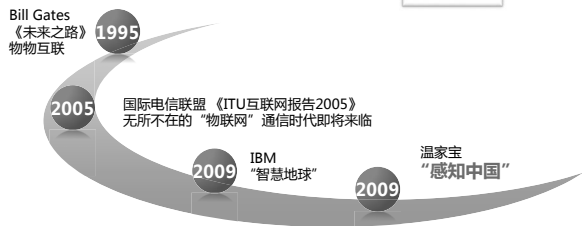


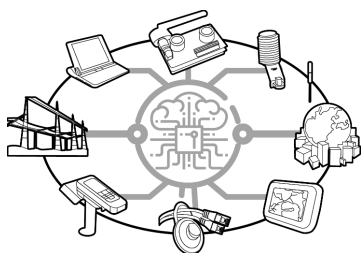
起源与发展

物联网的基本思想出现于20世纪90年代



3

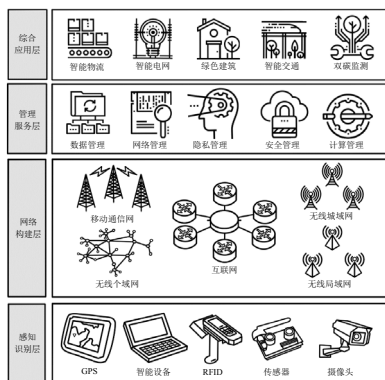
物物互联



物物互联：沟通物理世界与信息世界

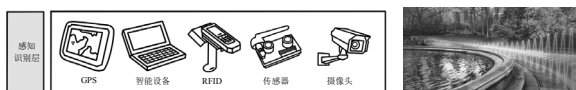
5

物联网四层模型



8

核心技术：感知识别层



感知识别是物联网的核心技术，其作用是从物理世界获取信息，直接连接物理世界和信息世界。

物联网的“触手”是位于感知识别层的大量信息生成设备，既包括RFID、无线传感器等信息自动生成设备，也包括各种辅助人工生成信息的智能电子产品，例如智能手机、平板电脑、笔记本电脑等。

感知识别层中多样化的信息生成方式是物联网区别于其他网络的重要特征。

感知识别层位于物联网四层模型的最底端，是所有上层结构的基础。

10

Q：什么是物联网？

概念的提出

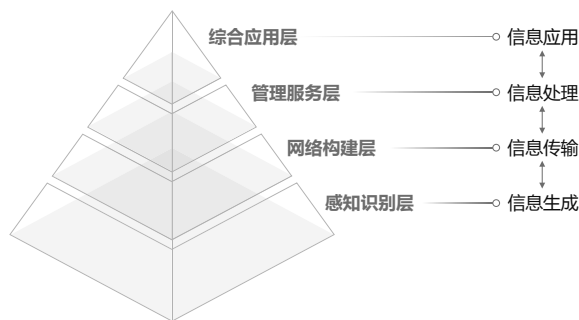
In computing, the Internet of Things refers to a network of objects, such as household appliances. It is often a self-configuring wireless network. The concept of the internet of things is attributed to the original Auto-ID Center, founded in 1999 and based at the time in MIT.



物联网这个概念实际是中国人提出的，整合了美国CPS(Cyber-Physical Systems)、欧盟IoT (Internet of Things)和日本i-Japan等概念。是一个基于互联网、传统电信网等信息载体，让所有能被独立寻址的普通物理对象实现互联互通的网络。普通对象设备化，自治终端互联化和普适服务智能化是其三个重要特征。

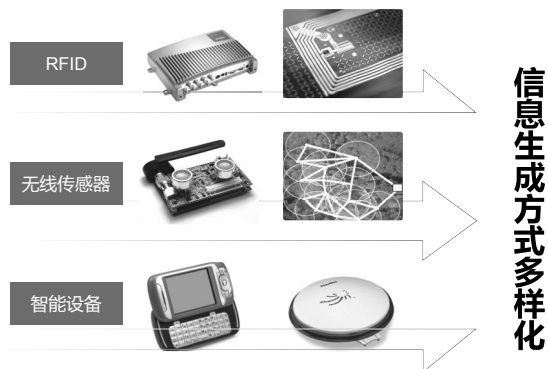
4

核心技术



7

核心技术 - 感知识别层



9

感知识别层技术举例：RFID



基本组成

工业界经常将RFID系统分为标签，阅读器和天线三大组件。

工作原理

阅读器通过天线发出电磁波；然后标签接收到信号后通过反射电磁波发送信息；阅读器再通过天线接收并识别标签发回的信息；最后，阅读器将识别结果发送给主机。

详见 第2章

11

感知识别层技术举例：定位系统

位置信息内涵扩展

空间信息→所在地理位置+处在该地理位置的时间+处在该地理位置的对象（人或设备）

定位系统与技术

室外定位系统：

- 卫星定位、蜂窝基站定位（GSM/CDMA/3G）

室内定位系统：

- RFID定位
- 声音信号定位
- 可见光信号定位

物联网环境下对定位技术的挑战

- 大范围场景下的精准定位
- 动态场景下维持定位鲁棒性
- 多目标同时定位

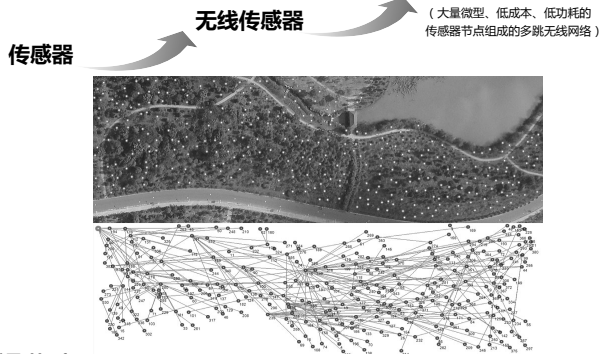


详见 第4章

12

感知识别层技术举例：无线传感网

发展历程



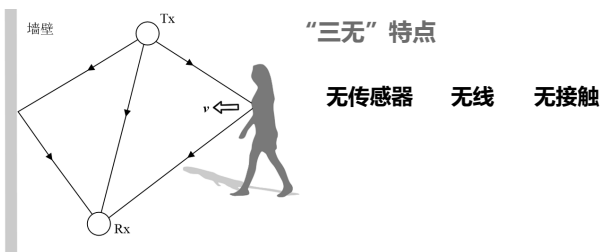
详见 第3章

13

感知识别层技术举例：非传感器感知

技术特征

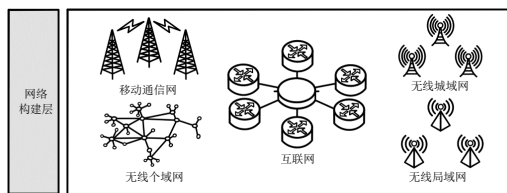
基于无线信号的感知技术称为非传感器感知技术。通过分析无线信号在传播过程中的变化，以实现对环境的感知。



详见 第3章

14

核心技术：网络构建层



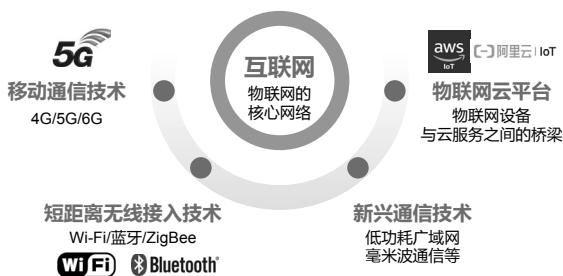
网络是物联网最重要的基础设施之一。

散落在世界各地的设备是如何被连接到同一个网络中的？移动互联网又是如何发展起来并深刻影响当代人生活模式的？

网络构建层在物联网4层模型中连接感知识别层和管理服务层，具有强大的纽带作用，高效、稳定、及时、安全地传输上下层的数据。

15

核心技术 - 网络构建层



详见 第5-6章

16

核心技术：管理服务层



管理服务层位于感知识别和网络构建层之上，综合应用层之下，是物联网智慧的源泉。在高性能计算和海量存储技术的支撑下，管理服务层将大规模数据高效、可靠地组织起来，为上层行业应用提供智能的支撑平台。

数据存储、大数据处理、云计算等为海量数据的存储与分析提供了强有力的支持与保障。

大量的私人数据被上传到网络上使信息安全和隐私保护变得越来越重要。

管理服务层解决数据如何存储、如何检索、如何使用、如何不被滥用等问题。

详见 第7-8章

17

管理服务层：物联网与安全

物联网设备连接以互联网为基础，物联网安全以互联网安全为基础，并建立在互联网安全之上。

相比互联网安全，物联网安全问题具有一些新的特征：

- 设备资源受限，更难抵抗攻击
- 会破坏硬件设备
- 更容易威胁到人身安全
- 部署规模大，数据隐私保护格外困难

物联网安全面临新的安全需求和挑战：

- 设备和用户身份验证
- 适用于大量设备通信场景的信任机制



详见 第7章

18

管理服务层：物联网与隐私

物联网终端的广泛引入在提供更丰富信息的同时，也增加了信息被暴露的风险。

物联网隐私问题现状：

- RFID标签不易支持密码学算法，容易泄露存储的隐私信息
- 手机和可穿戴设备的传感器数据泄露用户的行为、密码等
- 用户的历史位置信息泄露用户身份和参与的事件

物联网隐私安全防护方法：

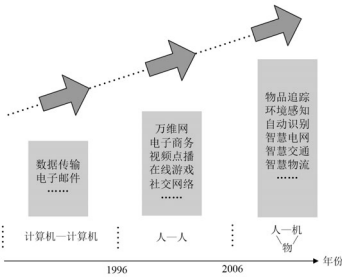
- 身份匿名
- 数据混淆



详见 第8章

19

核心技术 - 综合应用层

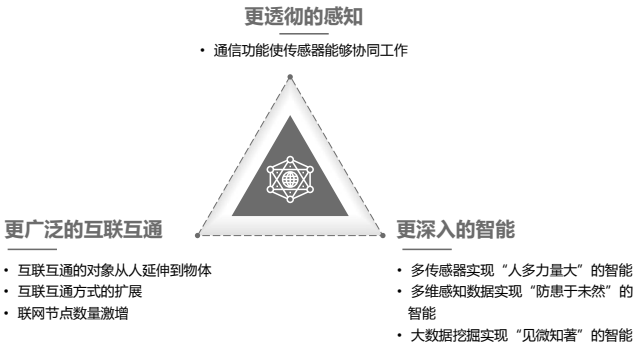


- 互联网从最初用来实现计算机之间的通信，进而发展到连接以人为主体的用户，现在正朝着万物互联这一目标前进。
- 网络应用数量激增，呈现多样化、规模化、行业化等特点。

详见 第9-12章

20

主要特点



22

发展趋势

非侵入、高精度和多模态感知更加成熟

- 利用环境中原本存在的无线信号实现非接触式、被动式的感知。
- 精确定位算法被写入协议，大幅提升定位精度。
- 处理多模态数据可以得到更高准确率、更有效和更易理解的上下文信息。

低功耗、长距离无线通信技术迅猛发展

- 低功耗广域网技术快速扩张，广泛应用在部署规模在千米级或更大尺度的物联网应用中。

24

发展趋势（续）

人工智能与物联网深度融合

- 人工智能技术在物联网应用中越来越普及，物联网产生的大量数据也给人工智能提供了新的应用方向。
- 人工智能运算大量在中断而非云端或边缘节点完成。

网络攻击向物理世界渗透

- 大量物联网设备部署在街道、工厂以及家庭等各个角落。网络攻击不仅仅破坏信息系统，更有可能造成物理世界的破坏。

25

内容回顾

前一章

介绍了物联网的基本概念，核心技术，主要特点和发展趋势。

把物联网分为

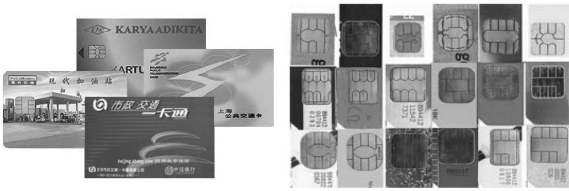
感知识别层、网络构建层、管理服务层和综合应用层四层。

2

智能卡

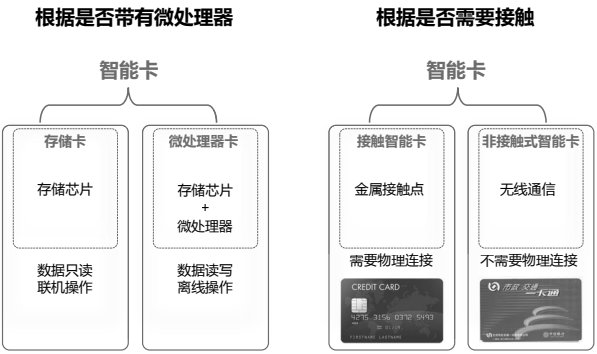
智能卡

又称集成电路卡（integrated circuit card，IC卡）或智慧卡（intelligent card），实际上是一种数据存储和处理系统。



4

智能卡分类



5

条形码技术：一维条形码

传统条形码（一维条形码）

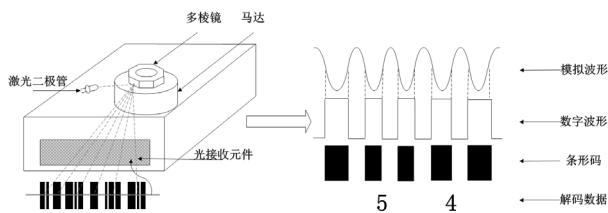
- 是将宽度不等的多个黑条和空白按照一定的编码规则排列，用以表达一组信息的图形标识符。常见的条形码是由反射率相差很大的黑条（“条”）和白条（“空”）排成的平行线图案。
- 一个完整的条码的组成次序依次为：静区（前）、起始符、数据符、（校验符）、终止符、静区（后）。



7

一维条形码：译码原理

条形码扫描器发出一束光线，经条形码反射后，反射光射入扫描器内部的光电转换器上，光电转换器将强弱不同的反射光信号转换为相应的电信号。



8

一维条形码：缺点

信息容量小

仅能容纳几位或者几十位信息量

- 标识一类商品类别
- 不包含对商品的描述
- 需要后台数据库辅助

无法表示汉字或者图像信息

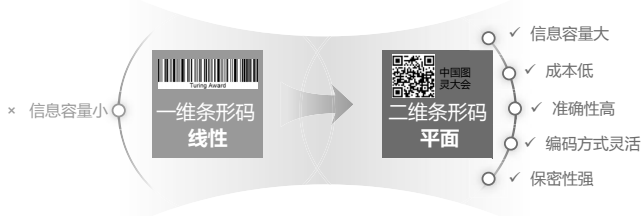
- 占用印刷面积大
- 不方便印刷和包装

9

条形码技术：二维条形码

二维码的工作原理

与一维条形码类似，需要扫描装置和译码装置来阅读条形码符号所包含的信息



10

二维条形码特点

二维条形码特点：

存储量大：可以存储更多的字符，而且能够存储英文、数字、汉字、记号等。

抗损性强：采用了故障纠正技术，遭受污染以及破损后也能复原，受损程度高达50%仍能解读出原数据。

安全性高：采用了加密技术。

显示多样性：支持黑白印刷和彩色印刷，印刷机器和印刷对象不受限制，可以显示在显示屏上。

抗干扰能力强：与磁卡、IC卡相比，具有强抗磁能力、抗静电能力。

识别方便性：普通智能手机利用摄像头就可以方便地读取



11

RFID技术

RFID，射频识别技术（Radio Frequency Identification），通过无线信号进行标识和识别。

是构建物联网的一项关键技术。



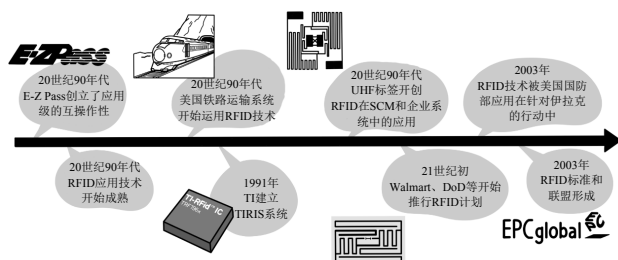
13

RFID发展历史



14

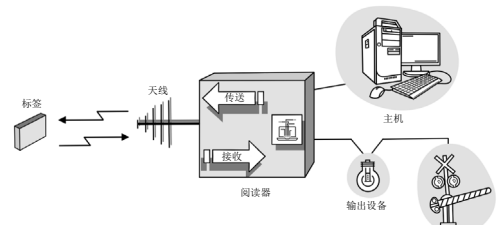
RFID发展历史



15

RFID工作原理

- RFID系统包括：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)。
- 工业界经常将RFID系统分为为阅读器、天线和标签三大组件。



16

RFID工作原理：阅读器

阅读器：RFID系统中最重要、最复杂的组件

- 通过标准网口、串口或USB接口同主机相连
- 通过天线同RFID标签通信

一般主动向标签询问标识信息，又被称为询问器（Interrogator）

阅读器和天线以及智能终端设备可以集成在一起，形成可移动的手持式阅读器



17

RFID工作原理：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，附着在物体上，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，利用感应电流获得能量通过反射信号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）



19

标签分类

被动式标签 (无源标签)	主动式标签 (有源标签)	半主动式标签
无电源	有电源	有电源
通过感应由阅读器发出的电磁波获得能量	电源为其通信提供能量	电源用于支持计算，通过感应阅读器电磁波进行通信
<ul style="list-style-type: none">• 通信距离短• 计算能力简单• 体积轻巧• 价格低廉	<ul style="list-style-type: none">• 通信距离远• 可支持复杂计算• 体积大• 价格昂贵	<ul style="list-style-type: none">• 兼有被动标签和主动标签的所有优点• 可携带传感器用于感知

21

RFID频率：低频（LF）

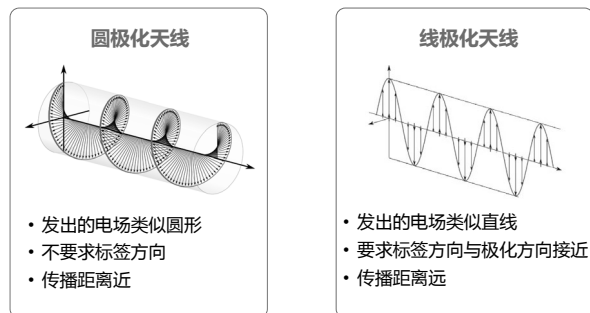
范围	30kHz-300kHz
典型工作频率	125kHz和133kHz
波长	大约为2500m
特点	一般都为无源标签，通过线圈电感耦合的方式从阅读器信号中获得工作能量。
通信范围	一般小于1米。
穿透性高	除金属材料外，能够穿过遮挡物且不降低读取距离。
典型应用	畜牧业管理系统、汽车防盗和无钥匙开门系统、自动停车场收费和车辆管理系统、门禁和安防管理系统等

23

RFID工作原理：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

按照极化方式分为圆极化天线和线极化天线



18

RFID标签与条形码相比的优点

体积小且形状多样：不受尺寸大小与形状限制。

环境适应性：对水、油等物质却有极强的抗污性。在黑暗的环境中也能被读取。

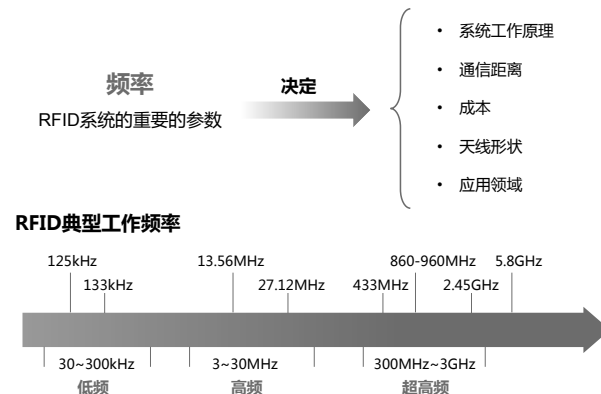
可重复使用：标签具有读写功能，电子数据可被反复覆盖，可重复使用。

穿透性强：被非透明材质包裹也可进行通讯。

数据准确性：利用循环冗余校验保证数据准确性。

20

RFID工作原理：频率



22

RFID频率：高频（HF）

范围	3MHz-30MHz
典型工作频率	13.56MHz
波长	约为22米
通信距离	一般小于1米
特点	不再需要线圈绕制，可以通过腐蚀印刷制作标签内天线，采用电感耦合的方式从阅读器辐射场获取能量。
穿透性	除金属材料外，能够穿过大多数遮挡物但会降低读取距离。
典型应用	图书管理系统、服装生产线和物流系统、三表预收费系统、酒店门锁管理、固定资产管理系统、智能货架管理等

24

RFID频率：超高频（UHF）

范围	300MHz-3GHz
典型工作频率	433MHz、860-960MHz
波长	大约30厘米
类型	超高频标签可以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。传输速率高，可短时间读取大量标签
通信距离	3-10米，最大可超过几十米。
穿透性	不能穿透水、灰尘、雾等悬浮颗粒物
典型应用	供应链管理、生产线自动化、航空包裹管理、集装箱管理、铁路包裹管理、后勤管理系统等

25

RFID数据存储：以UHF为例

保留区（reserved memory）：存储灭活口令和访问口令。	可读可写
EPC（electronic product code，电子产品编码）区：存储电子产品编码信息，赋予对象全球唯一的标识。	频繁读写
TID（tag identifier，标签识别号码）区：存储标签的识别号码，为出厂前就已固化的芯片序列号。	可读不可写
用户区（user memory）：用来存储用户自定义的数据。	可读可写

MemBank	
Bank 11	USER
Bank 10	TID
Bank 01	EPC
Bank 00	RESERVED

27

识别技术应用

智能卡产品的应用覆盖了社保、金融、交通、医疗、教育等国民经济的各个领域

二维码成为连接线上线下成本最低的接入口，手机扫码走天下已经成为人们的日常习惯

基于RFID标签对物体的唯一标识特性，引发了人们对物联网研究的热潮

- 日本和韩国将RFID视为未来关键发展技术，提出了泛在网络（UN）和泛在传感网络（USN）
- 中国在20世纪90年代开始了RFID的相关研究和应用试点，在各行各业的应用上取得了明显成效
- RFID技术在标准、成本、相关法律、技术成熟度等方面还存在挑战
- 但RFID技术的应用在物流、物资管理、物品防伪、快速出入、动植物管理等方面具有广阔的前景



30

本章小结

重点掌握

- 智能卡技术的基本概念、组成和分类
- 条形码的分类；条形码的工作原理，二维条形码与一维条形码的比较
- RFID的概念与现状
- RFID系统的组成，RFID标签的优点和特点，RFID标签的存储方式及分类，RFID系统的常见频率及其优缺点

32

RFID频率：其他频率

除了上述几个频段外，RFID标签还可以工作在2.45GHz和5.8GHz

由于传播衰减较大，这些频段多使用有源标签

日本的泛在识别（ubiquitous ID，UID）标准体系使用2.45GHz的RFID系统



26

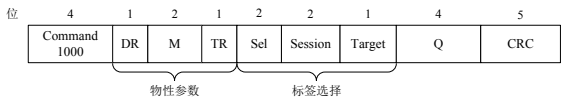
RFID消息格式

阅读器和标签通信的常见指令

Query、ACK、QueryRep、QueryAdjust、SELECT等

阅读器和标签通信的常见指令

- 消息总长22位
- Command字段通过代码1000来标识该消息是Query消息
- 标志位DR、M和TR，决定阅读器传输和标签响应的物理层参数
- Sel、Session和Target，用来选择相应的标签做出回应
- Q定义了标签响应的时隙总数2Q-1
- 校验和CRC，长度为5bit



28

本章小结

内容回顾

本章对常见的物联网识别技术做了介绍，包括：智能卡技术、条形码技术和RFID射频技术

本章重点讲述了RFID技术，包括RFID发展历史、RFID技术剖析和识别技术在物联网中的应用

31

内容回顾

前一章

介绍了识别技术的基本概念和典型应用，讨论了智能卡，条形码技术和RFID技术的历史发展，工作原理和优缺点。并描述了这类技术在生产生活方方面面的应用和未来发展趋势。

2

为什么需要定位

基于位置的服务

- 地图与导航 百度地图
- 搜索周边服务信息 大众点评
- 基于位置的社交网络 微信

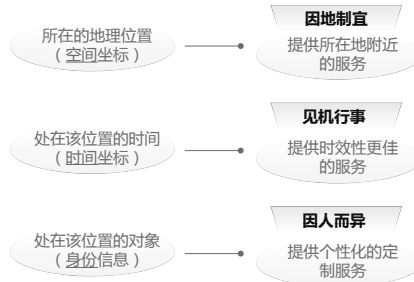


位置信息我们的生活息息相关

3

位置信息

位置信息不是单纯的“位置”



4

定位方法

定位的关键

- 有一个或多个已知坐标的参考点
- 测量待定位物体与已知参考点的空间关系
- 两个步骤

测量物理量 → 根据物理量确定目标位置

常见定位方法

- 基于距离（时间）的定位 (Time of Arrival, ToA)
- 基于距离（时间）差的定位 (Time Difference of Arrival, TDoA)
- 基于信号特征的定位 (Received Signal Strength, RSS)
- 基于到达角的定位 (angle of arrival, AoA)

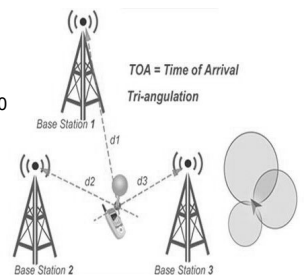


6

基于距离的定位（ToA）

距离测量方法

- 距离 $d = \text{波速} v \times \text{传播时间} \Delta t$
- 传播时间 $\Delta t = \text{收到时刻} t - \text{发出时刻} t_0$



问题

- 接收端如何得知 t_0 ?

7

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接收端记录

- 电磁波到达时刻 t_e
- 声波到达时刻 t_s

$$\text{距离 } d = \frac{v_r v_s (t_s - t_e)}{v_r - v_s}$$

由于 v_r 远大于 v_s ，上式可简化为 $d = v_s (t_s - t_e)$



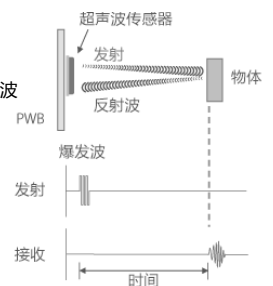
8

基于距离的定位（ToA）

方法2：测量波的往返时间

- 发送端于时刻 t_0 发送波
- 接收端收到波后，等待时间 Δt 后返回同样的波
- 发送端记录收到回复的时间 t

$$\text{距离 } d = \frac{v(t - t_0 - \Delta t)}{2}$$

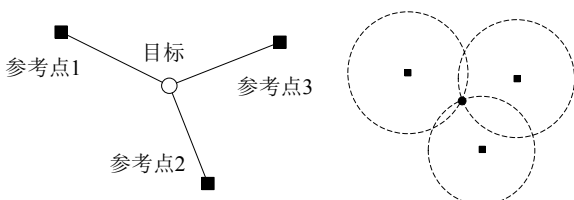


9

基于距离的定位（ToA）

位置计算方法：多边测量（也称多点测量）

- 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



10

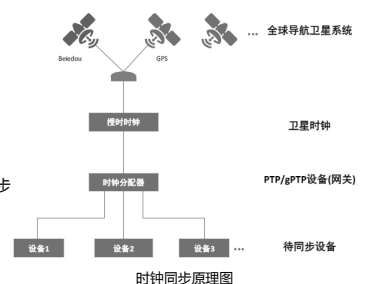
基于距离差的定位（TDoA）

ToA的局限

需要参考点和测量目标时钟同步

TDoA

- 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



11

基于距离差的定位 (TDoA)

距离差测距方法

测量目标广播信号

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

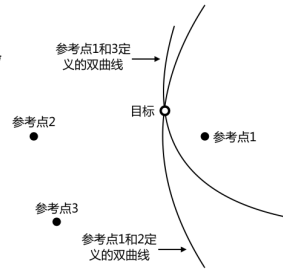
位置计算方法

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 $(x_i, y_i), (x_j, y_j)$
- 到参考点的距离 Δd_{ij}
- 构建方程: $\sqrt{(x-x_i)^2 + (y-y_i)^2} - \sqrt{(x-x_j)^2 + (y-y_j)^2} = \Delta d_{ij}$



12

基于信号强度测距的定位

ToA和TDoA都需要接收端特殊装置

基于信号强度测距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

13

基于信号特征的定位

解决方法

- 将信号强度特征看做“指纹”
- 预先布置N个参考节点
- 测出信号强度, 得到N维向量
- 事先测出每个位置的特征向量“指纹”
- 将目标测出的特征向量和数据库比对
- 找出最相似指纹对应的位置

缺点

不能应对动态变化



WiFi信号强度

14

基于信号特征的定位

右图以雷达图的形式呈现了空间中某个位置上的RSS特征向量

在这个位置上可以扫描到一系列Wi-Fi AP, 强弱不一

定位时根据当前位置的无线信号指纹, 在数据库中寻找最相似的



15

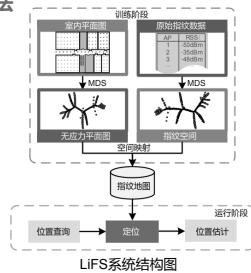
基于信号特征的定位

LANDMARC: 基于信号特征的动态定位方法

- 布置RFID标签作为参考标志
- 记录RSS信号强度特征向量
- 比对特征向量进行确定位置

LIFS: 基于群智感知的非现场勘测定位

- 关联RSS数据形成高维指纹空间
- 楼层平面图转换为无应力平面图
- 进行空间映射和指纹匹配
- 无需用户主动参与



16

基于到达角的定位 (AoA)

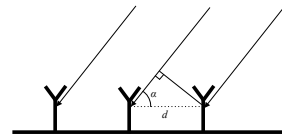
通过接收信号计算出信号到达的角度, 基于多个接收者的多个到达角度计算出目标的位置

在一个天线阵列上排布了多个规则放置的天线

基于在不同天线上收到的信号, 能够实际测量出 Δt

计算出到达角 α , 即目标到达天线的角度 $\Delta t = \frac{d \cos \alpha}{c}$

在有多组天线阵列时, 多个角度的交点就是目标的位置



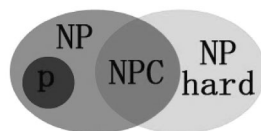
17

可定位性问题

网络可定位即网络中所有节点可定位

如何判断某个节点是否可以被定位?

当一个网络中仅有少量已知位置的信标点, 推算其他节点的位置是 NP-hard



可定位性问题也是网络管理和操作的重要基础

- 网络拓扑结构管理、网络节点部署、移动迁移管理、电源事务调度和路由转发机制都与可定位性紧密相关

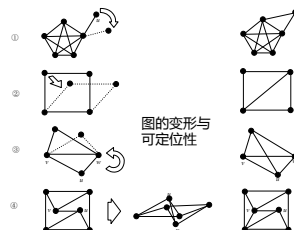
可定位性问题是定位的重要基础

19

网络可定位性

判断一个网络是不是可定位就是判断对应的图 G 是不是存在满足距离约束和 l 的唯一实现

一个网络可以被唯一定位的充要条件是: 该网络所对应的距离图是全局刚性的, 且该网络至少包含三个已知位置的节点



20

节点可定位性

节点可定位性问题具有更大的适用范围和可操作性

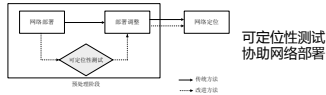
给定网络配置，如何判断某个节点是否可定位？

网络中有多少节点是可定位的？如何找出这些节点？

必要条件：如果一个节点是可定位的，那么它至少能够通过三条不相交的路径与三个已知位置节点相连接

充分条件：找到网络距离图的全局刚性子图并引入隐藏边

用节点可定位性改进过的方法分为两个阶段：数据预处理阶段和定位计算阶段



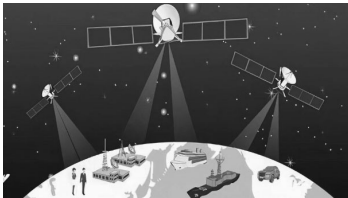
21

卫星定位

各国的卫星定位系统

- 美国：GPS (global positioning system)
- 俄罗斯：GLONASS
- 欧盟：伽利略 (Galileo satellite navigation system)
- 中国：北斗 (BeiDou navigation satellite system , BDS)

GPS是目前世界上最常用的卫星定位系统



24

现存主流定位系统

室外定位系统

卫星定位

- GPS
- 北斗卫星导航系统

蜂窝基站定位



室内定位系统

RFID 定位

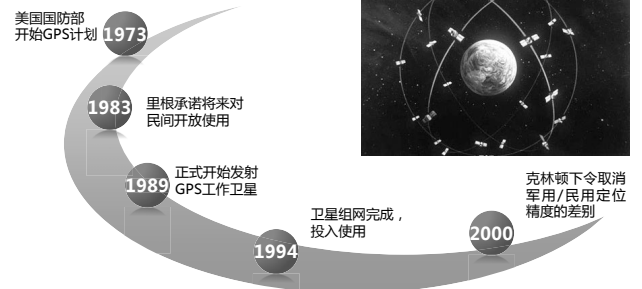
声音信号定位

可见光信号定位



23

起源与发展



25

GPS：系统结构

宇宙空间部分

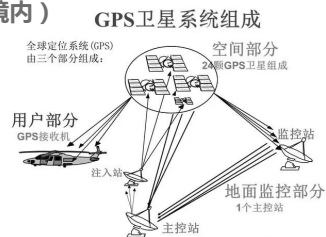
- 24颗工作卫星

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

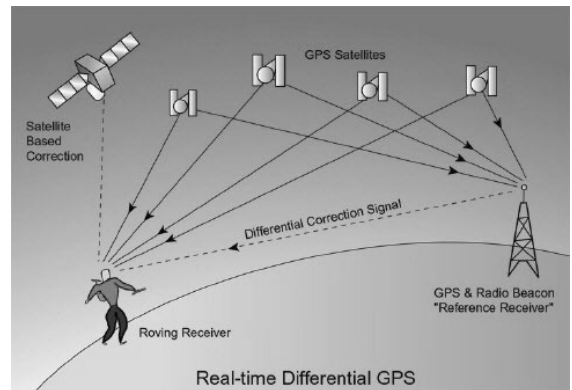
用户设备部分

- GPS接收机（一个和卫星通信的专用天线、用于位置计算的处理器以及一个高精度的时钟）



26

GPS：定位原理



27

GPS：主要优缺点

优点

- 精度高
- 全球覆盖，可用于险恶环境

缺点

- 启动时间长（初次定位需搜索几分钟）
- 室内信号差（电磁遮蔽的效应）
- 需要GPS接收机

28

A-GPS (Assisted GPS)

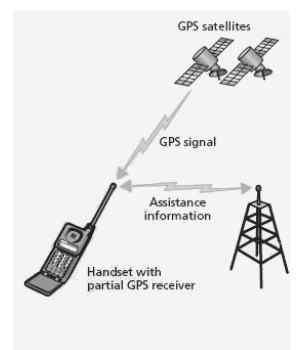
GPS定位和蜂窝基站定位的结合体

利用基站定位确定大致范围

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（几秒）

当前手机基本都采用A-GPS



29

GPS典型应用：汽车导航

最初仅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

互联网时代，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

物联网时代，感知更透彻

- 综合道路状况等各种因素找出最佳路线
- 由“以路为本”转变到“以人为本”



30

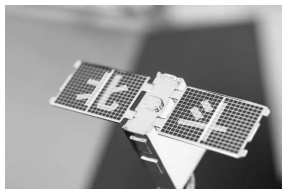
独门绝技

星间链路技术：将卫星与卫星、卫星与地面站均有联系起来，极大提升了安全性和定位精度

提供有源和无源两种定位服务：而GPS 只提供无源。有源定位能实现地面快速定位，容易指挥调度

短报文功能：卫星定位终端和卫星或北斗地面服务站之间能够通过卫星进行双向信息传输，GPS 只能单向

已有 120 多个国家和地区使用

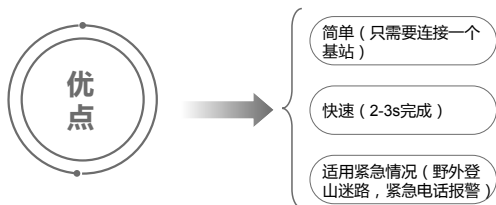


32

单基站定位法

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



34

蜂窝基站定位：主要优缺点

优点

- 不需要GPS接收机，可通讯即可定位
- 启动速度快
- 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

36

北斗卫星导航系统

空间部分：5 颗静止轨道卫星和 30 颗非静止轨道卫星

地面部分：主控站、注入站和监测站等 40 多个地面站

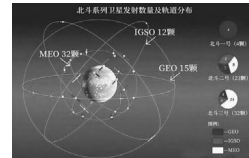
用户部分：成千上万的北斗用户及其他兼容的终端

北斗比GPS 多出 11 颗卫星

北斗 1 号：双星有源定位试验系统

北斗 2 号：亚太区域无源导航系统

北斗 3 号：覆盖全球的无源卫星导航系统

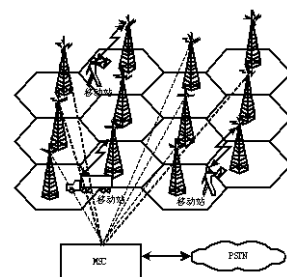


31

蜂窝基站定位

GSM蜂窝网络

- 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

- 对通讯设备进行定位

33

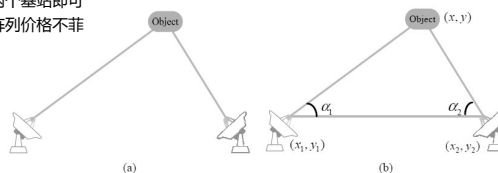
多基站定位法

ToA/TDoA定位法

- 测量无线信号传播时间，用信号到达不同基站的时间差来建立方程组求解位置，通过时间差抵消时钟不同步带来的误差
- 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

- 测量无线信号传播方向
- 需要两个基站即可
- 天线阵列价格不菲



35

典型应用：紧急电话定位

美国E-911系统

- 拨打报警电话时，根据基站定位手机位置，自动接到最近警局
- 综合了各种定位技术，包括ToA，TDoA，AoA，RSS，A-GPS
- 使用时尝试各种定位方法，择优而用



37

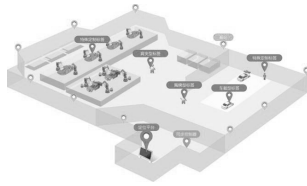
室内定位系统

GPS、北斗以及蜂窝定位等系统在空旷的室外场景下定位表现非常好

由于建筑物的遮挡，这些定位系统在室内无法获得足够的信号强度，因而无法提供精准的室内定位服务

用于室内的物联网定位典型技术

- RFID定位
- 声音信号定位
- 可见光信号定位



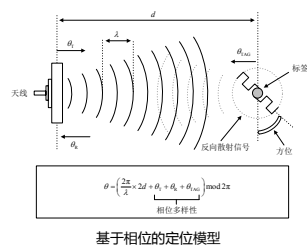
39

RFID 定位：相位

信号从阅读器发送，经过标签反射，又被阅读器接收

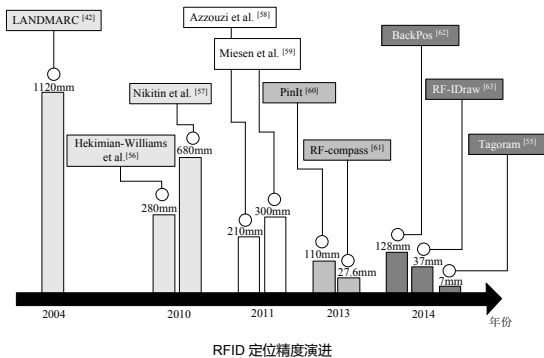
相位值与信号传播的距离 d 有关，信号每传播一个波长 λ 的距离，相位变化 2π

最终相位值受到阅读器信号发射器、接收器电路的物理特性与标签自身的反射特性的影响



41

RFID 差分增强全息图



43

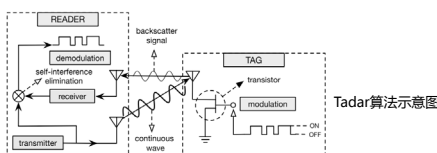
发展趋势：高灵敏度、非入侵、多模态

从设备绑定到非绑定

- 为了提升便利性和用户友好性，利用环境中原本的无线信号实现非接触式、被动式的感知

Tadar将定位范围延伸到隔墙定位移动物体

- 在墙外部部署一组标签形成天线阵列
- 分离和提取物体运动造成的信道变化
- 结合隐马尔可夫模型实现轨迹追踪
- 在隔墙条件下实现精确追踪



45

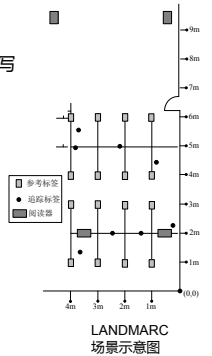
RFID 定位：RSS

定位背景：

- RFID通过标签反射的无线电信号实现对识别读写
- 无须建立机械或者光学接触
- 越来越多的物体上部署

定位原理

- 接收信号强度 RSS 随着距离的增加而衰减
- LANDMARC最早的非测距无线定位系统
- 网络信号强度分布与环境高度相关
- 提出在线定位模式，误差在1m左右



40

RFID 差分增强全息图

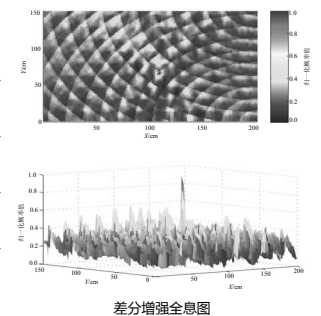
差分增强全息图 (DAH) 精度达到毫米级，精度最高

细粒度划分环境空间

采集目标标签的相位值

构造空间全息图

寻找概率最大的位置



42

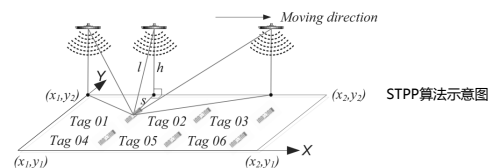
发展趋势：高灵敏度、非入侵、多模态

从绝对定位到相对定位

- 在一些应用中如图书馆书籍排序管理、仓库货物管理等，人们更关注一组标签之间的相对顺序，而无须知道它们的绝对位置

STPP提出一种基于相位值的标签排序算法

- 标签的相位值会随着距离变化先增大后减小
- 通过相位曲线峰值出现的先后顺序推断相对位置关系
- 可以在图书馆中实现智能图书排序



44

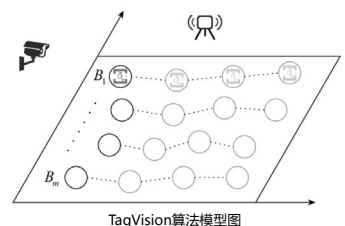
发展趋势：高灵敏度、非入侵、多模态

从单模态到交叉融合

- 将RFID与移动机器人、无人机、计算机视觉、SLAM等融合
- 不同模态数据优势互补，提取更加丰富的特征
- 提升定位精度和鲁棒性，拓展更多的智能化、自动化应用

TagVision将计算机视觉技术结合到RFID系统上

- RFID采集相位，视觉进行细粒度检测和追踪
- 融合数据计算匹配度来衡量其携带目标标签的可能性
- 硬件开销小，追踪精度高

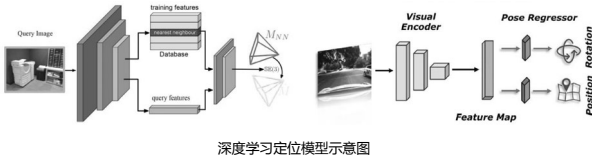


46

发展趋势：高灵敏度、非入侵、多模态

从基础模型到高级算法

- 早期主要使用基础的感知模型
- 后来机器学习方法提高性能
- 近年来，以卷积神经网络为代表的深度学习技术弥补传统方法的弊端，提高了定位系统的精度和鲁棒性
- 但需要大量被标记的数据并具有不可解释性等



深度学习定位模型示意图

47

发展趋势：高灵敏度、非入侵、多模态

从商用设备到专用设备

- RFID商用设备在带宽、稳定性，精度和鲁棒性方面存在问题
- 通用软件无线电外设（universal software radio peripheral, USRP）等专用设备可以获得更高分辨率的信息，从而提取更稳定的无线信号特征，实现更加普适性的高精度定位
- 专用设备的研究也有利于RFID通信协议的改进与开发，从根本上提升RFID系统的性能，但部署与开发成本高，难以普及



48

声音信号定位

智能设备普遍配有扬声器和麦克风，可以发送和接收声波信号

声音信号的传播速度远远低于电磁波信号，估算信号飞行时间（time of flight, ToF）更准确

声音信号的采样频率也更低。一般手机为48kHz，处理开销更小，时延更低，更适合算力有限的物联网设备



49

声音定位类型

基于设备的定位（device-based）

- 定位目标本身发出声音或者接收声音
- 对发声设备或声音接收设备的空间位置进行估计

与设备无关的定位（device-free）

- 定位目标本身不发出或者接收声音
- 借助人体或物体对声音信号的反射估计反射物的位置
- 反射物如手掌，手指，心脏等



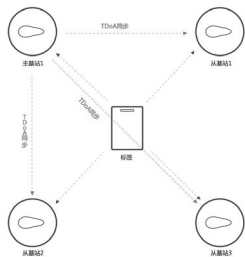
基于声音相位的目标追踪技术

50

声音定位技术（TDoA）

基于到达时间差（TDoA）

- 需要用到4个声源
- 定位误差控制在几十厘米范围内
- 通过计算TDoA解决发送端和接收端时钟不同步问题



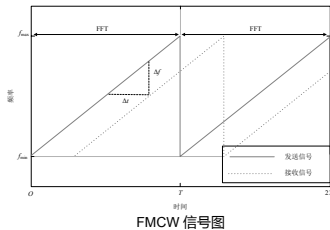
TDoA算法示意图

51

声音定位技术（FMCW）

基于调频连续波（FMCW）

- 可以将对ToF的测量转换为对信号频率差异的测量
- 通过持续测量声音设备到多个已知位置设备的距离变化量，可以实现对声音设备位置的追踪
- 当设置多个FMCW发送和接收设备时，即可实现对反射物体的定位，即与设备无关的定位



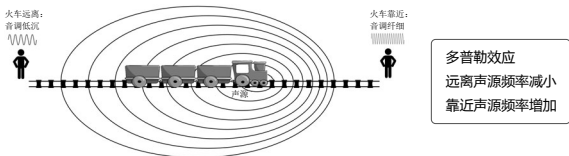
FMCW信号图

52

声音定位技术（多普勒）

基于多普勒效应

- 当波源与观察者存在相对运动时，观察者接收到的波的频率与波源发出的频率不同，且跟相对速度有关
- 利用短时傅里叶变换，分别对原始发送的信号和接收信号进行频谱分析，即可计算出频率的变化
- A.A.Mouse在位置固定的设备上播放声音信号，通过移动设备接收声音并测量频率变化情况，实现运动轨迹的追踪

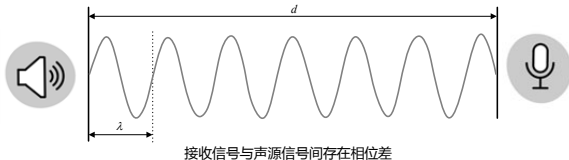


53

声音定位技术（相位偏移）

基于相位偏移

- 声音信号的相位特征也与传播路径长度密切相关
- 接收端收到的信号与声源处的发送信号之间相位差为 $\text{Phase} = 2\pi \frac{d}{\lambda}$
- 通过持续测量信号相位，计算相邻两次测量之间的相位变化，可以计算出相邻两次测量时接收端与声源之间距离的变化量
- Vernier结合游标卡尺的原理，计算得到精准的相位变化信息，在移动设备上实现了毫米级别的实时设备追踪



54

声音定位优缺点

优点

- 只需要扬声器和麦克风等简单硬件
- 对设备计算能力要求不高

缺点

- 声音信号在空气中的衰减严重
- 覆盖范围非常有限（如 2 ~ 3m）
- 与设备无关的定位方法基于反射信号，强度衰减更大，其有效工作范围更小。

55

可见光信号定位

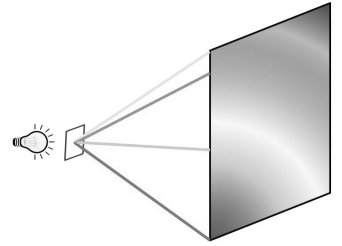
物联网设备可以对可见光进行控制，如控制 LED

使可见光信号特征与空间位置信息产生对应关系

光强传感器、光电二极管或相机等采集特征

分析光信号中携带的信息来推断接收端位置或朝向

从而实现定位、追踪和姿态感知



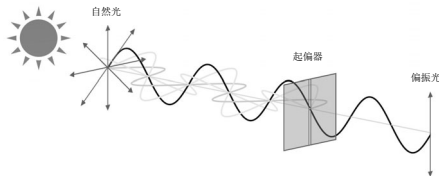
56

光的偏振

1801 年托马斯·杨进行了著名的杨氏双缝实验

光的偏振（polarization）是光的横波重要性质

自然光在通过作为起偏器的偏振片后，只剩下了特定振动方向的光线。穿过起偏器的光的震动只沿着单独的一个方向，这种光被称为“偏振光”



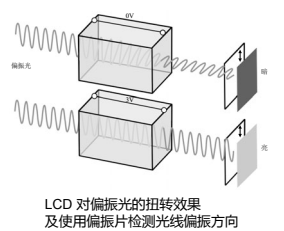
57

液晶显示器与偏振方向

液晶显示器（liquid crystal display, LCD）是常见的用于改变光线偏振方向的器件

改变电压就可以控制发射光线的偏振方向

在接收端的光强传感器前加上一层偏振片，根据穿过偏振片的光线强度来判断偏振方向



58

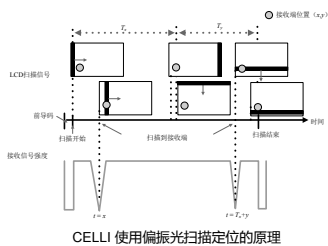
CELLI偏振光扫描定位原理

CELLI先水平条带扫描，再竖直扫描

控制条带上的偏振光与接收端透振方向垂直

当条带扫描经过接收端时会检测到光线强度降低

接收端根据两次条带扫过的时间来计算自身所在的位置

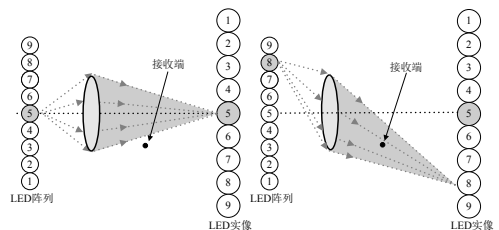


CELLI 使用偏振光扫描定位的原理

59

可见光空间特征定位

SmartLight 通过使用一个闪烁的 LED 阵列和一个凸透镜向空间中投射带有闪烁频率信息的可见光信号，实现利用可见光空间特征对接收端的定位



SmartLight 定位原理示意图

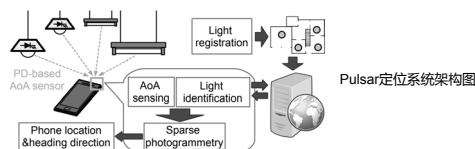
60

可见光空间特征定位

Pulsar 借助 LED 灯和荧光灯等光源自身固有的闪烁频率特征来识别光源身份的方法

利用光电二极管接收光源信号并测量光源频率，基于频率信息识别光源身份

借助光线入射方向和光电二极管采集到的光强之间的关系，反推出光线的到达角。基于 AoA 对接收端定位



Pulsar定位系统架构图

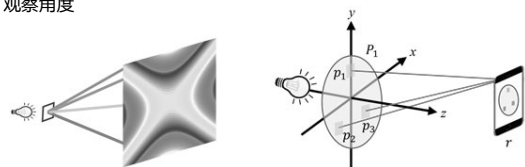
61

基于可见光空间分布特征

RainbowLight 实现在单个光源下对移动设备的三维定位

在单个光源前部署多个显色偏振膜片

用相机捕捉到的多个显色偏振膜片的颜色信息得到相机到各个膜片的观察角度



RainbowLight显色与方向的对应关系和系统示意图

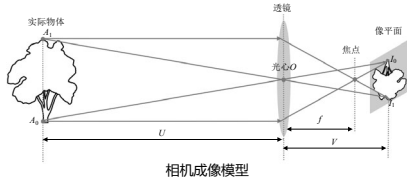
62

基于相机成像几何关系

光沿直线传播：物点、相机光心和像点位于同一直线上

当已知参数的相机拍摄到多个已知空间位置的物点，利用几何关系约束可以得到相机位置

借助用于 SLAM 的视觉标签，计算得到相机与标签之间的相对位置，可以反推出标签在空间中的位置



相机成像模型

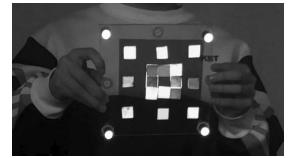
63

可见光定位应用示例

Luxpose和PIXEL为每个光源编码身份ID，在相机同时拍到3个以上光源时，计算出光源在照片中的像素位置，得到相机的位置和朝向

LiTell和iLAMP提出利用光源自身的闪烁频率或发光模式特征来对区分，降低改造电路的部署成本

LiTag结合显色偏振膜片、反光材料制作出不需要供电的纯被动式光学标签，结合RainbowLight中的显色偏振定位原理以及相机成像中的投影变换关系，实现无须相机参数的可见光定位系统



LiTag可见光定位偏振片效果图

64

可见光定位优缺点

优点

- 光源在环境中普遍存在
- 接收装置也很常见
- 不受多径和无线信号的干扰
- 天然地携带方向信息
- 低成本、易获取

缺点

- 容易被遮挡而无法工作
- 精度一般在十几厘米

65

物联网定位技术的现状

随着物联网的兴起，传统的室外定位方式已无法满足物联网场景下的定位需求

基于 RFID、声音信号、光信号等的新型定位方式的出现为物联网环境中的定位问题提供了新的解决思路

其他尝试如利用地磁信号的特征实现室内定位、利用震动传感器定位走动中的人体等



地磁效果图

67

物联网定位技术的挑战

应用场景要求严格

环境多变影响效果
环境的动态性造成的多径效应

定位范围相对有限
设备与已知位置的锚点
距离增加

多目标场景难以处理



68

物联网定位技术的前景

如何提高？
定位的范围实现
全场景覆盖

如何提高？
定位方法的鲁棒性
以适应高度动态的环境

如何实现？
高精度的大量目标定位

“基于位置的服务”正向我们展现出广阔的市场前景



更大的挑战
也意味着更大的机遇

69

本章小结

内容回顾

本章介绍了位置信息的基本概念，重点讨论了五种室内外定位系统以及四种典型的定位方法，并推导了网络和节点可定位性理论，最后探讨了物联网定位技术的挑战和前景

重点掌握

- 了解位置信息的三要素
- 了解GPS和蜂窝基站定位的系统组成，技术原理，典型应用和优缺点
- 了解RFID，声音，可见光室内定位的技术原理和优缺点
- 了解可定位性的理论分析以及网络和节点满足可定位性的条件

70

本章小结

重点掌握续

- 掌握基于距离的定位中距离测量的两种方法
- 掌握基于距离差的定位所采用的测量方法和位置计算方法，以及与基于距离的定位相比有何优缺点
- 掌握基于信号特征的定位方法
- 掌握基于到达角的定位方法
- 说明物联网定位技术的挑战和前景

71

承前启后

前一章

介绍了我们常见的一些定位技术和定位系统，包括GPS，北斗等室外卫星定位系统和LANDMARC等室内RFID定位系统

本章

我们主要关注物联网中的感知技术，包括传统的传感器和传感网感知，以及新兴的非传感器感知和群智感知。希望通过本章的学习，我们能掌握物联网感知技术的现状和未来发展趋势

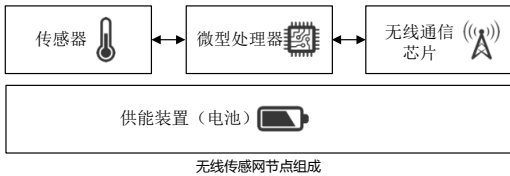
从传感器到传感网

传感网的诞生

- 传感器只能单点测量，网络化的程度有限，缺少信息共享
- 传感网则集成多个传感器，结合感知、计算与通信于一体，可进行规模化的有效感知。其中通信功能是最关键的不同点

传感网的基本组成

- 除传感器外，还集成了微型处理器、无线通信芯片和供能装置（电池）



软硬件平台

传感器

- 种类丰富，从相对简单的光传感器、温度传感器，到比较复杂的二氧化碳传感器等
- 处理器通过模拟和数字信号两种方式与传感器进行交互。基于模拟信号的传感器必须先数字化，而基于数字信号的传感器可直接使用

微型处理器

负责计算的核心

微处理器芯片集成了内存、闪存、模/数转换器 and 数字输入/输出（input/output，I/O）等



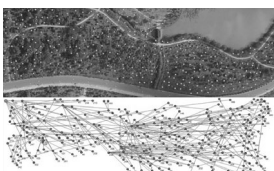
自组织网络协议

为什么不直接使用互联网的TCP/IP协议

- 资源限制：传感网节点资源有限，而实现和运行完整的TCP/IP协议是比较消耗资源的
- 大材小用：传感网数据采集传输的功能相对简单，是否有必要采用功能强大的TCP/IP协议存在疑问

什么是自组网

指网络中没有固定的网络结构，网络设备需要在不依赖于中央控制设备的情况下实现自组网，处理节点移动、加入和退出等操作



GreenOrbs中的自组网

传感器

什么是传感器

- 人类是通过视觉、听觉等感性的方式感知周围环境的
- 而传感器是能感受被测物理量并按照一定规律转换成可用输出信号的器件或装置



传感器的基本组成

- 一般由敏感元件、转换元件和基本电路组成
- 敏感元件是指能直接感受被测物理量的部分
- 转换元件将敏感元件的输出转换成电路参量，如电压、电感等
- 基本电路最终将电路参数转换成电量输出



从传感器到传感网

传感网的历史

美国军方在越南战争期间部署“雪屋”系统

1967

1996 UCLA的威廉·凯泽教授开展LWIM项目

1996 加州大学伯克利分校和军方发起了“智慧尘埃”项目



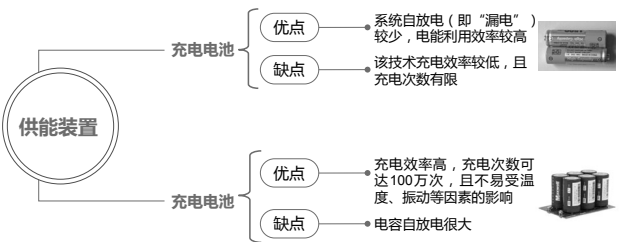
大鸭岛传感器网络节点和部署环境

2002 在美国大鸭岛（Great Duck Island）实现部署

软硬件平台

无线通信芯片

- 通信芯片能耗是节点能耗的主要来源。例如，TelosB节点上CPU工作电流仅为500μA，而通信芯片工作电流达近20mA。且通信芯片各工作状态消耗的能量差别不大
- 通信芯片传输距离是节点的重要指标，其受芯片的发射功率等因素影响



自组织网络协议

设计方法

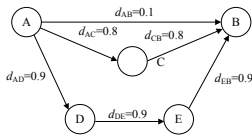
- 网络的建立依赖于对链路和路径质量的测量和评估，典型的组网协议可以选择到达目的节点最短的路径
- 期望传输次数（expected transmission count，ETX）是无线传感网中广泛使用的路由指标之一
- 记 d_f 为从源节点到目的节点的收包率， d_r 为从目的节点到源节点的ACK的收包率，则有：

$$ETX = \frac{1}{(d_f \cdot d_r)}$$

自组织网络协议

期望传输次数

- 把传输代价最小化，提高带宽利用率，减少能量消耗
- 测量双向链路质量，能有效避免非对称链路带来的影响
- 一条路径的ETX为该条路径所有链路的ETX之和。如图所示：（假设链路反向的收包率 d_{r} 均为1）



路径A→B：ETX=10

路径A→C→B：ETX=1.25+1.25=2.5

11

传感网系统探索

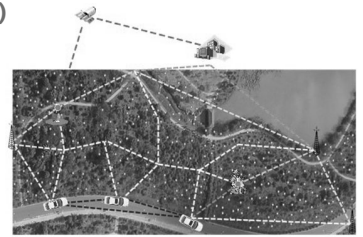
绿野干传（GreenOrbs）

清华大学研究团队发起的大规模室外无线传感网项目

用途：森林碳监测传感网系统

部署地点：

- 浙江省天目山自然保护区
- 浙江农林大学校园部署



GreenOrbs系统部署（森林区域）

12

无线传感网发展中的挑战

传感失谐 → 传输和感知不匹配

- 图像等数据量大且要求实时传输，难度大
- 部分数据缺乏对应可大规模部署的低成本传感器

诊疗失据 → 网络管理困难

- 节点环境恶劣且通信和计算资源有限，类似SNMP类型的Agent汇报机制无法被有效支持

模型失用 → 模型过于理想

- 基于理想化的模型假设忽略了无线传感网运行过程中的不确定物理因素和环境动态性，与实际情况之间有落差

13

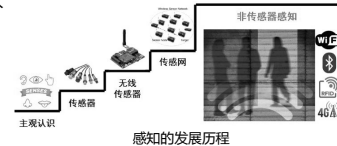
从传感网到无传感器感知

传统感知暴露问题

- 传感系统的部署和维护成本太高

非传感器感知打破传统思维

- 利用环境中已有的感知媒介，如声、光、射频信号等无线信号
- 通过分析无线信号在传播过程中的变化，获得信号传播空间的特性，以实现对环境感知。将感知与通信合二为一
- 具有“三无”的特性：无传感器、无线和无接触
- 基于雷达系统、超宽带信号和WiFi信号的感知技术层出不穷。以WiFi感知为例介绍无线感知技术

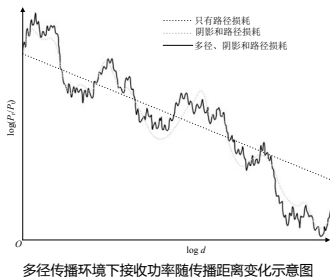


15

基于接收信号强度RSS

用RSS表征接收机位置信息

- RSS的强弱在一定程度上反映了信道质量的好坏
- 但RSS会因信号阴影衰落、多径等影响而不再随传播距离增加而单调递减，从而限制测量精度

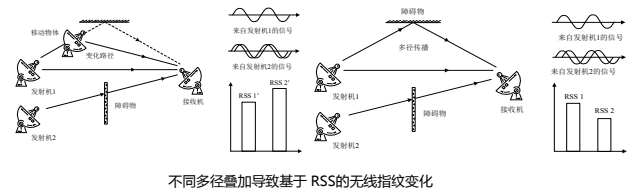


多径传播环境下接收功率随传播距离变化示意图

16

基于接收信号强度RSS

且RSS是多径叠加的结果，不能区分多径



不同多径叠加导致基于RSS的无线指纹变化

17

基于信道冲激响CIR

用CIR表征接收机位置信息

- 为刻画多径传播，无线信道通常可用信道冲激响CIR建模
- 在线性时不变假设下，CIR可表示为：

$$h(\tau) = \sum_{i=1}^N a_i e^{-j\theta_i} \delta(\tau - \tau_i)$$

- 式中： a_i 、 θ_i 、 τ_i 分别为第*i*条路径的幅度衰减、相位偏移和时间延迟。N为传播路径总数。 $\delta(\tau)$ 为狄拉克（Dirac）脉冲函数。式中的每一项从时域上表示了一条传播路径的幅度、相位和时延

对于WiFi信号

- WiFi设备可从每个接收数据包中获取一组CSI，每组CSI代表了一个正交频分复用OFDM子载波的幅度和相位，即：

$$H(k) = \|H(k)\| e^{j\angle H(k)}$$

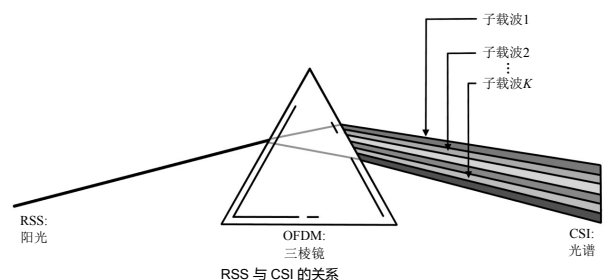
- 式中： $H(k)$ 为第*k*个子载波的CSI。 $\|H(k)\|$ 和 $\angle H(k)$ 分别为其幅度和相位

18

RSS与CSI的特性比较

CSI可以看作RSS的升级版

若RSS是白光，则CSI是以OFDM为棱镜色散出的光谱。每一束单色光（对应OFDM中的不同子载波）都呈现了不同频率下多径传播的幅度和相



RSS与CSI的关系

19

RSS与CSI的特性比较

CSI可以看作RSS的升级版

- CSI同时测量多个子载波的频率响应
- CSI不仅测量子载波的幅度，还测量对应的相位信息

类别	RSS	CSI
网络层次	MAC层	物理层
时间分辨率	数据包尺度	多径信号簇尺度
频率分辨率	无	子载波尺度
稳定性	低	高 (CSI整体结构)
普适性	几乎所有WiFi设备	部分WiFi设备

人员检测

PADS

- 人员会遮挡部分原始反射的信号，同时引入额外的反射信号
- PADS提出对CSI的幅度和相位分别提取协方差矩阵，即

$$A = \left[\text{cov}(\overline{H_i}, \overline{H_j}) \right]_{K \times K}$$
$$B = \left[\text{cov}(\overline{\phi_i}, \overline{\phi_j}) \right]_{K \times K}$$

式中： $\overline{H_i}$ 为第i个子载波上的CSI幅度归一化之后的值。 $\overline{\phi_i}$ 为第i个子载波上的CSI相位归一化之后的值。K为WiFi信号子载波的个数。

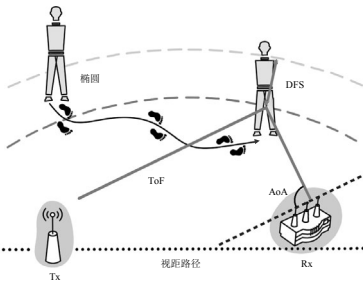


人员检测示意图

位置追踪

Widar 2.0

- 根据CSI的相位得到信号飞行时间ToF，那么人的位置就在以收发机为焦点的椭圆上
- 用3根等间隔摆放的天线计算出信号到达角AoA，进一步追踪

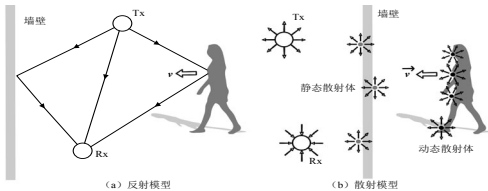


基于 CSI 的人员位置追踪模型

身份识别

GaitWay

- GaitWay提出一种新型的散射模型应对多径复杂的场景
- 通过散射体速度与CSI的关系，建立CSI与人体运动速度的定量关系
- 从中提取特征用于SVM分类器识别，达到90.4%的手势识别率

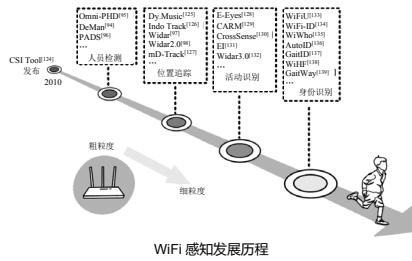


信号的反射模型与散射模型

WiFi感知粒度的进步

WiFi感知技术的对象多样，应用丰富

提取WiFi网卡CSI的工具推动了感知粒度的发展

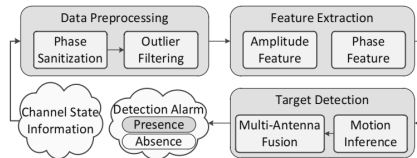


WiFi 感知发展历程

人员检测

PADS

- PADS分别提取了两个协方差矩阵各自两个最大的特征值组合成最终用于识别的特征向量，即 $[\alpha_1, \alpha_2] = \text{max}(\text{eigen}(A))$ $[\rho_1, \rho_2] = \text{max}(\text{eigen}(B))$ $F = [\alpha_1, \alpha_2, \rho_1, \rho_2]$
- 基于上述特征向量，PADS训练了一个支持向量机SVM用于对特征进行二分类
- 在区分噪声和人员引起的CSI扰动时，平均检测准确率97%

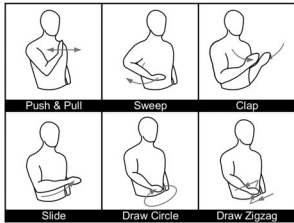


PADS人员检测模型

活动识别

Widar 3.0

- 提出人体坐标系速度谱BVP的概念，反映了人体所有反射点的运动速度的能量分布
- BVP通过旋转、放缩等操作来补偿人体的旋转、加减速等运动对信号的影响，并将环境反射的静态分量滤除
- 使用卷积神经网络CNN与循环神经网络RNN联合识别模型，达到92.7%左右的手势识别精度



Widar 3.0活动识别模型

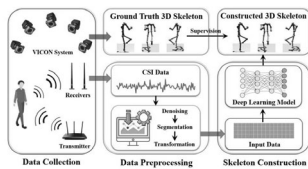
从朴素算法到人工智能

传统的朴素算法遇到瓶颈

- 难以满足高精度、高鲁棒性的感知需求

WiFi感知借力人工智能

- XModal-ID尝试将计算机视觉技术与WiFi感知紧密结合
- WiPose建立了CNN+RNN联合深度学习模型
- STFNets提出短时傅里叶神经网络



WiPose人体姿态构造模型

非传感器感知技术前景

非传感器感知未来发展的挑战

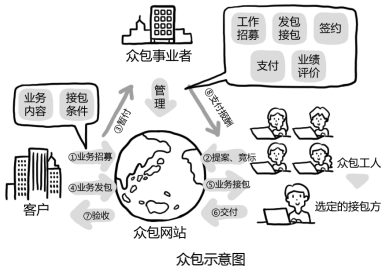
感知维度	目前感知还主要集中在对位置和动作的感知。
感知精度	现实中感知受噪声干扰，感知目标复杂，导致实际感知精度降低。
场景适应	许多感知工作只能在可控的实验场景下达到较好的感知效果。
部署成本	感知信号的收发和处理仍需要专门设备，增加了部署成本。
隐私问题	感知覆盖的场景和范围较大，会对人的隐私造成一定影响。

28

感知任务的分发与收集利用

众包

- 企业利用互联网将工作分配出去、发现创意或解决技术问题
- 通过互联网，这些企业可以利用大量用户的创意和能力
- 与外包的不同点在于，任务和问题是外派给不确定的群体



31

感知任务的分发与收集利用

reCAPTCHA利用全球智慧数字化古籍

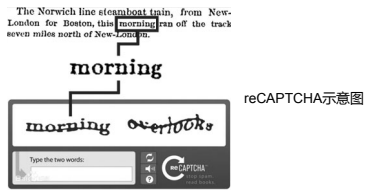
早期验证码是将随机字符串图像进行设计而成的



Luis von Ahn提出用这些脑力解决“图书数字化”问题

reCAPTCHA让人们每次辨识两个而非一个验证码

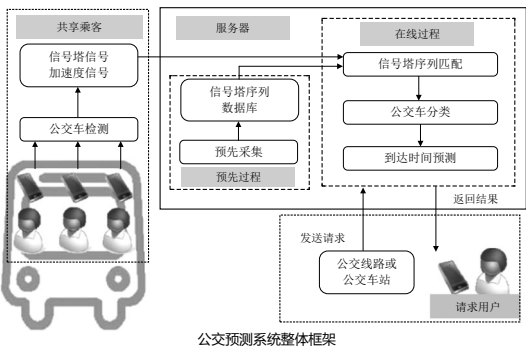
其中一个为早期验证码，而另一个则是从印刷品中选取的计算机不认识的字符图像



33

案例分析

公交车到站时间预测



35

概念

什么是群智感知

- 大量普通用户使用手机等移动设备作为基本感知单元
- 通过移动互联网进行协作，实现感知任务分发与数据收集利用
- 最终完成大规模的、复杂的感知任务

群智感知的特点

- 参与者无须是拥有专业技能的人士，可主动参与或被动参与
- 群智感知中的感知任务常是复杂的

30

感知任务的分发与收集利用

SETI@home 足不出户寻找外星人

- Arecibo望远镜搜索太空中的无线电信号并记录
- SETI@home服务器端将收集到的数据划分为工作单元，并通过互联网传送到全球各客户端进行处理
- 客户端在闲置时对数据进行预处理，完成后送回并下载新的数据
- 服务器收集数据，并筛选出可用信号在下次观测太空中在同一方位进行确认
- 一旦信号被确认，SETI@home将发表公告。相关客户端会被一起赋予“合作发现者”的称号

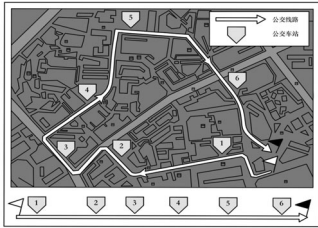


32

案例分析

公交车到站时间预测

- 公交车线路是一条特定的直线
- 利用手机信号形成一个信号塔序列



34

发展趋势

群智感知未来发展的挑战

数据质量管理

- 用户的感知数据存在不精确、不完整等质量问题
- 用户感知方式的不同影响感知数据的正确表达和解释
- 如何有效管理不同参与者提供的感知数据质量是重要挑战

多维数据融合

- 手机上的传感器数据包括加速度计、摄像头等，需要经过不同层次的加工，才能展现出人们感兴趣的内容
- 如何利用多维传感器，挖掘社会事件与人群活动是重要挑战

用户协同感知

- 用户的社交行为是多个移动设备上感知信息协同处理的基础
- 如何利用多用户协同感知提供有效的群智感知的结果是重要挑战

36

本章小结

内容回顾

本章我们介绍了物联网中的感知技术，包括传统的传感器和传感网感知，以及新兴的非传感器感知和群智感知

重点掌握

- 了解传感网感知的概念与实现
- 理解非传感器感知的原理
- 了解群智感知计算的概念与常见应用

37

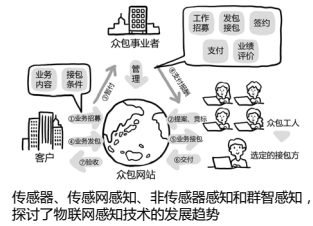
内容回顾

前一章

介绍了物联网中的感知技术

重点讨论了

传感器、传感网感知、非传感器感知和群智感知，探讨了物联网感知技术的发展趋势



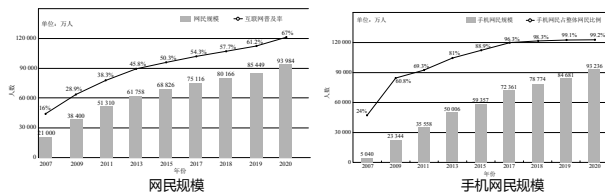
2

概论：移动互联网时代

截至2020年6月，中国手机网民规模已突破9.3亿，中国网民规模达到约9.4亿

设备接入

- 移动通信技术接入运营商网络
- 短距离接入技术（无线）接入互联网



4

移动通信技术发展

第一代移动通信 (First Generation, 1G)

- 20世纪80年代
- 提供模拟语音服务



第二代移动通信 (2G)

- 数字化传输，仍在使用
- 支持传统语音通信、文字、多媒体短信、电子邮件、传真等应用
- 代表性网络：全球移动通信系统GSM，码分多址访问系统CDMA



5

移动通信技术发展

第三代移动通信 (3G)

- 数字信息多元化
- 支持带宽多媒体服务



第四代移动通信 (4G)

- 支持图片、视频在智能移动终端快速传输
- 网络吞吐量提升
- 时延降低



6

移动通信技术发展

第五代移动通信 (5G)

海量物体无线联网

结合云计算和大数据技术，充分物联化和智能化

技术指标

- 峰值速率：20Gb/s
- 用户体验数据率：100Mb/s
- 移动性：500km/h
- 时延：1ms
- 连接密度：每平方公里百万个
- 流量密度：10Mb/s/m²

主要通信应用场景

- 增强型移动带宽
- 大规模机器通信
- 超高可靠低时延通信



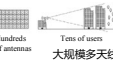



7

移动通信技术发展

第五代移动通信 (5G)

关键技术

毫米波技术 毫米级波长，工作频段30-300GHz，增加可利用带宽  毫米波	微基站技术 小体积、低功耗、低部署成本  微基站	大规模多天线技术 源自多输入多输出 (MIMO) 系统，使用多路天线，同时面向更多用户接收 (发送) 数据  Hundreds of antennas Tens of users 大规模多天线	波束成形技术 聚集信号能量至比较窄的方向，发射信号具有高度方向性  波束成形
---	---	---	---

8

移动通信技术发展

第五代移动通信 (5G)

技术标准 (3GPP发布)

- Release 15: 2019年4月完成
- Release 16: 2020年7月完成
- Release 17: 2022年完成

截至2020年11月，全球范围内共部署了122个商用5G网络；129个国家的407家运营商对5G系统提供投资，包括测试、获取运营许可、网络部署等领域



9

移动通信技术发展

第六代移动通信（6G）：

预计提供

- 更高频率效率和能量效率的全球网络覆盖
- 更低成本
- 更好智能控制水平
- 更强大安全性

《2020高技术发展报告》

- 在未来的6G中，网络与用户将被作为一个整体，进一步挖掘和实现用户的智能需求



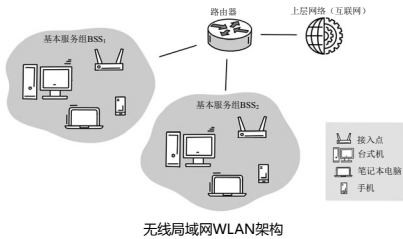
10

802.11架构

基站模式

基本服务组（Basic Service Set, BSS）

- 多个无线用户（笔记本电脑、台式机）：通过与接入点相关联获取上层网络数据
- 一个接入点（基站）：通过有线网络设备（交换机/路由器）连入上层公共网络。“无线路由器”是接入点和路由器功能的结合体



无线局域网WLAN架构

13

蓝牙

起源

1994年，瑞典爱立信公司研发短距无线通信技术，并用Harald Blatand（英译为Harold Bluetooth）国王的名字命名

标志

保留了蓝牙名字的传统特色，包含了古北欧字母“H”和一个“B”

蓝牙技术联盟

成立于1998年，成员包括爱立信、IBM、Intel、东芝和诺基亚等国际通信巨头



15

蓝牙

蓝牙4.0

- 2010年7月7日推出
- 模式：高速蓝牙、经典蓝牙和低功耗蓝牙（Bluetooth Low Energy, BLE）
- 目的：应对以数据交换与传输、信息沟通与设备连接、低带宽设备连接为主的不同应用需求

技术规范	传统蓝牙	低功耗蓝牙
无线频率	2.4GHz	2.4GHz
理论通信距离	100m	>100m
空中数据率	1~3Mb/s	1Mb/s
支持活跃外围设备数	7	未定义（理论最大值为2 ³² ）
延迟	100ms	6ms
安全性	64/128bit AES	128bit AES
语音能力	有	无
耗电量	1W（参考值）	0.01~0.5W（依赖使用情况）
峰值电流消耗	<30mA	<15mA

传统蓝牙和低功耗蓝牙的技术指标对比

17

Wi-Fi：无线局域网

Wi-Fi

一般指IEEE 802.11系列协议



IEEE802.11协议

目的：规范和统一无线局域网

典型使用频段

- 2.4-2.485GHz公共频段
- 5.1-5.8GHz高频频段

物理层技术

- 直接序列扩频DSSS
- 正交频分多路复用OFDM

IEEE 802.11协议	发布时间	频宽 (GHz)	最大带宽 (Mbps)	调制模式
IEEE 802.11-1997	1997.6	2.4~2.485	2	DSSS
IEEE 802.11a	1999.9	5.1~5.8	54	OFDM
IEEE 802.11b	1999.9	2.4~2.485	11	DSSS
IEEE 802.11g	2003.6	2.4~2.485	54	DSSS或OFDM
IEEE 802.11n	2009.10	2.4~2.485或5.1~5.8	100	OFDM
IEEE 802.11ac	2014.1	5.1~5.8	866.7	OFDM

不同802.11协议的不同特征

12

802.11架构

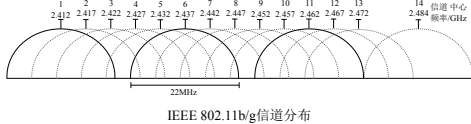
基站模式

用户与接入点关联方式

- 被动扫描：接入点广播“识别帧”，用户接收“识别帧”
- 主动扫描：用户广播“探测帧”，接入点返回“回应帧”

接入点参数

- MAC地址：唯一确定了网络接入点的身份
- 服务集标识符SSID：接入点管理者为每个SSID指定一个频段作为通信信道



IEEE 802.11b/g信道分布

自组织模式

- 无需基站
- 每个无线网络用户既是数据交互的终端，也可作为数据传输过程中的中继和转发者

14

蓝牙

蓝牙技术IEEE 802.15.1标准

- 物理层：跳频扩频结合的调制技术
- 频段范围：2.402GHz-2.480GHz
- 通信速率：1Mbps左右
- 设备角色：中心设备，外围设备
- 同一个蓝牙设备可以在两种角色之间转换
- 一个中心设备可以最多同时和7个外围设备通信
- 在任意时刻，中心设备单元可以向任何一个外围设备单元发送信息，也可以用广播方式同时向多个外围设备发送信息



发展

- 截止到2020年1月，共七个版本V1.1/1.2/2.0/2.1/3.0/4.0/5
- 美国《网络计算》杂志曾将其评为“十年来十大热门新技术”之一

16

蓝牙

蓝牙5

2016年12月推出

支持基于天线阵列测量到达角（AoA）



模式

- 短距离快速传输模式：将数据率提升为BLE的2倍，即2Mb/s
- 长距离低功耗传输模式：将通信距离提升为BLE的4倍，理论上的有效距离可达400m



蓝牙耳机



蓝牙鼠标



蓝牙键盘



蓝牙游戏手柄

18

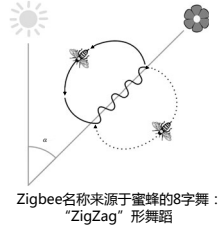
ZigBee

起源

基于IEEE 802.15.4标准的低功耗局域网协议

功能

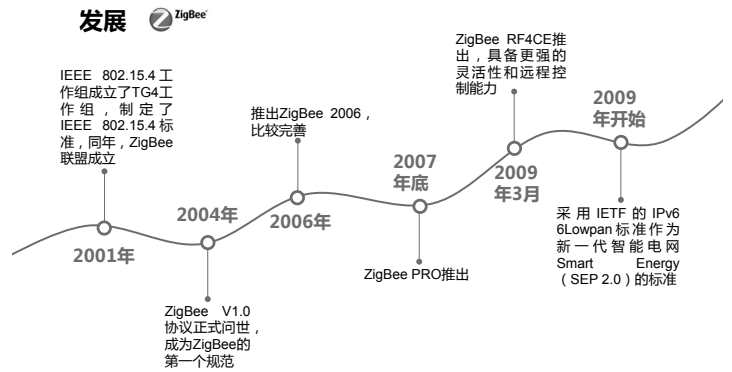
实现类似于蜂群通信的低功耗、低复杂度、低速率、自组织的短距无线网络，为个人或家庭范围内不同设备之间的低速互连提供统一标准



19

ZigBee

发展



20

ZigBee

工作频段

最高传输速率

2.4GHz (全球流行)	250kbit/s
868MHz (欧洲流行)	20kbit/s
915MHz (美国流行)	40kbit/s

传输距离：10-180m(室内一般不超过60米，室外一般不超过180米)



21

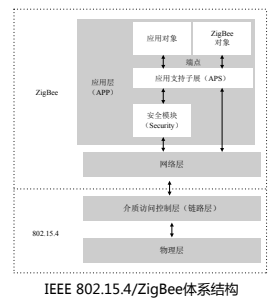
ZigBee

协议栈

开放系统互联 (OSI) 五层模型，包括物理层、介质访问控制层、网络层、传输层，以及应用层

IEEE 802.15.4标准规定了物理层和链路层的规范

ZigBee则提供网络层、传输层和应用层规范

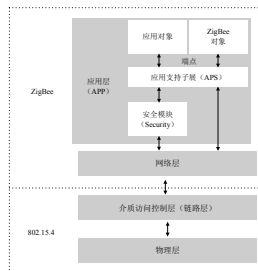


22

ZigBee

标准规范

- 物理层**：最早采用直序扩频DSSS，具有很好的抗干扰效果。在发射功率为0dBm时，室内能达到30~50m通信距离，室外能达到100m以上通信距离
- MAC层**：通过采样侦听 (sampling listening) 方式实现低功率侦听 (low power listening, LPL) 协议
- 网络层**：基本路由协议是按需距离矢量路由协议 (ad hoc on-demand distance vector routing, AODV)

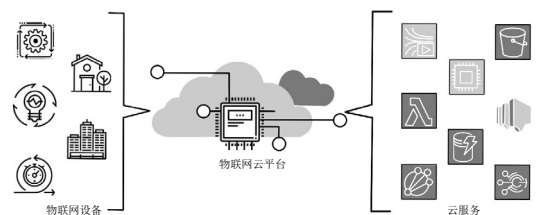


23

物联网云平台

简介

- 物联网设备深入人类生活各个角落，实现感知功能的大范围覆盖
- 云计算技术利用高性能与大规模的服务器集群，实现对海量数据的快速处理
- 物联网云平台作为物联网设备与云服务的桥梁，结合二者的优势，向下管理各种边缘设备、向上为云服务提供各种帮助

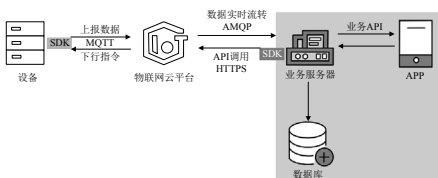


25

物联网云平台

工作流程

- 数据由设备上到物联网云平台
- 云平台对数据进行存储、计算
- 云平台将数据提供给上层云服务
- 云服务可以通过物联网云平台给处于网络边缘的设备发送指令



阿里物联网云平台工作流程

26

基于物联网云平台搭建物联网

优势

- 使用云服务商提供的各种云服务
- 利用云服务商提供的大数据、人工智能等平台，使物联网的应用信息化、数字化和智能化
- 基于云平台搭建的物联网，能享受云计算、云存储、云网络等基础服务所带来的便利
- 物联网云平台使用虚拟化技术，可以满足物联网的多接入、多并发、弹性伸缩、自动运维、快速部署的需求



27

总结

移动互联网是物联网的基础，其原因在于随着网络技术的发展，移动互联网形成了一个覆盖全球的、高速的、稳定的信息高速公路。在此基础上，海量的感知数据才能被有效地收集和利用，智能的决策才能及时地反馈到广袤的物理世界中

移动互联网不仅是物联网中物物互联的基础，也是整个社会信息交流的基础设施。移动互联网本身包含了宏大的技术体系和大量不断发展的技术

承前启后

前一章

介绍了物联网中移动通信技术与短距离接入技术，以及这些技术的重要作用。

本章我们主要关注

低功耗广域网、毫米波通信、声音通信、可见光通信以及跨协议通信等新兴通信技术的方法和特点。

低功耗广域网的发展

传统网络技术或不支持远距离通信、或消耗终端大量能量，为满足物联网连接需求，一批远距离、低功耗、低带宽的协议大量涌现。

对于这类远距离、低功耗、低带宽的协议，我们统一称之为低功耗广域网（Low Power Wide Area Network）技术。

远距离 乡村区域最远可达10公里

低速率 Kb/s 数量级

低成本 <\$5

低功耗 电池寿命超过10年

技术特点

低功耗广域网

低功耗广域网特征

- 数据速率：带宽较小，适合数据速率要求低的应用
- 传输距离：传输距离较远，适合数据分布在各家各户的应用
- 通信能耗：一般部署规模大且采用电池供电，为了保证长期工作且避免频繁更换电池，设备的通信能耗应尽可能低。

低功耗广域网典型应用

植被监测



智能水表



环境治理



本章小结

内容回顾

本章介绍了移动互联网的发展，重点介绍了3种常见的短距离无线接入技术，并讨论了物联网云平台在移动互联网中的作用

重点掌握

- 了解移动互联网的发展历程
- 认识不同移动通信技术标准的特点以及区别
- 了解3种常见的短距离无线接入技术
- 了解物联网云平台的概念

低功耗广域网的发展

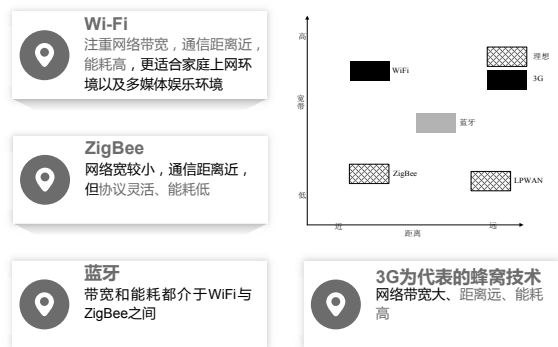
物联网发展提出不同类型的应用需求

催生出多样化通信协议



低功耗广域网

不同的网络技术分别对应不同的应用场景与需求



低功耗广域网

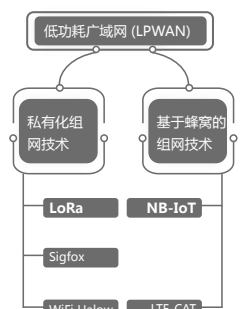
低功耗广域网技术分类

私有化组网技术：以LoRa为代表

- 高灵敏物理层调制技术
- 低占空比通信模式
- 工作在免费频段ISM
- 允许用户通过自行部署网关构建私有化网络系统

基于蜂窝的组网技术：以NB-IoT为代表

- 由电信运营商和设备商主导
- 基于已有的3G、4G长距离通信系统
- 简化协议架构、降低占空比，压缩终端能耗



LoRa协议

2013年Semtech公司发布了SX127x系列芯片，LoRa协议自此登上了无线通信的历史舞台

2016年，荷兰电信运营公司KPN宣布，荷兰已经成为世界上第一个推出全国性LoRa物联网应用网络的国家

包括中兴在内的多家相关企业加入LoRa联盟，进一步推动LoRa协议、芯片和应用平台的发展

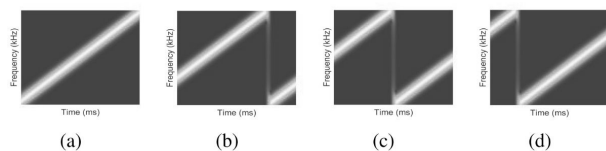


9

LoRa为什么能远距离

LoRa物理层信号调制策略

- 在频域循环频移chirp进行数据的编码，不同的起始频率代表不同的数据
- 如图，在带宽B内四等分标四个起始频率，我们可以得到4种类型的符号，分别表示00, 01, 10, 11



- 在接收端，只需要将这个起始频率计算出来，就可以计算出每一个chirp对应的比特数据

11

LoRa物理层信号调制

LoRa数据包结构

- 前导码 (Preamble)：前导码包含6~65535个标准upchirp和两个标识网络号的其他chirp符号
- SFD (Start Frame Delimiter)：2.25个标准downchirp，作为SFD标识数据段的开始
- 数据部分 (Data)：数据包包含着若干编码了数据的数据 chirp



13

LoRa与ZigBee对比

协议	ZigBee	LoRa
芯片	CC2420 (TI)	SX127x (SemTech)
发射功率	0dBm (1mW)	20dBm (100mW)
传输距离	100 ~ 300m	最高3km
调制方式	DSSS	CSS
带宽	250kbps	0.3 ~ 22kbps
单个包长	128字节	256字节
MAC协议	无特定MAC协议，可实现ZigBee不同模式	LoRaWAN三种不同模式
接收敏感度	+3dB高于噪声平面	19.5dB低于噪声平面

15

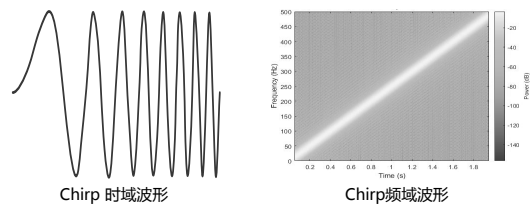
LoRa为什么能远距离

使用线性扩频CSS，频率充满整个带宽

抗干扰极强，对多径和多普勒效应的抵抗也更强

接收灵敏度高达 -148 dBm

以偏小的数据速率 (0.3-50kbps) 换取更高的通讯距离 (市内3km，郊区15km)



10

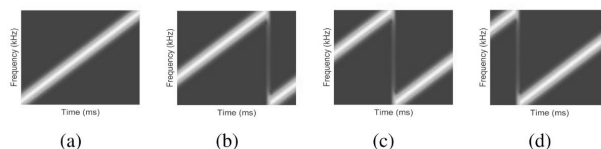
LoRa为什么能远距离

LoRa物理层信号调制策略

- LoRa规定了一个扩频因子SF，其定义为：

$$2^{SF} = T \times B$$

- 给定带宽B，SF越大chirp长度T越长，通讯距越远。一般来说每一个chirp可能的起始频率数目是 2^{SF}



12

LoRa协议的三种工作模式

Class A: 双向终端设备模式

- 节点只能在有数据上传时下载数据。可以减少大量能量开销

Class B: 有接收时隙的双向终端设备模式

- 节点可以在固定的时隙内下载数据

Class C: 最大化接收时隙的终端设备模式

- 节点有几乎连续的接收时隙

思考：三种工作模式各自优缺点是什么？

14

NB-IoT协议

NB-IoT支持蜂窝连接

• NB-IoT相比GSM

- 覆盖能力提升了20 ~ 30dB
- 支持每平方千米10万台设备连接
- 终端电池寿命长达5 ~ 10年
- 芯片成本低至1美元

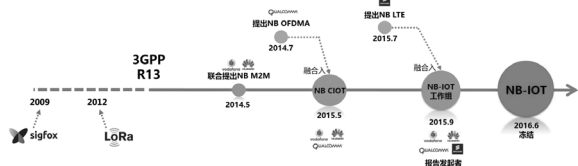


NB-IoT极大地延伸了蜂窝网络的应用边界，适应了物联网时代的连接需求

16

NB-IoT协议

- 最初以沃达丰和華為提出的NB M2M为基础。
- 在高通加入后，发展为NB-CIoT。
- 随后，NB-CIoT与爱立信的NB LTE合并，最终形成了NB-IoT



技术融合：继承融合多项技术与标准——NB M2M、NB OFDMA、NB CIoT、NB LTE

关键时间节点：2016年冻结核心协议标准（3GPP R13），第一批芯片同年年底投入商用

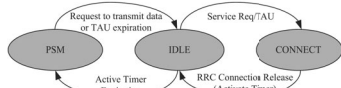
资本助推：设备商、运营商和芯片厂商大力推动，加速部署，后来居上

17

NB-IoT工作模式

沿用传统LTE休眠模式

- 当用户无数据传输或活动定时器超时，终端从CONNECT（连接态）切换到IDLE（空闲态）
- 终端在IDLE态时，射频模块不完全关闭，仍与MME保持连接进行移动支持



NB-IoT新增PSM (power saving mode) 模式

- 节点关闭所有射频模块，PSM模式下核心网无法与节点建立通信连接
- PSM期间，来自核心网的下行消息缓存在eNodeB，直至节点主动从PSM切换到IDLE然后到连接态
- PSM模式最长可持续310小时

19

NB-IoT协议优缺点

NB-IoT和LoRa的技术指标区别不大

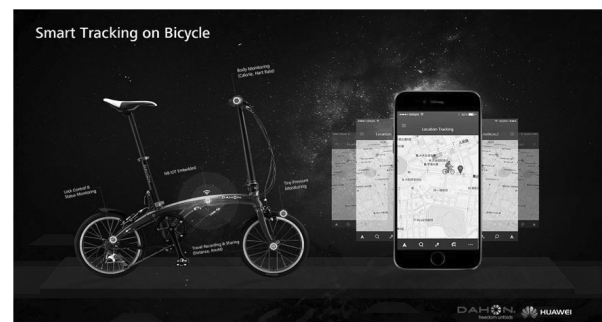
NB-IoT技术能够与现有的移动通信基站相结合，易部署于现有的无线基站上

NB-IoT目前得到了一级运营商（如沃达丰）以及设备制造商（如华为）的支持。这对于NB-IoT技术的推广和应用将起到至关重要的作用

目前市场上仍未有公开商用的NB-IoT芯片，其具体性能和在应用中可能存在的问题尚不可知

21

NB-IoT的应用



华为将联合自行车领域的合作伙伴，推出基于NB-IoT技术的智能自行车。该自行车将具备位置定位的防盗功能，以及其他的信息上报和跟踪功能

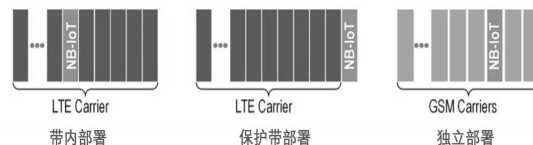
23

NB-IoT部署模式

基于LTE基站，通过协议栈升级使其支持与NB-IoT节点互相传输

- 与LTE设备使用频段部分重合——三种部署模式：

- 带内部署：在LTE频段内，使用空闲的LTE资源块
- 保护带部署：LTE频段边缘设置有保护频段，在该保护频段内分配NB-IoT资源块
- 独立部署：在LTE暂未使用的注册频段中为NB-IoT分配资源块

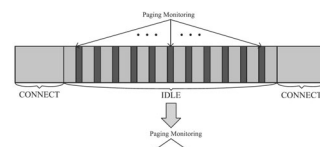


18

NB-IoT工作模式

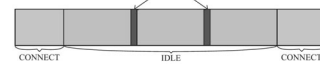
DRX (LTE中使用)

- 非持续接收：IDLE模式下使用，需要终端周期性地与核心网连接进行网络激活
- UE在预先调度好的时间片中接收指令或数据：需要终端与核心网精准同步



eDRX (NB-IoT中使用)

- IDLE模式下使用，在DRX基础上，延长节点两次接收窗口的间隔
- 最长窗口间隔从2.56s (DRX) 延长到2.92h (eDRX)



20

NB-IoT的应用



华为联合产业合作伙伴Firefly，为其提供NB-IoT技术支持，打造一款智能拉杆箱。该拉杆箱将具备智能追踪，超距告警，电子锁控制，电池监控等基于NB-IoT技术的应用

22

毫米波通信的兴起

什么是毫米波？

毫米波指的是频率在30 ~ 300GHz频段内的无线信号（相应的波长为1 ~ 10mm）。

无线接入技术的蓬勃发展造成了2.4GHz和5GHz频段的拥挤，为了缓解频谱资源的紧张，人们的目光开始转向更高频率的频段，其中最具有代表性的就是毫米波频段。

此外，半导体工业的发展推动毫米波频段，尤其是60GHz频段的射频收发器的成本大大降低，使大规模应用毫米波频段成为可能。



25

毫米波通信的优点

丰富的频谱资源

中国将59~64GHz划分为ISM频段，美国、日本分别将57~64GHz、59.4~62.9GHz划分为ISM频段，而欧洲更是划分了高达9GHz（57~66GHz）的ISM频段。

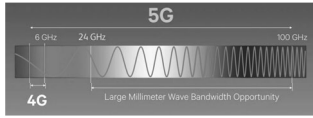
目前主要使用的802.11n技术，其有效带宽约为660MHz，远远少于60GHz毫米波无线通信技术。

高传输速率

IEEE 802.11ad技术可以支持高达8Gbps数据传输速率。

波长短

60GHz信号的波长为毫米级别，其元器件的尺寸很小，便于集成化，同时易于实现波束成型。



26

毫米波通信的优点

高方向性

- 60GHz通信采用波束成形（Beamforming）技术，将99.9%的波束集中在4.7度范围内
- 同时传输的信号在空间中重叠度小，不易产生干扰

安全性

- 毫米波在传播过程中的能量衰减远高于低频信号，在短距离通信的安全性能和抗干扰性能上存在优势
- 可将信号限制在有限区域内，物理隔离信号传播、保障安全性

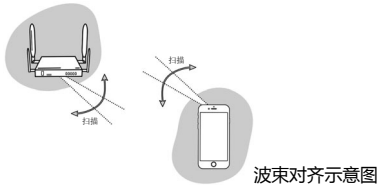


27

挑战：波束成形与波束对齐

为了抵御毫米波信号传播过程中的强度衰减及信号干扰，毫米波通信使用波束成形（Beamforming）技术将信号的能量聚集到一个比较窄的方向上，形成一个非常窄且能量非常集中的波束。

由于该技术形成的波束很窄，因此发射器和接收器之间要进行波束对齐（Beam Alignment）之后才能进行通信。



波束对齐示意图

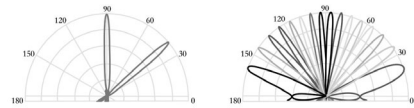
28

挑战：波束成形与波束对齐

当前用于波束对齐的方案需要发射器和接收器扫描整个空间，直至两者找到最佳对齐角度，整个过程会造成极大的时间开销。

Agile-Link提出了一种快速波束对齐的方法

通过移相器来创建多重波束，可以同时空间中的多个方向进行检测。使用了随机多次检测，令其检测方向能够覆盖到整个空间，最后通过多数投票的方法选出信号最强的方向。

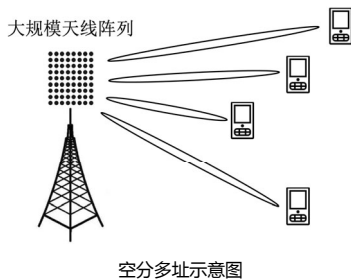


多重波束与随机化检测

29

挑战：空分多址技术

空分多址是指通过利用毫米波通信的高度定向性，通过使用不同的空间波束能够对来自不同方向的用户进行隔离，从而实现在空间域中对不同用户进行多路复用



空分多址示意图

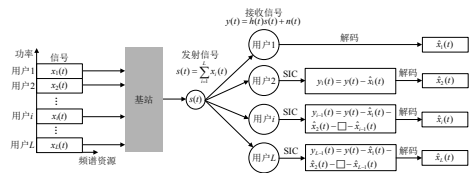
30

挑战：空分多址技术

挑战：当用户数量大于基站的射频链路数量时，如何为多个用户提供服务

解决思路：对处于同一个波束覆盖的一小片区域内的用户，使用非正交多址技术来提供服务

- 非正交多址在发射端不会对频谱资源进行分割，每个用户可以占用所有的时频资源，提高资源利用效率
- 在接收端，通过使用串行干扰消除等技术来实现对每个用户所需信息的解码



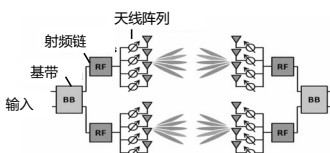
31

挑战：大规模MIMO

由于天线尺寸较小，毫米波通信基站可以支持上百个天线的天线阵列，能够实现大规模输入输出（Massive MIMO）技术，同时向更多用户发送数据，极大提高通信速率

挑战：获取准确的信道状态信息CSI

解决思路：利用深度学习来对大规模MIMO系统进行信道估计，将要估计的多天线信道矩阵看作二维图像，并使用图像处理中用于图像恢复的去噪卷积神经网络来对信道参数进行学习和估计



32

毫米波通信研究方向

毫米波天线设计

更高增益，更低成本的天线。

预编码技术

对发送的信号进行预先编码，使其在MIMO通信中与多用户更好地匹配。

标准化与大规模部署

为毫米波通信制定更完善的标准以及进行实际场景中的大规模部署。

毫米波感知

使用毫米波通信设备来实现物体的感知、成像、定位、追踪等功能。

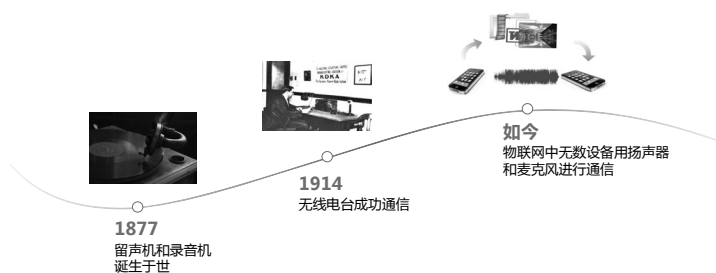
后续章节将向读者介绍毫米波感知技术的最新研究进展，进一步展示毫米波技术在物联网应用中的特点和优势。



33

声音通信

起源

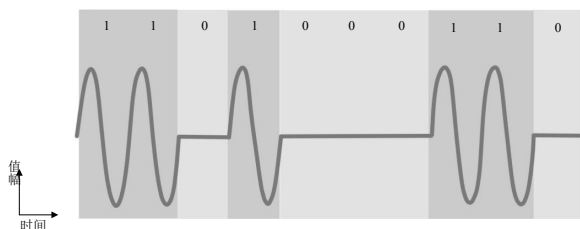


编码方式

幅移键控编码ASK

使用不同强度的信号代表不同的数据

开关键控使用振幅为0和振幅为1的信号分别代表“0”和“1”



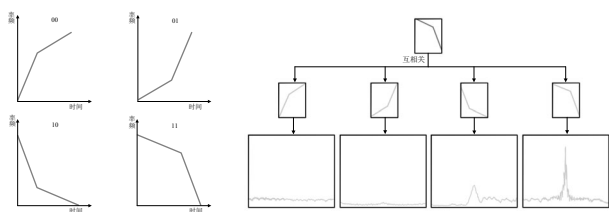
37

编码方式

基于扫频信号的声音通信

用4种不同走势的扫频信号代表00, 01, 10, 11

通过互相关的方式来判断收到的是哪一种扫频信号

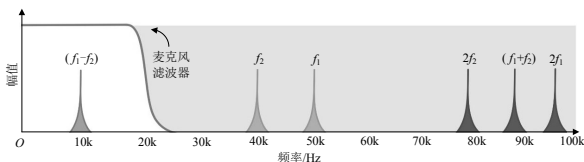


39

非线性效应

BackDoor

- 当输入信号是两个单一频率的信号时，即： $V_{in} = \sin(2\pi f_1 t) + \sin(2\pi f_2 t)$
- 输出信号的二次项则满足下面的公式，即： $V_{in}^2 = (\sin(2\pi f_1 t) + \sin(2\pi f_2 t))^2 = \cos(4\pi f_1 t) + \cos(4\pi f_2 t) + \cos(2\pi(f_1 + f_2)t) + \cos(2\pi(f_1 - f_2)t)$
- 用低通滤波器滤掉高频信号后，得到频率为 $f_1 - f_2$ 的信号



41

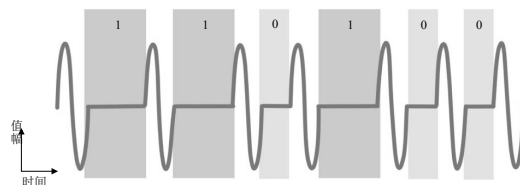
编码方式

脉冲间隔编码PIM

使用相邻脉冲之间的间隔长度来编码信息的方式

设置不同的间隔长度代表不同的数据。如长度为T的间隔代表“1”，长度为T/2的间隔代表“0”

间隔分得越细，编码能力越强。但解码难度越高



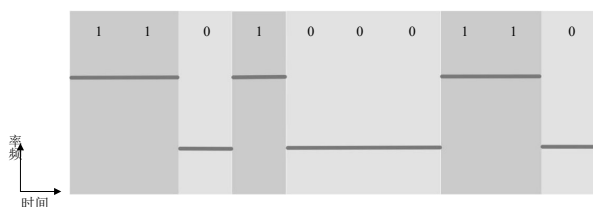
36

编码方式

频移键控编码FSK

利用不同的信号频率代表不同的数据

如下图用两种不同的频率分别代表“0”和“1”



38

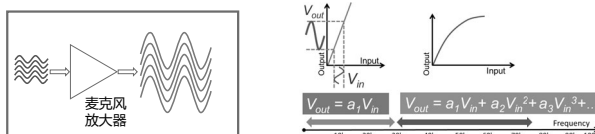
非线性效应

BackDoor

- 多数声音通信使用18~24kHz的超声信号。这些频段虽然对成年人影响不大，但对婴儿和宠物有较大干扰。
- 为减少干扰，BackDoor利用麦克风放大器的非线性效应实现了用40~50kHz超声信号向普通的麦克风传输信息，即：

$$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + a_4 V_{in}^4 + L$$

式中， V_{in} 为接收信号和 V_{out} 为记录下来的信号



40

可见光通信

什么是可见光通信？

可见光通信VLC指的是利用可见光频段（波长为400~700nm）来编码通信内容的光学无线通信系统。



常见形式

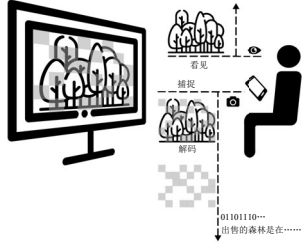
- 用LED光源或者显示屏等发光设备作为信号的发送端。
- 用光电二极管或相机等光信号接收设备作为信号接收端。
- 可通过开关键控来编码信息，即发光设备的“亮”和“暗”各代表一种数据状态。

43

显示屏-相机通信

原理

- 人眼的低频特性无法捕捉显示屏上以高频率闪烁的信号
- 显示屏以120Hz以上的刷新率持续输出不同亮度的可见光，作为可见光通信的发送端

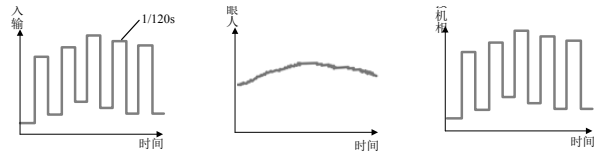


44

显示屏-相机通信

原理

- 假设显示屏上互补像素对（相邻两帧同一位置的像素点）的平均亮度为 V
- 显示屏将互补像素对的亮度设置为 $(V+V, V-V)$ 或 $(V-V, V+V)$ 两种不同的方式来编码“1”或“0”，从而达到发送数据的目的
- 画面的平均亮度没变，人眼只能感知到平均亮度。但相机较高的捕捉频率可以解码信息



45

显示屏-相机通信

最新进展

- ChromaCode：提出在均匀颜色空间对亮度进行改变，大大提升了用户观感体验。将有效数据传输率提升到120Kb/s，可以支持图片等传输形式
- AirCode：利用视觉里程计技术准确定位并追踪显示屏边框，降低误码率，将有效数据传输率提升到1Mb/s以上，使“视频中传视频”的场景成为可能



46

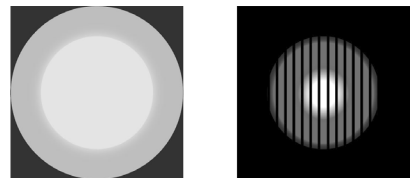
LED可见光通信

LED

利用LED灯快速的明暗变化来传输数据，在接收端使用光电二极管感知光强的变化。

由于相机的卷帘快门机制，照片中获得的是亮暗条纹相间分布的光源图像。

条纹代表不同时刻的明暗信息。宽度代表状态持续时间。接收端可以此解码。

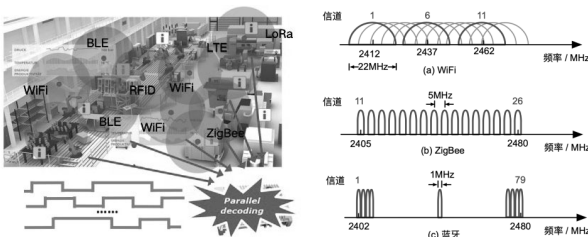


47

无线共存

无线共存问题

- 无线信道在共享频段上普遍重叠，导致信道竞争和信号冲突
- 不同的无线技术之间主动进行数据传输和融合协调是解决共存问题的突破口

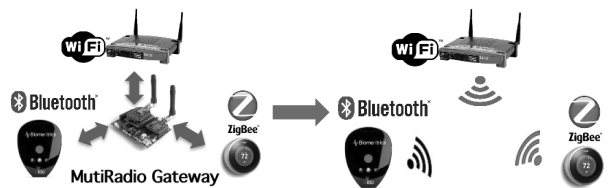


49

跨协议通信

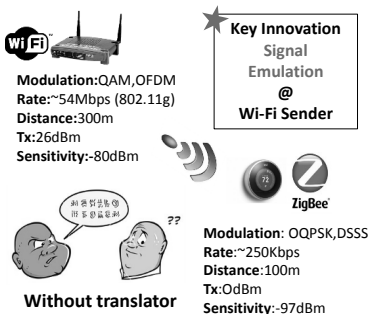
什么是跨协议通信

- 两个采用不同通信协议的无线设备（如WiFi和ZigBee）之间实现直接的数据传输和信息交换
- 应用在家居、工业、医疗等方面，实现更好的网络控制、干扰管理、交互操作和异构融合



50

技术挑战



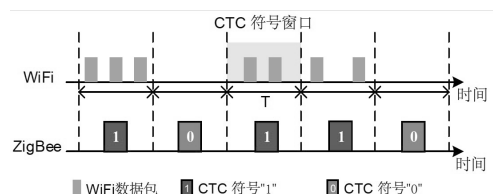
信息屏障
异质网元共存的“信息屏障”，不同无线技术的物理层采用不同的通信协议标准，这些标准是不兼容的，互相不认识
媒介缺失
异构网络协同的“媒介缺失”，不同无线技术的编码调制方式不同，相应的解调解码方式也不同，说话听不懂
管理失衡
共享信道资源的“管理失衡”，不同无线技术的带宽、速率、接收灵敏度、抗噪声干扰、抢占信道的能力是不同的，能力非对称

51

数据包级别的跨协议通信技术

数据包级别的跨协议通信

- 挖掘侧信道，利用数据包级别的特征实现异质设备之间的数据传输
- 特征类型：数据包的发送能量、长度信息、发送间隔、发送顺序
- 侧信道类型：接收信号强度（RSS）、信道状态信息（CSI）



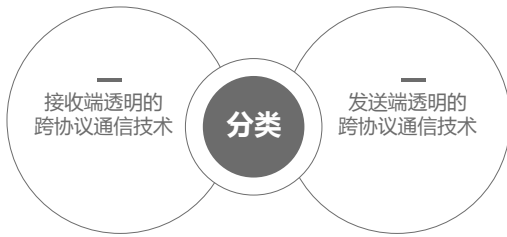
基于发送能量能量的数据包级别跨协议通信技术

52

物理层级别的跨协议通信技术

物理层级别的跨协议通信

发现不同调制解调技术间的潜在兼容性，实现物理层的信息传输。
提高跨协议通信的传输效率，实现Mb/s级别的数据率。



53

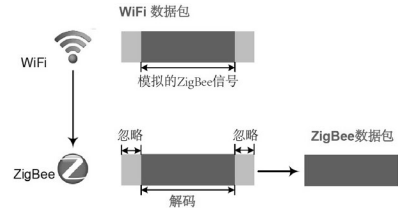
物理层级别的跨协议通信技术

接收端透明的跨协议通信技术

发送端通过改变数据包的内容来模拟接收信号的波形或相偏序列

接收端不需要任何修改就可以直接解码其他异构无线信号

从高端无线设备（如Wi-Fi）到低端无线设备（如ZigBee）的跨协议通信链路



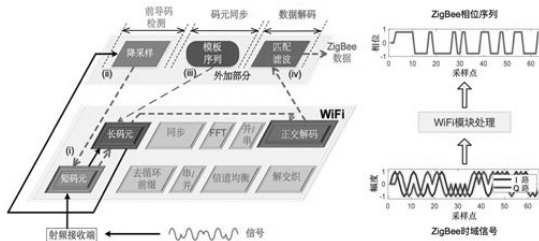
54

物理层级别的跨协议通信技术

发送端透明的跨协议通信技术

核心思想是交叉映射

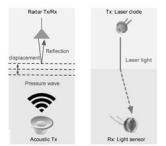
通过发送端信号和接收端解码出的信号之间的映射关系，实现跨协议信息的传输和解码



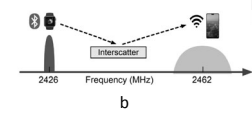
55

未来展望

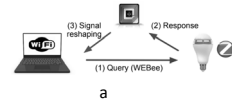
跨介质的通信传输



跨频率的通信传输



跨网络的通信传输



56

本章小结

内容回顾

本章我们详细介绍了低功耗广域网、毫米波通信、声音通信、可见光通信以及跨协议通信等新兴通信技术的方法 and 特点。

重点掌握

- 掌握各通信技术所涉及的原理和方法。
- 了解各通信技术分别所适应的应用场景。
- 理解各通信技术之间的优势缺点以及相应原因。

57

内容回顾

前一章

介绍了物联网中的新兴通信技术，包括低功耗广域网、毫米波通信、声音通信、可见光通信以及跨协议通信的方法和特点



2

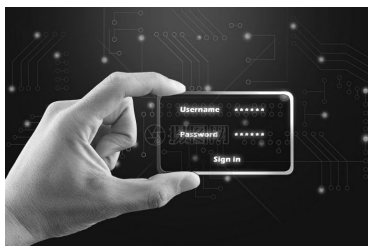
物联网中的密码学概述

密码技术功能

- 提供机密性、完整性、真实性、不可否认性的保障
- 密码学是确保数据安全与隐私的重要工具

密码学算法

- 加解密算法：机密性
- 摘要算法：完整性
- 消息认证码：真实性
- 数字签名：不可否认性
- 随机数生成算法



4

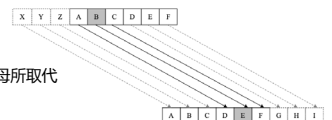
加解密算法

秦兵书《六韬》

太公曰：“主与将有阴符，凡八等：有大胜克敌之符，长一尺；破军擒将之符，长九寸；降城得邑之符，长八寸；却敌报远之符，长七寸；警众坚守之符，长六寸；请粮益兵之符，长五寸；败军亡将之符，长四寸；失利亡士之符，长三寸。诸奉使符，稽留者，若符事泄，闻者告者皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。故虽圣智，莫之能识。”

凯撒密码

- 相传由古罗马帝国的凯撒皇帝发明
- 做法：每个字母被往后位移 3 个字母所取代



现代密码学

- 对称加密
- 非对称加密(也称为公钥加密)

5

加解密算法

常见对称加密算法

DES(data encryption standard , 数据加密标准)

- 将固定长度的明文通过一系列复杂的代换操作变成同样长度的密文的算法

AES(advanced encryption standard , 高级加密标准)

- 基于代换操作
- 根据密钥长度不同, 代换的轮数不同
- 比DES要小, 速度更快



SM1、SM4 和 SM7

- SM4算法密钥长度为128位, 加密采用32轮迭代完成, 是我国无线局域网标准WAPI中所采用的分组密码标准
- SM1、SM7算法不公开, 需要使用专用芯片

Salsa20、ChaCha20

- 流加密算法
- 对数据流加密, 加密和解密双方使用相同伪随机加密数据流作为密钥, 明文数据每次与密钥数据流顺次对应加密, 得到密文数据流

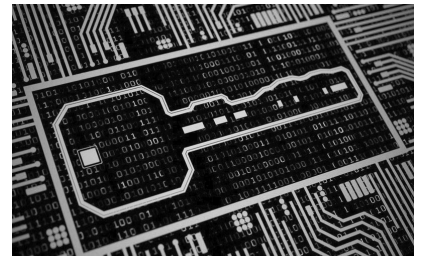
6

加解密算法

工作模式(mode of operation)

简介: 分组加密算法

的加、解密操作单位都是块, 通常较小(如 DES 的块大小为 8B), 在实践中, 如果加密多于一块的数据, 就需要工作模式的支持



常用的工作模式

- 电子密码本模式
- 分组链接模式
- 计数器模式

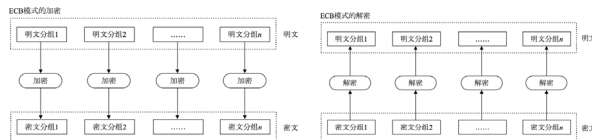
7

加解密算法

电子密码本(electronic codeBook , ECB)模式

加密的消息按照加密算法的块大小分为若干块, 每个块独立加密

缺点: 相同的明文块会被加密成相同的密文块, 加密数据容易被分析, 因此并不常用



8

加解密算法

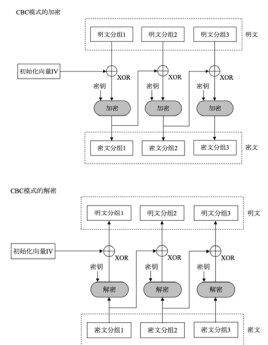
分组链接模式

先加密的块会影响后加密的块

同样的明文块加密后, 不会得到相同的结果

分类

- 密文分组链接 (cipher-block chaining, CBC) 模式: 除首块外的每个明文块先与前一个密文块进行异或后再进行加密, 而第一个块需要与初始化向量 (initialization vector, IV) 异或
- 密文反馈 (cipher feedBack, CFB) 模式
- 输出反馈 (output feedback, OFB) 模式



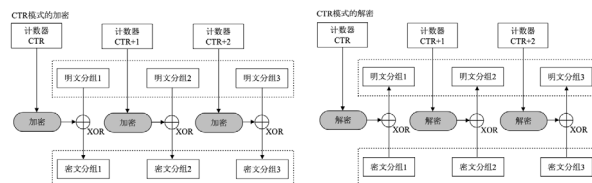
9

加解密算法

计数器(counter , CTR)模式

使用递增的计数器, 通过对计数器的值加密产生连续的密钥流, 与明文异或得到密文分组

在加密和解密的过程都可以并行处理



10

加解密算法

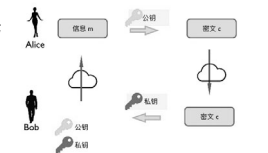
非对称加密算法(也叫公钥加密算法)

需要两个密钥

- 一个是公开密钥, 通常用作加密和验证签名; 另一个是私有密钥, 通常用作解密和签名

常见算法

- RSA 算法和椭圆曲线算法



RSA 算法

依赖于大整数不易分解质因数的数论难题

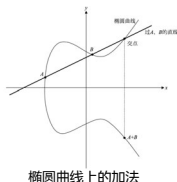
记 RSA 算法中, 用户的公钥和私钥分别为 K^+ 和 K^- , 相应的操作为函数 $K^+(\cdot)$ 和 $K^-(\cdot)$, $K^+(K^-(m))=m=K^-(K^+(m))$

11

加解密算法

椭圆曲线(elliptic curve)算法

- 相比于 RSA, 密钥长度较短。
- 长度为 256 位的椭圆曲线密钥, 安全性与长度为 3072 位的 RSA 密钥相当。
- 可以表示(或经过变换)为下面的方程, 即 $y^2 + axy + by = cx^3 + dx^2 + ex + f$
- 考虑一组特殊的曲线: $y^2 = x^3 + ax + b$, 在曲线上定义两点 A 和 B 的加法为: 两点连线(两点重合时为切线)与椭圆曲线交点关于 x 轴的对称点。
- 取一个随机的大数 k 作为私钥, 计算曲线上一点 G 的 k 倍点 kG (即 k 个 G 相加)作为公钥。



椭圆曲线上的加法

12

摘要算法

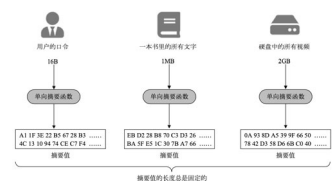
也叫散列算法或哈希算法, 是一种从任意数据创建出小数据的算法

特点

- 单向的, 无法从摘要中恢复出任何消息
- 根据任意长度的输入都可计算出固定长度的摘要值
- 不同的输入通常产生不同的输出, 相同的输入一定产生相同的输出
- 不同的输入产生相同输出(称为“碰撞”)的概率极低

用途

- 保护用户口令: 数据库里存储用户的口令(往往还需一些额外的数据处理)的摘要值而非原始值
- 数据校验: 验证文件的完整性
- 作为消息验证码或数字签名的一部分



13

摘要算法

常用的摘要算法：

MD5

曾经非常常用，输出长度为 128 位

SHA-1/2/3

由于 MD5 存在碰撞攻击的缺陷，美国国家标准技术研究院制定了 SHA-1 算法作为 MD5 的继任者，但 SHA-1 也被发现存在安全问题。截至目前，还未出现对 SHA-2/3 系列算法的有效攻击

SM3

我国国家密码管理局于 2010 年发布的摘要算法，目前已被收录于国际标准 ISO/IEC 10118-3:2018 中



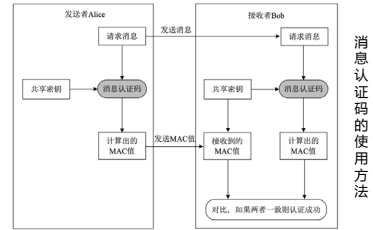
14

消息认证码

既确认消息完整性，又对消息进行认证的算法

常用的消息认证码算法

- 基于摘要算法的 HMAC 算法
- 基于分组密码的 CBC-MAC 算法
- 基于流密码的 MAC 算法



15

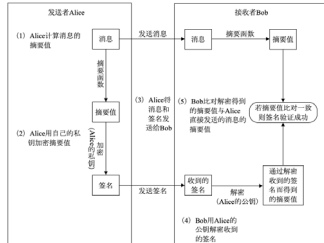
数字签名

使用非对称密钥的方法，来区分生成消息签名和验证消息签名两个行为

必须使用私钥才能签名，可以同时做到识别篡改和防止抵赖

常用的数字签名算法

- RSA 算法
- DSA 算法
- ECDSA 算法



16

随机数生成算法

分类

弱伪随机数

- 使用伪随机数生成器生成的随机数
- 只具备随机性，即满足一定的概率分布

强伪随机数

- 使用密码学伪随机数生成的随机数
- 除了具备随机性外，还具备不可预测性，即攻击者知道过去生成的伪随机数也无法预测下一个伪随机数

真随机数

- 使用真随机数生成器生成的随机数
- 除了具备上述的随机性和不可预测性外，还具备不可重现性，即无法重复随机数的生成过程



17

物联网的安全现状

对物联网的常见攻击方式

拒绝服务攻击(denial-of-service, DoS)

- 目标：让被攻击的机器或网络资源无法向目标用户提供服务
- 分布式拒绝服务(distributed denial-of-service)DDoS

物理攻击

- 目的：破坏硬件设备

隐私攻击

- 窃听和被动监测



物联网新的安全需求与挑战

身份验证和管理：安全地管理用户和设备对信息的访问权限

访问控制：人或物在通过身份验证后，有没有访问特定资源的权限

信任机制：参与通信的实体之间的信任和对物联网系统的信任

19

低功耗蓝牙安全

低功耗蓝牙 BLE

一种低功耗、低成本的通信技术，由蓝牙技术联盟设计并制定规范，广泛应用于个人穿戴设备、智能家居和智能医疗设备中，如手环、智能手表、智能锁等

在实验室场景下，通信范围可达到 250m，同时保持 100Kb/s 的数据传输速率

参与 BLE 通信的两个设备分别叫做中心设备和外围设备

中心设备

- 请求数据的一方，功耗相对较高
- 多为个人计算机、智能手机等拥有更多计算和内存资源的设备

外围设备

- 提供数据和相关功能的设备，功耗通常较低
- 多为各种手环、智能手表等计算和内存资源较少的设备

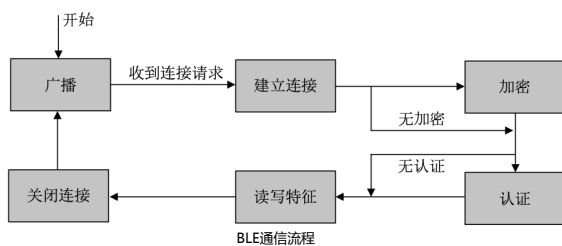


21

低功耗蓝牙安全

中心设备与外围设备通信的主要过程

- 外围设备发送广播数据(advertising data)
- 中心设备和外围设备建立连接
- 完成要求的加密和认证过程，读写数据
- 关闭连接，外围设备重新进入广播状态



22

低功耗蓝牙安全

协议层加密方法目的

- 对敏感信息进行保护，防止第三方的窃听

配对

- 定义：加密密钥的协商生成过程。
- 一般仅发生在两个设备还未共享过加密密钥的情形
- 可以由中心设备或者外围设备的任意一方发起，交换配对参数后计算出加密密钥

根据中心和外围设备的输入输出能力协商加密密钥的方式

- Just Works
- Numeric Comparison
- Passkey Entry



23

低功耗蓝牙安全

具体过程

- 双方共享加密密钥后，就可以对通信连接进行加密以防止窃听
- 一方发送加密请求(LL_ENC_REQ)包
- 另一方回复 LL_ENC_RSP 包接受加密请求，或回复 LL_REJECT_IND 拒绝加密请求，中断加密流程
- 加密过程可以在任何需要的时间由任一方发起或中断

安全挑战

- 协议层的身份欺骗
- 构造虚假的数据包来伪造自身的能力
- 中心设备长时间未收到同意加密请求的 LL_ENC_RSP 数据包，会中断加密请求
- 设备再次重新连接时，身份验证是可选的而非强制的



24

近场通信安全

NFC Forum 组织3 种通信模式

- 读写器模式、卡模拟模式和点对点模式

特点

- 工作距离短、通信速度快、标签或卡无须电源

应用场景

- 非接触式支付、门禁、票务等智慧城市 和家居场景，电子钥匙、个性化驾驶等智能驾驶场景，以及设备认证、固件升级等智能工业场景



NFC 标签根据物理层和数据的组织方式分为 5 类 (Type1-5)

- 在我国应用最广泛的是 Type 2 和 Type 4
- Type 2 普遍用于非金融领域，典型的应用场景是一般的身份验证
- Type 4 适用于更复杂的数据交换，特别是各种支付(如公共交通、金融)和密钥交换认证等应用

25

近场通信安全

NFC 技术的安全性

- 针对智能卡(或标签)的攻击
- 针对银行卡的攻击：利用特殊的装置窃取信用卡和 POS 机之间的非接触式交易，提取有用信息
- 中继攻击：利用一些设备做数据的转发，将 NFC 的通信距离延长



26

LoRaWAN安全

LoRaWAN

由节点、网关、网络服务器和应用服务器(入网服务器)构成

协议 1.1 版中规定

- 使用对称加密算法(AES-128) 对节点和服务器发送的数据载荷
- 使用 MAC 命令进行加密和解密

激活

一个节点在加入网络时，需要进行设置与激活来获取相应的密钥，从而能够与服务器进行通信

激活的方式

- 手动激活(activation by personalization)
- 无线配对激活(over-the-air activation)



27

LoRaWAN安全

手动激活

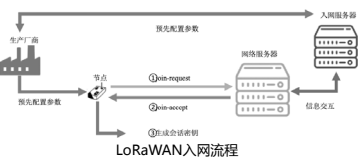
所有的密钥和相关信息通过数据线直接烧录到节点中安全的存储单元内

无线配对激活

节点通过发送加入请求 (join-request) 命令申请加入网络，入网服务器回复允许入网 (join-accept) 命令，将一些加密参数发送给节点，用于生成节点与服务通信所需的对称密钥

对LoRaWAN的攻击

- 拥塞攻击
- 重放攻击
- 信标同步攻击
- 网络流量分析
- 中间人攻击



28

物联网攻击检测

蜜罐系统

一种特殊的系统，在被全面监控的情况下接入网络，本身不提供任何有用的功能，就是等待着被入侵和攻击

正常情况下，任何人或程序都不会访问蜜罐

分类

- 高交互式蜜罐(high-interaction honeypot)
- 低交互式蜜罐(low-interaction honeypot)

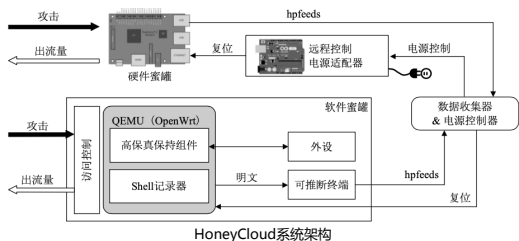
比较项	低交互式蜜罐	高交互式蜜罐
操作系统	不直接依赖	高度依赖
被攻击风险	低	高
维护代价	低	高
保真度	低，只能捕获已知类型攻击	高，可以捕获各种攻击

29

物联网攻击检测

蜜罐系统的搭建

- 传统蜜罐方案不易于直接迁移到物联网环境中
- 硬件蜜罐（单板机）：具有最高的保真度，可以直接捕获针对设备的攻击和威胁，因而是了解针对物联网设备网络攻击的最直接、最有效的工具
- 公有云蜜罐（HoneyCloud）：降低成本，提高可靠性，并且能方便地在全球部署

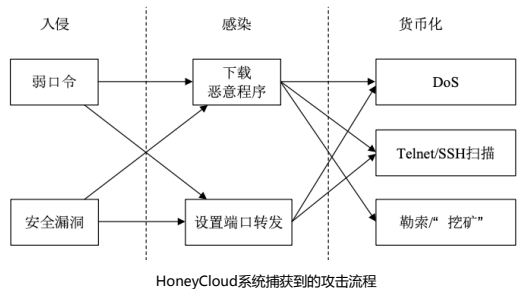


30

物联网攻击检测

攻击步骤

- 常规：入侵、感染、货币化
- 无文件攻击：在感染和货币化两个步骤的操作与常规攻击有所不同



31

总结

由于设备性能有限，目前还难以在物联网设备内部署较高级的安全防护产品(如防火墙、杀毒软件及入侵检测系统等)

这给黑客以及网络黑色产业带来了可乘之机，网络攻击也逐渐从传统的信息空间向物理空间渗透，攻击不仅仅是破坏信息系统，更有可能造成物理世界的破坏

随着网络攻击向物理世界的不断渗透，物联网安全问题将尤为突出

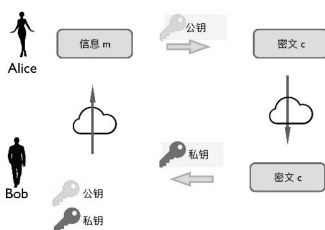
设备安全、系统安全及法律保障等多层次物联网安全，将是全方位构建更安全可信的物联网的关键手段

33

内容回顾

前一章

介绍了物联网安全的相关内容。首先介绍了网络安全中的基本安全目标。之后讲物联网的密码学基础，介绍了常用的五类物联网中的密码学算法。然后介绍了物联网的安全现状与特点，并介绍了一些安全案例，再次强调物联网安全的重要性



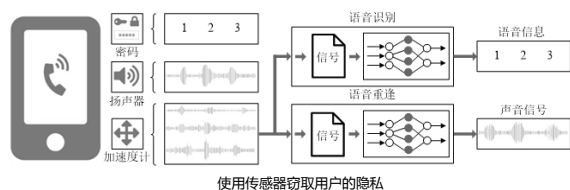
2

传感器的分类

隐私不敏感的传感器

- 加速度、陀螺仪
- 看似提供信息不多，容易对其放松警惕，但经过特殊设计，也能窃取到很多隐私信息

典型的隐私泄露案例：密码盗窃 轨迹泄露 语音窃听



使用传感器窃取用户的隐私

5

基于流量的隐私泄露

智能家居

- 使用WiFi接入互联网
- 嗅探网络空间中物联网常用协议的信号，推测智能家居的运转情况
- 捕捉空间中智能家具信号，通过神经网络处理信号，推断各设备的工作情况，推测用户的活动情况



8

本章小结

内容回顾

本章介绍了物联网的安全问题，包括物联网中使用的密码学基础概念与算法，不同类型物联网的安全现状，以及常见的物联网的攻击与防御方法

重点掌握

- 掌握常见的密码学基础概念，了解经典的密码学算法
- 了解物联网安全的现状
- 掌握常见的物联网攻击与防御方法与特点

34

传感器的分类

隐私敏感的传感器

- 摄像头、麦克风等
- 能轻易地窃取人们的隐私，被严加看护



Google眼镜



Hololens



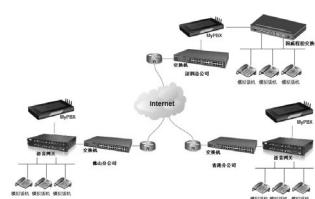
小米手环

4

基于流量的隐私泄露



网络加密语音通话VoIP并非牢不可破



7

物联网隐私安全防护手段

身份匿名

将数据中的真实身份信息替换为一个匿名的代号，隐藏位置信息中的“身份”

服务商能利用位置信息提供服务，但无法推断用户身份

常用技术

- K匿名：引入可信中介，让用户发布的信息和另外k-1个用户的信息变得不可分辨



10

保护位置隐私的手段

数据混淆

基本思想

- 通过对数据进行混淆，避免攻击者得知用户的精确信息

三种方法（以位置隐私为例）

- 模糊范围：降低位置信息的精度，从精确位置到区域
- 声东击西：偏离精确位置
- 含糊其辞：引入模糊语义词汇，例如“附近”



11

本章小结

内容回顾

本章介绍了物联网中特有的感知隐私与位置隐私问题

重点掌握

- 了解传感器隐私泄露的安全隐患
- 掌握基于流量的隐私泄露
- 掌握几种保护位置隐私的手段

13

工业革命发展历程

人类社会在过去200多年中高速发展

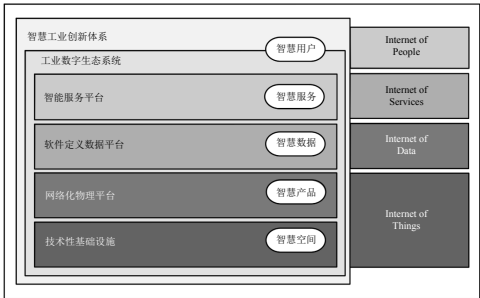
- 珍妮纺织机等工业机器的出现标志着第一次工业革命的诞生
- 以电力驱动的大规模生产的出现标志着第二次工业革命的开始
- 第三次工业革命依托于电子信息技术的进步
- 再到近10年，以物联网、信息物理系统等技术理念为核心的新一轮信息科学技术变革纷至沓来...



4

智慧工业—创新体系下的深层含义

创新型工业数字生态系统



智慧工业创新体系下的深层含义

6

保护位置隐私的手段

从感知数据的特点出发

通过主动检测手段找出或干扰攻击者预先放置的物理嗅探设备或软件

- 摄像头：频闪灯光
- 网络摄像头：分析网络流量
- 无线嗅探装置：主动发射数据



12

承前启后

前一章

介绍了我们智慧供应链，智慧供应链中的物联网技术及其具体应用

本章我们主要关注

智慧工业与其核心要素工业数据。明白智慧工业是如何借助物联网“感、联、知、控”四层体系架构中的关键技术的

2

智慧工业的诞生

“第四次工业革命”

- 21世纪初国际金融危机后，各大强国与企业意识到以工业为主体的实体经济的战略意义
- 人们试图借助信息科学技术来寻找新的原动力。当工业系统与信息系统深度融合的时候，“第四次工业革命”悄然而至



5

智慧工业—创新体系下的深层含义

网络连接技术

- 智慧工业互联互通的支撑。包含有线连接和无线连接两大类
- 有线连接依赖于同轴电缆、双绞线或光纤等线缆基础设施，在传输速率、吞吐量及抗干扰性上有较大优势
- 无线技术具有建设维护成本低、部署灵活等优点

数据

- 智慧工业的核心要素。工业数据测点众多、种类繁多，需恰当的数据存储技术，如清华大学研究团队推出的Apache IoTDB
- 数据计算也是智慧工业的重要一环

7

智慧工业—创新体系下的深层含义

平台集成技术

- 是工业全要素链接的枢纽与工业资源配置的核心，也是智慧工业落地实施与生态建设的关键载体
- 包含设备注册、接入管理、运行监控、数据可视化及数据远端推送等
- 2021年全球工业互联网平台厂商已经超过了1000家。按照企业性质，可分为设备商、运营商与云服务商这三大类别

信息安全技术

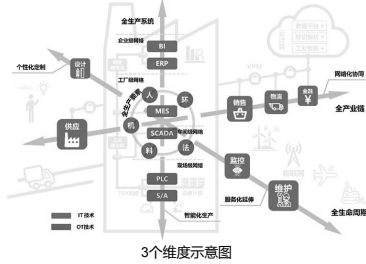
- 智慧工业发展的有力保障
- 保障工业生产环节的可靠性、隐私性、可用性及安全性等

8

智慧工业的特点

互联

- 最重要的特点就是互联，可从“1个趋势、3个维度”来理解
- 1个趋势就是互联——全生产要素的互联互通
- 3个维度是指“全生产系统、全产业链、全生命周期”



10

智慧工业的特点

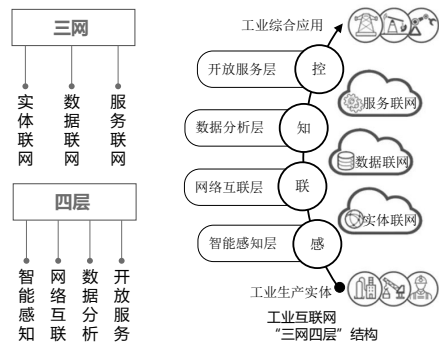
互联

全生产系统互联	全产业链互联	全生命周期互联
将企业内的商业智能、资源计划、制造执行系统、数据采集与监控系统等全生产系统连接，使信息技术与生产技术深度融合	产业链各环节的企业，包括供应商、制造商、销售商和金融机构等，协同优化，形成合力	使产品永远处于“在线”状态，从最初的设计、制造阶段，用户就可以参与其中，实现产品的个性化定制

11

智慧工业的特点

从技术角度来解释工业互联网

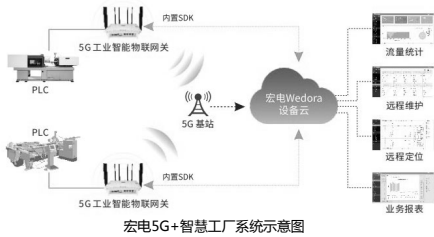


12

5G+智慧工业

基于5G通信的智慧工业

- 5G通信具备增强移动宽带、超高可靠低时延通信和海量机器类通信三大技术特性。能应对智慧工业中海量工业设备与传感器的连接问题
- 5G+移动边缘计算将计算逻辑下沉，能够有效降低上层应用处理时延
- 5G专网基础设施建设为数据打通、平台集成与信息安全等提供了核心载体

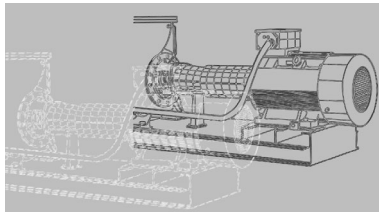


14

西门子数字孪生系统—PlantSight

数字孪生

- 2011年美国空军研究实验室于在一次公开演讲中正式提出
- 数字孪生是指以数字化方式为物理对象创建的虚拟模型，它能够反映物理对象的全生命周期
- 通过数字孪生完成对物理对象状态的监测、仿真与预测，从而获得对物理对象进行控制和改善的能力



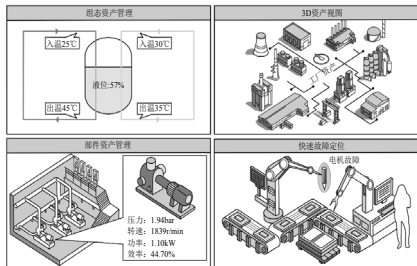
智慧工业中泵机系统的数字孪生

15

西门子数字孪生系统—PlantSight

PlantSight

- 2018年10月，西门子与美国建筑工程软件行业龙头本特利系统公司联合推出了智慧工厂数字孪生系统



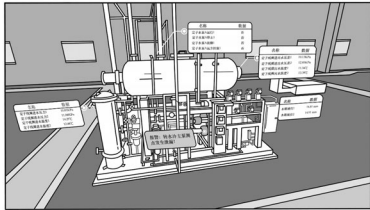
西门子公司PlantSight 数字孪生系统功能介绍

16

调相机无人值守监测和诊断系统

Pavatar

- 国家电网公司大力推动构建全球能源互联网。特高压换流站是其中一个非常重要的基础设施，相当于各个片区的核心路由
- 清华大学研究团队研发调相机无人值守监测和诊断系统Pavatar
- Pavatar系统借助物联网等技术，为调相机运维提供信息支撑和辅助决策，用以维持电网电压水平并改善系统供电质量



物联网数据实时3D可视化

17

油田智慧运营平台VGIS

VGIS

- 马基努油田是世上储量最丰富的油田之一，储量约为380亿桶。但不断变化的现场给提高效率和降低风险带来了巨大的挑战
- VGIS可视化地理信息系统支持协同工作和智能决策
- VGIS平台利用地理信息技术，构建了马基努油田的3D电子地图
- VGIS对数据进行组织，构建了统一的油田时空数据模型
- VGIS提供BI和数字化管理座舱等多种管理视图



VGIS 数字化管理座舱

发展与展望

智慧工业涵盖的内容很丰富

- 从德国的工业4.0到美国的工业互联网联盟，从石油钢铁到物流快递，从卡斯树根到华为阿里，从PLC到Cloud
- 工业互联网产业联盟发布的工业互联网垂直行业应用案例中，包括制造与工艺管理等六大应用场景，涉及十几个行业领域

核心趋势是生产全要素之间更广泛的互联互通

在全生产系统、全产业链、全生命周期3个维度上展开

展望

除了工业领域的数字化转型将可预见地带来生产方式的变革外，农业、经济等领域的数字化转型也将会给所在行业带来翻天覆地的变化，实现真正的万物互联，引领社会进入数字化经济时代

油田智慧运营平台VGIS

VGIS

- 还引入了虚拟现实和增强现实技术，结合手机等边缘设备，将油田的统一时空数据模型投射在真实环境当中
- 实现了基于虚拟现实技术的多人异地协作、教学培训和安全模拟，基于增强现实技术的现场巡检等功能



基于 VGIS 系统的油田现场 AR巡检

本章小结

内容回顾

本章我们主要了解智慧工业的诞生历程和深层含义。重点介绍了智慧工业互联的特点，并描述了如5G+智慧工业和西门子数字孪生系统等典型的智慧工业案例

重点掌握

- 了解智慧工业的诞生历程和深层含义
- 从1个趋势、3个维度理解智慧工业互联的特点
- 掌握典型的智慧工业案例，如5G+智慧工业等