+

第七章 物联网安全技术

第七章 物联网安全技术

- 随着人工智能、大数据、云计算等技术的不断突破，特别是5G技术的商业推广实现，安全物联网在自然资源、交通、住建、水利、能源、文旅古建等领域的价值越来越得到政府和公众的认可。
- 安全物联网采用“感、传、知、用”等物联网技术手段，综合利用无线传感、云计算、大数据等技术，通过互联网、无线通信网、专网等通信网络，形成多重分级预警。

第七章 物联网安全技术

物联网是通过射频识别(RFID)装置、红外感应器、全球定位系统、激光扫描器、传感器节点等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理等功能的一种网络。

物联网的核心是完成物体信息的可感、可知、可传和可控。

•

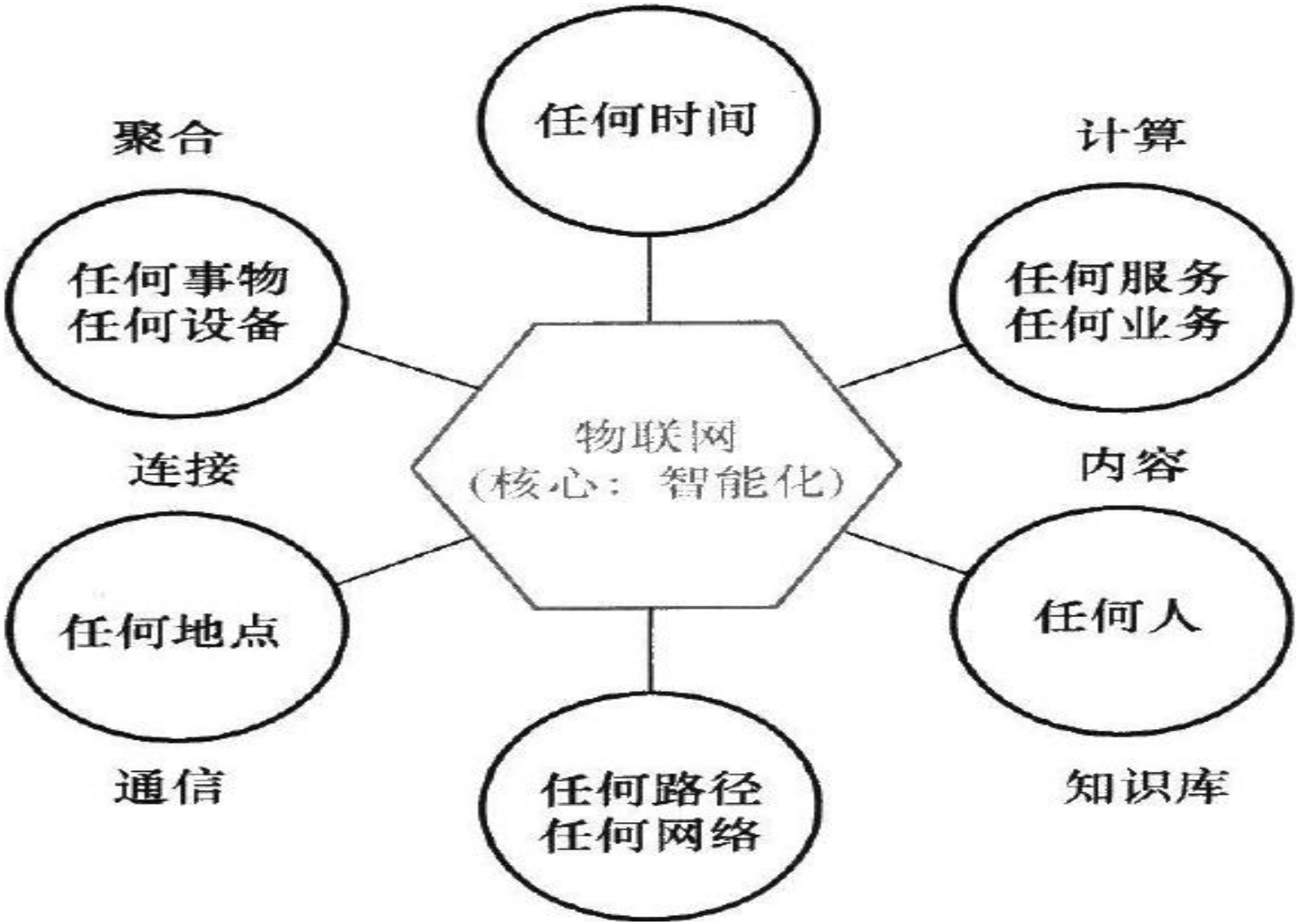
物联网有五个基本特征

- **1. 全面感知：**
- 即利用条形码、射频识别、传感器等各种可用的感知手段，实现对物品自身或环境状态信息的全面实时采集；
- **2. 无缝互联：**
- 即通过各种信息通信技术和网络技术的融合，实现异构网络的无缝连接与互通；
- **3. 可靠传递：**
- 即通过现有的互联网、广播电视网、通信网等网络设施和通信技术，基于可信的数据传输机制或冗余的网络通信链路等实现数据的可靠传输；

第五章 物联网安全技术

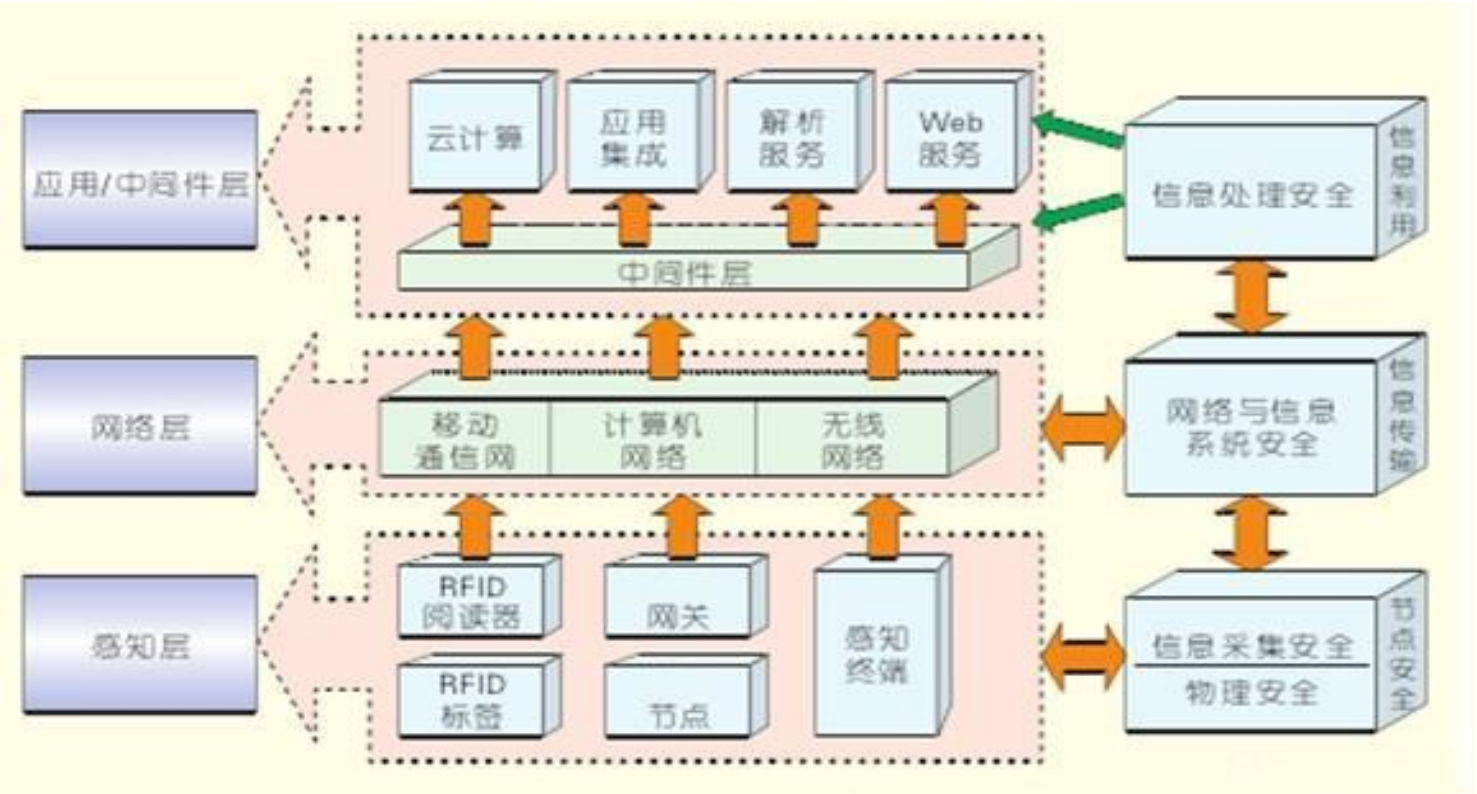
- **4. 智能处理：**
- 利用云计算、模糊识别、人工智能(Artificial Intelligence，AI)、神经网络、数据挖掘等智能计算技术对海量的数据和信息进行分析和处理，以便按需、自动地获取有用信息并对其进行利用，表现出高度的智能化；
- **5. 协同互动：**
- 嵌入传感器和微处理器的物品越来越具有智能性，能够协同获取和处理感知信息，为高效管理和控制提供决策支持。

第五章 物联网安全技术


任何时间
聚合
计算
任何事物
任何设备
任何服务
任何业务
物联网
(核心：智能化)
连接
内容
任何地点
任何人
通信
知识库
任何路径
任何网络

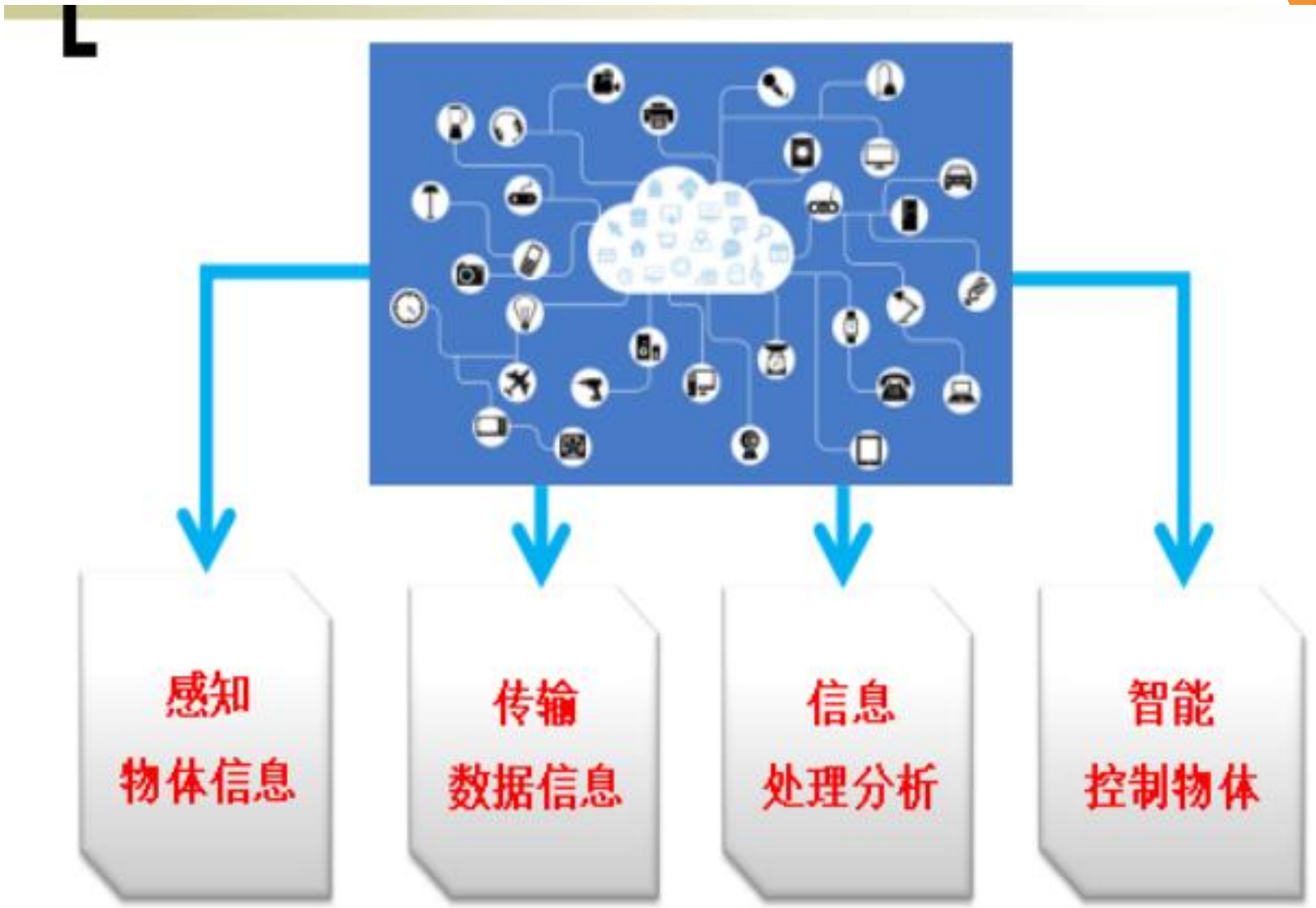
第五章 物联网安全技术

从信息与网络安全的角度来看，物联网作为一个多网的异构融合网络，不仅存在与传感器网络、移动通信网络和因特网同样的安全问题，同时还有其特殊性。



第五章 物联网安全技术

- 物联网安全架构：
-



物联网面临的安全问题

- 作为“互联网+”的典型代表，物联网基于互联网发展而来。物联网尽管超越了传统互联网，但并未脱离互联网，因此，物联网所面临的安全问题既有传统的网络安全威胁，又有不同于互联网的新威胁。

➢ 感知层威胁

➢ 网络层威胁

➢ 应用层威胁

物联网感知层安全威胁

任务	全面感知外界信息	
典型设备	RFID、传感器、图像捕捉装置、位置感知器、激光扫描仪	
安全挑战	感知节点所感知的信息被非法获取	感知节点所感知的信息不采取防护措施或防护强度不够，则很可能被第三方非法获取信息，导致大量的信息被公开，可能引起严重后果
	关键节点被非法控制	一个关键节点实际被非法控制的可能性很小，因为需要掌握该节点的密钥，但如果攻击者掌握了一个关键节点和其他节点的共享密钥，就可以控制该关键节点；如果不知道该共享密钥，则只能组织部分或全部信息的发送
	普通节点被非法控制	该情况较为普遍，攻击者可以获取关键节点与这些普通节点交互的信息，还可以传输一些错误数据
	普通节点被非法捕获	该攻击更为常见，攻击者不需要解析他们的预置密钥或通信密钥，只需要鉴别节点种类
	节点受到来自于网络的DOS攻击	DOS攻击即拒绝服务攻击，由于感知层最终要接入其他外在网络，且感知节点通常计算和通信能力有限，所有易受DOS攻击
	接入到物联网的超大感知节点的标志、识别、认证和控制问题	感知层接入互联网或其他类型网络所带来的问题不仅仅是感知层如何对抗外来攻击的问题，更重要的是如何与外部设备相互认证的问题；对外部互联网来说，如何区分数字庞大的不同感知系统或者网络数量，并有效识别他们，是安全机制能够建立的前提

物联网网络层安全威胁

任务	把感知层收集到的信息安全可靠地传输到应用层，然后根据不同的应用需求进行信息处理	
基础设施	互联网、移动网及专业网（如国家电力专用网、广播电视网）等	
安全挑战	非法接入	将导致网络层负担加重或者传输错误信息
	DOS攻击、DDOS攻击	物联网网络层的核心载体是互联网，而互联网遇到的DOS和DDOS攻击仍存在，因此需要更好的防范措施和灾难恢复机制
	假冒攻击、中间人攻击	在异构网络的网络认证方面，难免存在中间人和其他类型攻击
	跨异构网络的网络攻击	在网络层，异构网络的信息交换将成为安全性的脆弱点
	信息窃取和篡改	信息在网络上传输时，很可能被攻击者非法获取到相关信息，甚至篡改信息，所以必须采取保密措施进行加密保护

物联网应用层安全威胁

特点	智能（使处理过程方便迅速）	
缺点	智能仅限于按照一定规则进行过滤和判断，攻击者很容易避开这些规则	
安全挑战	来自于超大量终端的天量数据的识别和处理	当不同性质的数据通过一个处理平台处理时，该平台需要多个功能各异的处理平台协同处理；但首先应该知道将哪些数据分配到哪个处理平台，因此数据必须分类；同时，许多信息以加密形式存在
	自动变为失控	可控性是信息安全的重要指标之一
	非法人为干预	如内部攻击
	智能变低能/设备的丢失	

感知层安全

- 感知层安全主要分物理安全和信息安全两类，本节只讨论感知层的信息安全。
- 在感知层，要确保安全通信机制，因此需要从如下几个方面考虑安全性：
- 提供点对点的安全通信服务，需要相应的密钥管理方案作为支撑；针对传感网络的多样性，保证安全路由和连通性，机密性和认证性是必须的，对称密码方案效率高、计算量小，优先考虑；针对不同的安全需求，配置不同的安全模块，提供不同的安全服务。

感知层安全可以提供以下安全服务：

1 保密性

保密性是无线传感网络军事应用中的重要目标，在民用系统中，除部分隐私信息，很多信息并不需要保密

2 完整性

完整性是无线传感器网络安全最基本的需求和目标。虽然很多信息不需要保密，但这些信息必须保证没有被篡改

3 鉴别和认证

对于无线传感网络，组通信是经常使用的通信模式。对于组通信，源端认证是非常重要的安全需求和目标

4 可用性

可用性也是无线传感器网络安全的基本需求和目标。可用性是指安全协议高效可靠，不会给节点带来过多的负载导致节点过早消耗完有限的电能

5 容错性

容错与安全相关，也可以称为使可用性的一个方面。当一部分节点失效或者出现安全问题时，必须保证这个无线传感器网络的正确和安全运行

6 不可否认性

利用不可否认性，节点发送过的信息可以作为证据，证明节点是否具有恶意或者进行了不符合协议的操作。但是，由于传感器的计算能力很弱，该不可否认性不能通过传统的非对称密钥的方式来完成

7 扩展性

WSN的可扩展性表现在传感器节点数量、网络覆盖区域、生命周期、感知精度等方面的可扩展性级别，所以安全保障机制必须提供支持该可扩展性级别的安全机制和算法，来使传感器网络保持正常运行