题

物联网的网络层实际涵盖现有的各种网络形式，包括移动通信网、互联网、卫星网络、集群通信网等等。这些网络原有的安全问题都会被引入到物联网中。并且由于物联网的特殊性，原有的网络安全问题可能会被放大。

特殊性	安全威胁	描述
大量的设备接入网络带来的安全问题	网络拥塞	物联网的设备数量巨大，短时间内大量接入网络，很可能会带来网络拥塞，而网络拥塞会给攻击者带来可趁之机。
	认证和密钥生成机制受到挑战	当大量物联网设备接入网络时，如果按照原有的逐一认证产生密钥的方式，会给网络带来大量的资源消耗。
感知网络和通信网络分离产生的安全问题	“中间人攻击”	通过窃取、篡改、伪造信息，威胁、干扰感知网络和通信网络之间的正常通信。

物联网体系框架

服务






应用层

应用层：包含应用支撑平台和应用服务

- 应用支撑平台子层用于支撑跨行业、跨应用、跨系统之间的信息协同、共享、互通的功能。
- 应用服务子层包括智能交通、智能医疗、智能家居、智能物流、智能电力等行业应用。

网络层

感知层

RFID/
无线传感网络

应用层面临的安全问题

物联网的应用层包括共性业务支撑平台和构建在其上的各个行业和领域的应用服务。应用层主要面临以下安全威胁：

隐私威胁 → 业务滥用 → 身份冒充 → 信息窃听/篡改/伪造 → 抵赖和否认 → 信令拥塞

- 隐私威胁包括用户，个人兴趣爱好、信息。
- 恶意

隐私侵犯者可以通过标签的位置信息获取标签用户的行踪。

有可能出现用户使用未授权或者合法用未定制的情况的发生。

无人值守设备被劫持，然后伪装成客户或应用服务器，据信息、执

网络的异构不同网络的制相互独立应用层数据很可能被窃听、注入、篡改和伪造。

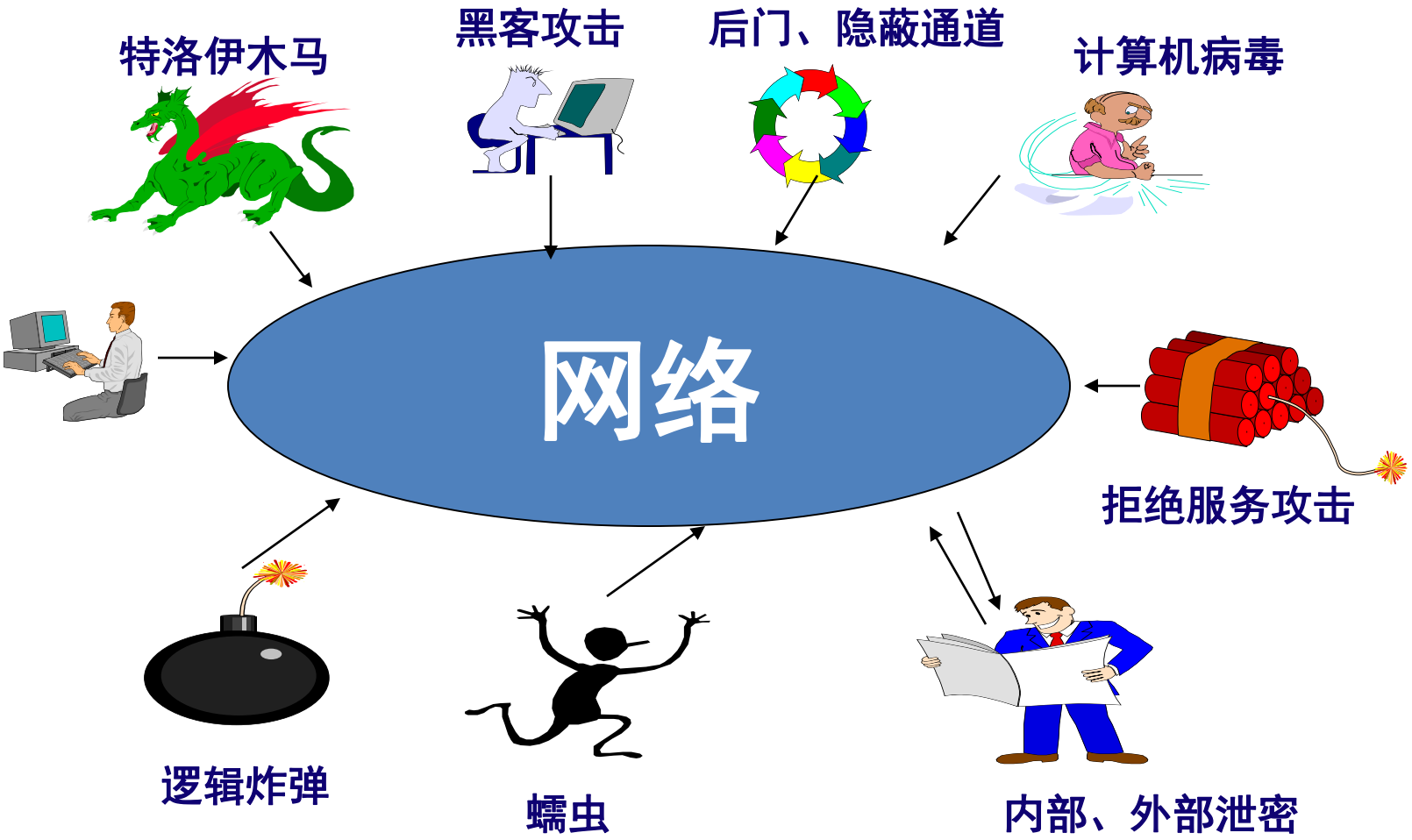
业务能否认完成的

短时间内大量终端向应用服务器发送接入请求，有可能导致应用服务器过载，使得网络中信令通道拥塞。

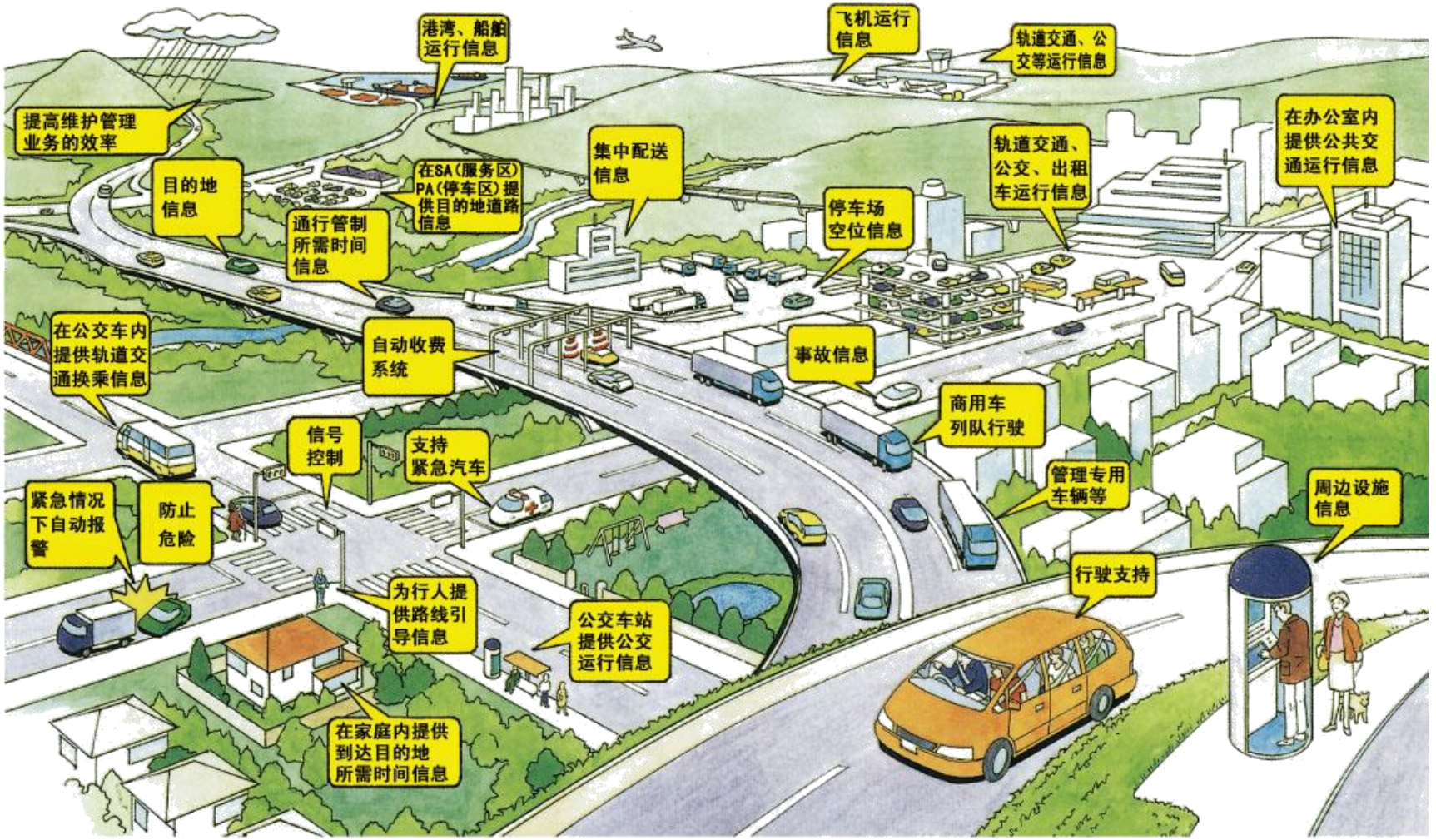
物联网的安全问题：三个要素

- 物联网的安全问题
  - 信息系统的安全：安全、可靠的基础设施
- 物联网的隐私保护问题
  - 信息自身的安全：安全、可信的信息内容
- 物联网的可信问题
  - 信息应用的安全：安全、可控的控制应用

传统安全仍然长期存在



交通物联网中的安全问题



公交卡欺诈、充值

射频卡欺诈、克隆

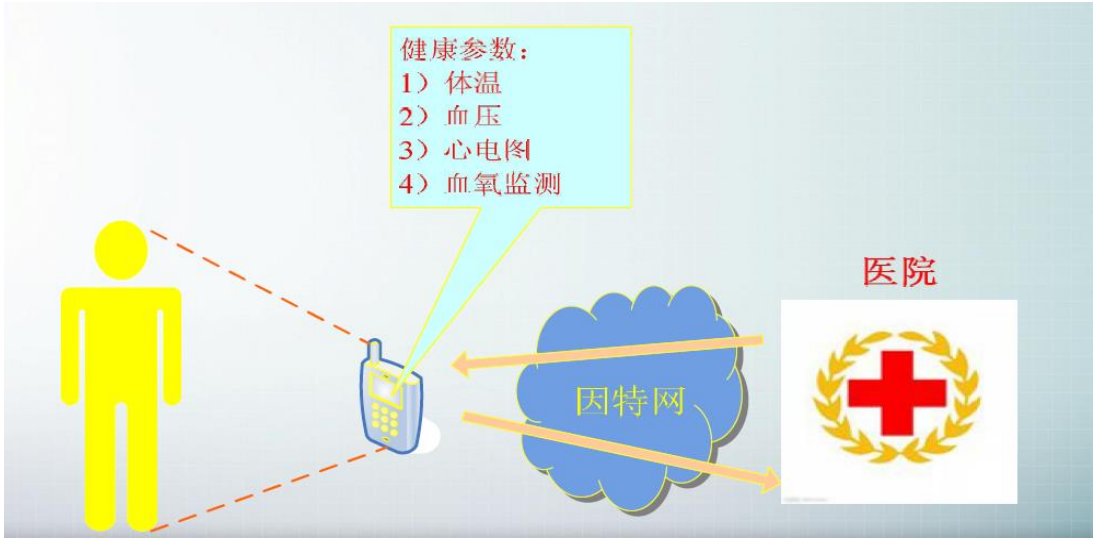
车牌证照欺诈、伪装

美国尝试远程对工业基础设施发动物理上的摧毁性攻击，导致发电机、变电器过载烧毁

- 美国总审计署2011年报告列出了国家电网现代化面临的六大安全挑战。
  - **缺乏了解：**只有很少的用户愿意为安全和可靠的系统买单，从而所致电力不愿意提高与网络安全有关的花费。直到用户充分了解了智能电网系统在成本、风险等的好处，电力公司才会为智能电网的安全防护投资。在这之前，不法分子攻击取得成功的机率将会增大。
  - **缺乏关注：**目前的大环境中，电力行业将重点放在了遵守相关安全规定，而不是获得有效的安全防护。专家称，这些电力公司重点是遵守最低的安全标准，而不是采取有效措施确保系统安全。
  - **缺乏安全特性：**目前智能电网系统中缺乏安全特性。安全特性没有内置在智能电网设备中。比如，有专家称，目前一些智能电表在设计时就没有采用安全架构，缺乏重要的安全特性，如探测和分析攻击的辨别能力。
  - **缺乏信息共享：**对于网络攻击和其它问题，电力公司之间并没有一个有效的信息共享机制。电力行业缺乏一个可以有效公布关于智能电网弱点、事故、威胁、教训、经验做法的机制。
  - **缺乏评估机制：**电力行业没有网络安全评估指数。电力行业还遭遇到了没有网络安全评估指数的问题，这导致行业很难估算应当对网络安全进行什么样的投资。
  - **管理问题：**目前的监管难以确保智能电网系统的安全。目前联邦政府和州政府对智能电网的监管权限和职责都没有明确的划分，特别是在网络安全方面。

医疗物联网中的安全问题

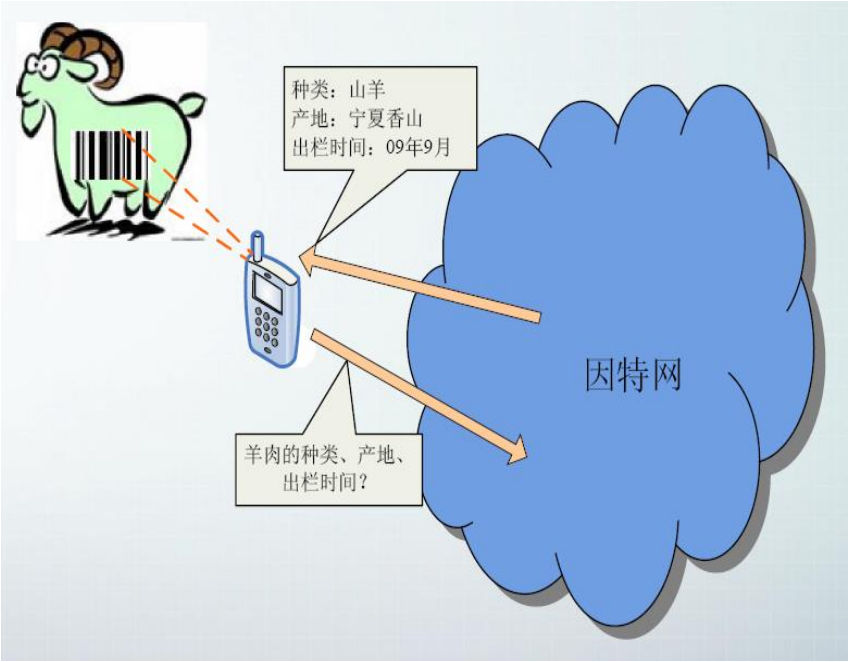
- 人身上可以安装不同的传感器，对人的健康参数进行监控，并且实时传送到相关的医疗保健中心，如果有异常，保健中心通过手机，提醒您去医院检查身体。
- 智慧医疗是一个以医疗物联网为核心、信息高度移动、信息高度共享的医疗信息化生态系统。
- 通过自动追踪和记录患者、医疗设备和资产的状态，帮助医生定位患者，并确定医疗活动的优先级。



- 隐私信息泄露
- 信息篡改引发的 医疗事故
- 血型、药物过敏等库存信息修改等
- 监测信息篡改

食品安全物联网中的安全问题

- 给放养的牲畜中的每一只动物都贴上一个二维码，这个二维码会一直保持到超市出售的肉品上，消费者可通过手机阅读二维码，知道牲畜的成长历史，确保食品安全。

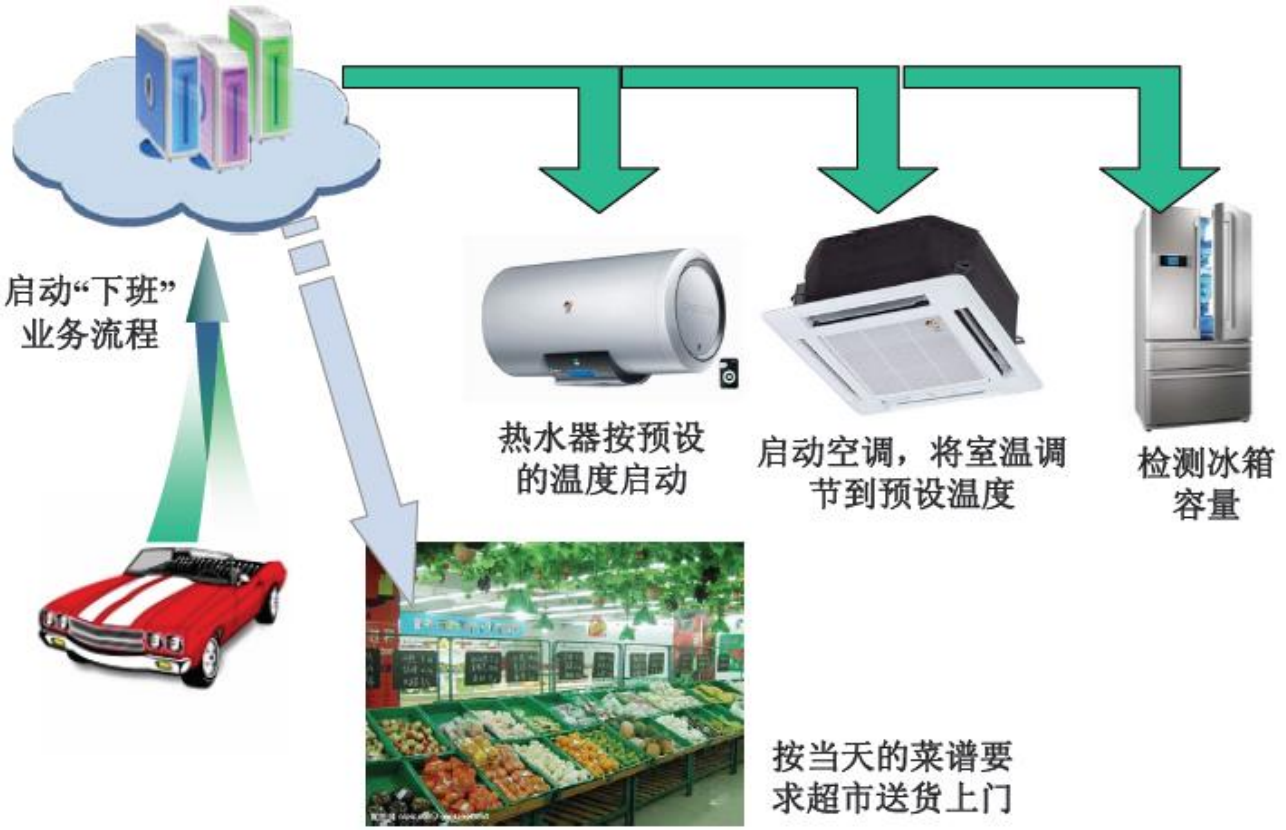


- 中间是否有人更换信息？
  - 来源的真实性如何保证？
  - 身份的真实性如何保证？
  - 信息造价是否更具有欺骗性（如同真瓶假酒）

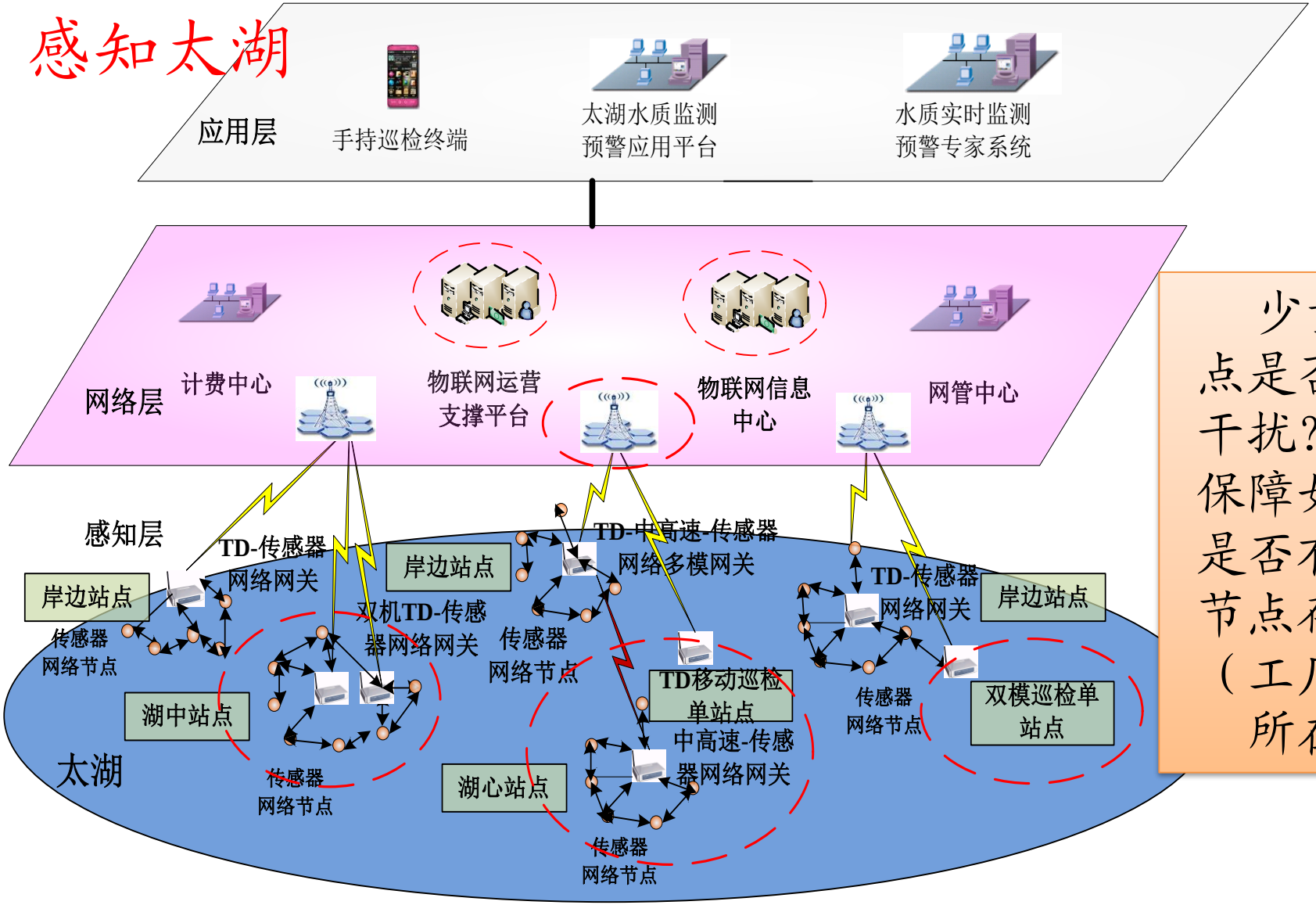
家庭物联网中的安全问题

家庭控制信息的危害性如何？非授权控制将会如何？

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。



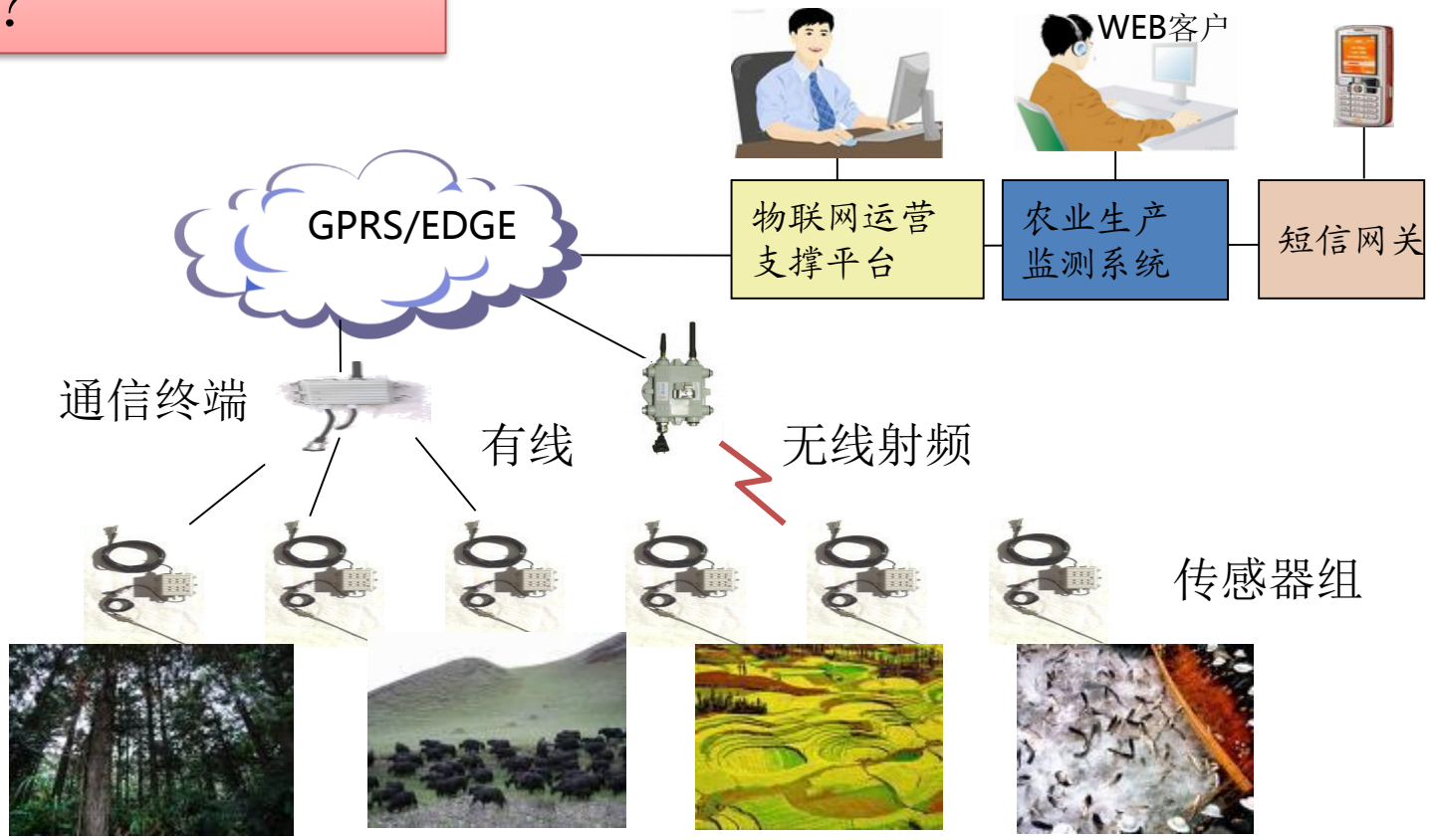
水利物联网中的安全问题



少量的节点是否会被干扰？能源保障如何？是否有欺骗节点存在？（工厂利益所在）

农业物联网中的安全问题

新疆短信灌溉控制，控制源头的真实性如何保证？



谢 谢!