中国科学技术大学
University of Science and Technology of China

物联网安全基础

中国科学技术大学
曾凡平
billzeng@ustc.edu.cn

創寰宇學府
育天下英才
嚴濟慈題
一九八八年五月

物联网安全基础

1.物联网概述

2.物联网面临的安全问题

3.物联网安全概念

4.物联网安全需求

5.物联网安全体系

6.物联网安全挑战

7.物联网安全现状与发展趋势

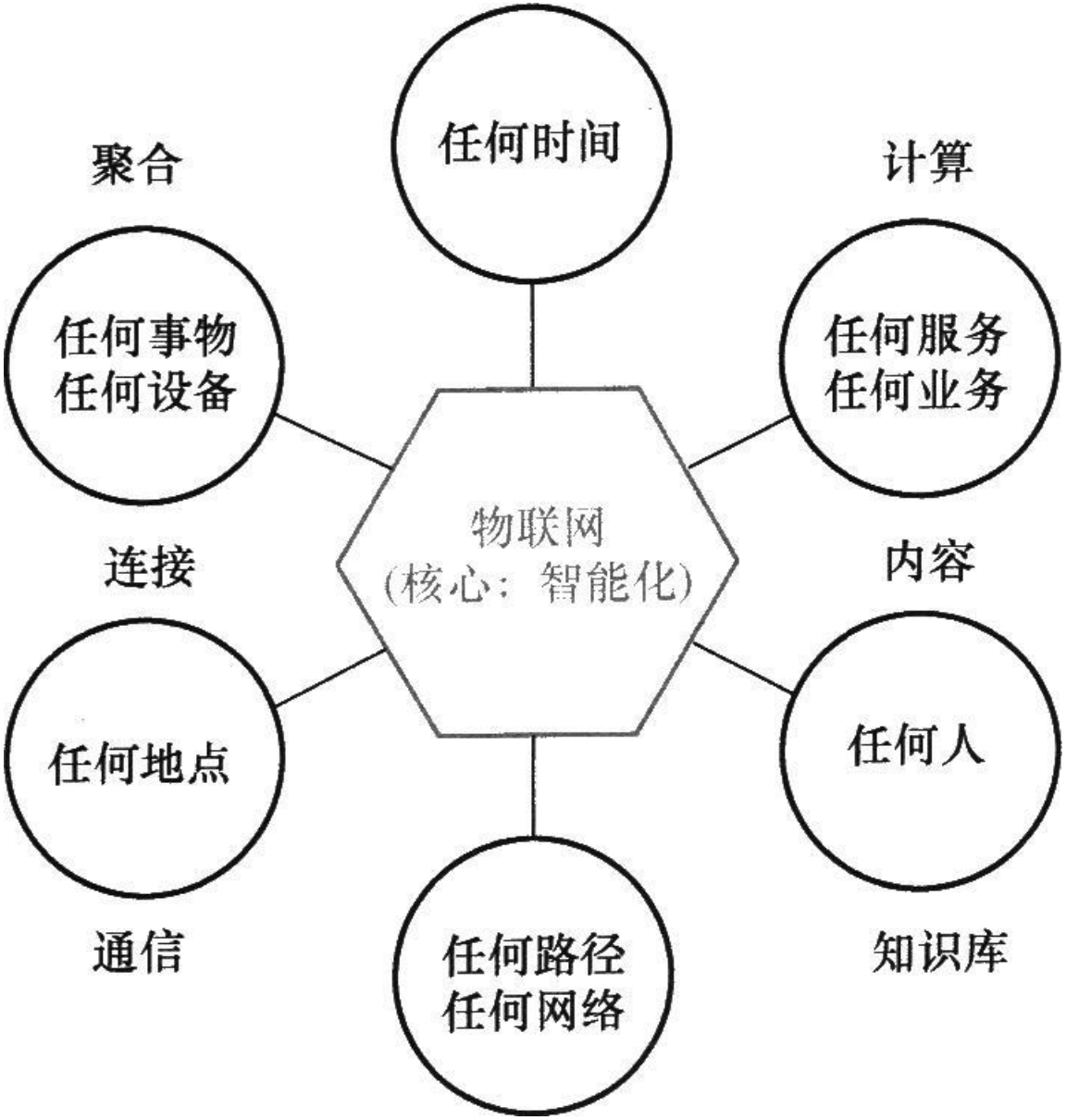
- 胡向东主编.《物联网安全——理论与技术》，北京: 机械工业出版社，2017年.

1. 物联网概述

- 物联网(Internet of Things)是一个基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。它具有普通对象设备化、自治终端互联化和普适服务智能化3个重要特征。
- 基于物联网的英语表述“The Internet of things”可知，物联网就是“物品级的互联网”或“有物品参与的互联网”，是“互联网+”，这里的“+”意味着传统互联网的延伸、拓展与融合，主要有三个方面的含义：

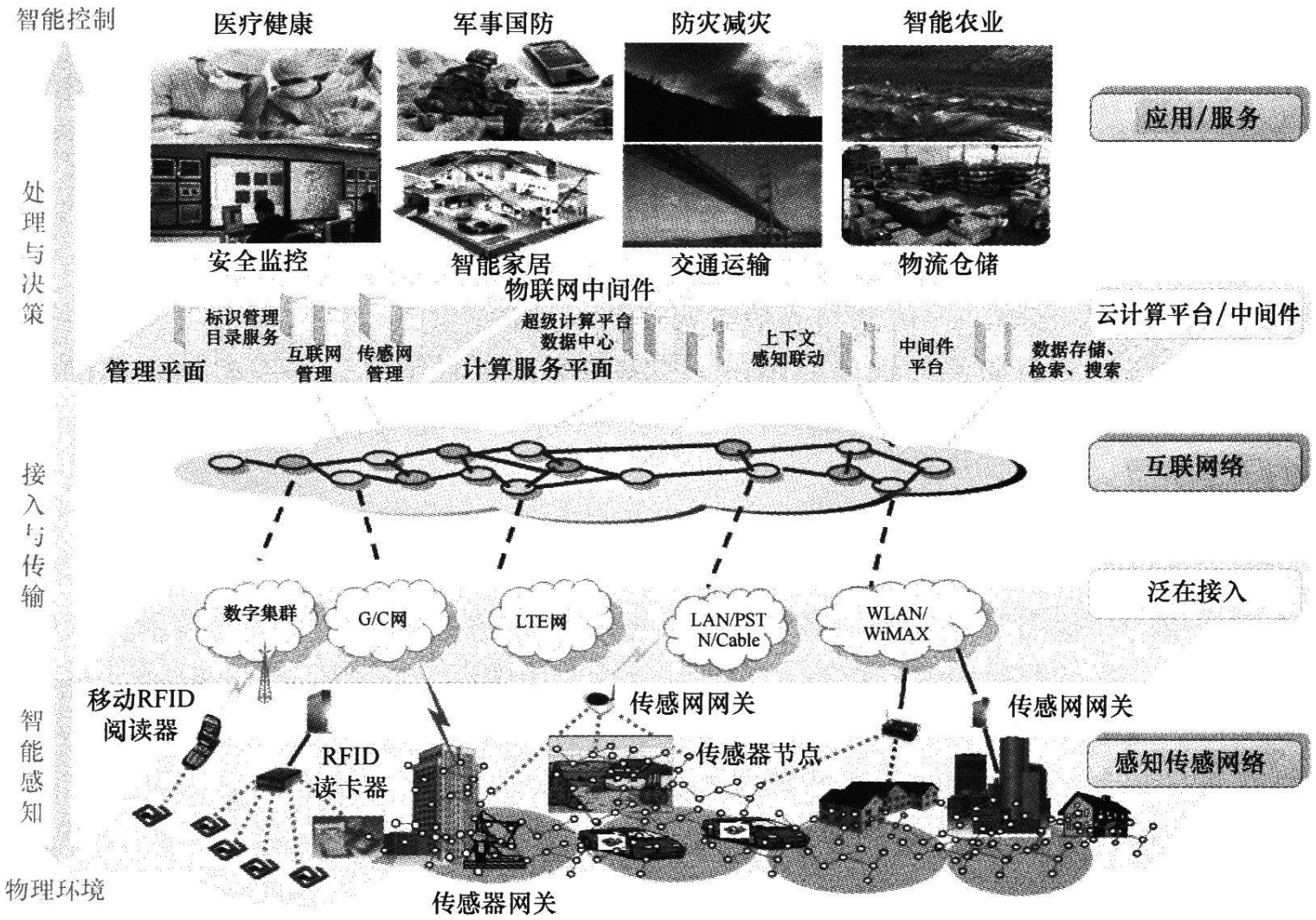
- 1)Internet + things，即互联网的用户端延伸到物品，最明显的变化是由人及物，强化“万物互联”，使得人与人、人与物、物与物之间的互动方式发生改变，均能基于该网络进行信息交换与通信。
- 2)互联网(Internet)本身拓展为互联网、电信网（特别是移动通信网）、广播电视网和传感网等不同形态网络的融合，最关键的变化是在信息传输网络基础上融合了信息感知网络。
- 3)互联网+各个传统行业，是互联网思维在应用实践上的拓展并推动经济形态不断演变，即利用信息通信技术及互联网平台，充分发挥互联网在社会资源配置中的优化和集成作用，将互联网的创新成果与传统行业进行深度融合，创造新的发展形态，提升全社会的创新力和生产力，形成以互联网为基础设施和实现工具的经济发展新形态。

- 物联网的目标在于将虚拟空间与现实世界完美结合，使得现实世界中的“物”可以通过虚拟空间中的“信息”进行连接和控制，实现异构网络的融合、海量终端的互联、超海量数据的增值、各行业应用的支撑等。
- 物联网使得人和物在任何时间(Anytime)、任何地点(Anywhere)，使用任何的路径或网络(Anypath/Anynetwork)、任何的服务与业务(Anyservice/Anybusiness)，与任何的事物(Anything/Anydevice)、任何人(Anyone)无缝地联系(“6A”)，将聚合(Convergence)、内容(Content)、知识库(Collections)、计算(Computing)、通信(Communication)和连接(Connectivity)等元素(“6C”)集成在一起形成一个**以智能化为核心的有机整体。**


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
任何路径
任何网络
知识库

物联网的基本内涵

物联网的3层体系结构：感知层、网络层、应用层



物联网的体系结构

(1) 感知层

- 感知层主要由传感器网络、RFID标签与阅读器、条形码及其阅读器、摄像头、GPS等各种具有信息感知与采集能力的终端设备（传感器件），以及执行器（控制器件）组成（可以认为智能机器人是其中的一个特殊部件），用以完成对信息的采集、转换或执行控制操作。
- 物联网的泛在特性就体现于感知层节点数量众多、具有广泛的覆盖能力，能够实现无所不在的布设，它是整个网络的“神经末梢”“神经元”或“信息元”。

(2)网络层

- 网络层包括泛在接入网和核心的骨干网。泛在接入网包括数字集群、GSM/CDMA网、LTE网、LAN/PSTN/Cable以及WIAN/WiMAX等，负责将感知层收集的信息汇聚起来，然后交由核心的骨干网进行传输，或者将来自骨干网的测控指令分发给感知层的测量或控制节点；
- 骨干网以现有互联网为基础，融合电信网、广播电视网等构成，是完成物联网信息传输的主通道和核心，是物联网的“信息高速公路”。

(3)应用层

- 应用层主要通过对来自传输层的信息进行智能分析、处理，得出决策方案，从而实现智能控制，完成特定业务系统的应用服务。它由业务支撑平台和各种业务应用系统组成。
- 业务支撑平台通常以中间件的形式存在。业务支撑平台从功能上可分为管理平面和计算服务平面两部分，前者负责互联网管理、标识管理、目录管理、安全管理等，后者负责数据处理、存储、检索，以及上下文感知联动、云计算等。物联网的智能化主要体现在业务支撑平台对信息的智能处理与决策控制，即智能信息处理，为层出不穷的应用创新提供支持。业务应用系统由物联网的实际应用领域确定，如医疗健康、军事国防、防灾减灾、智能农业、安全监控、智能家居、交通运输、物流仓储等等。

物联网的本质属性

- 物联网虽起源于互联网，却超越了互联网，形成了自身特有的一些属性。物联网的本质属性可以从以下三个方面来理解：

(1)融合性

- 融合是物联网发展最重要的理念之一，物联网是全面的“互联网+”，具有无穷的包容潜力，基于互联网的延伸、拓展将传统互联网、电信网、广播电视网和传感网等融合起来，将人与物更紧密地连接起来，形成一个广阔无垠的智慧空间。物联网的融合性还表现为信息感知、通信、智能信息处理和信息应用等多学科科学技术的交叉集成；通过设备融合、网络融合、平台融合、技术融合实现服务融合、业务融合和市场融合等。

(2)泛在性

- 物联网发展成一个覆盖世界上万事万物，以无所不在、无所不包、无所不能为基本特征的“6A”网络(Anyone、Anything、Anytime、Anywhere、Anypath、Anybusiness)，基于顺畅的通信实现人与人、人与物、物与物之间按需进行信息获取、传输、处理和应用等，这就是物联网的泛在性。

- 基于物联网的泛在特性可将其称为**泛在网(Ubiquitous network)**。

(3)创新性

- 物联网的创新性不仅表现为在传统互联网基础上实现了三大革命性改变，而且基于这三大变革为智能信息获取与处理及层出不穷的物联网应用创新提供了坚实的基石，物联网的核心理念在于智能化和创新性，从而其堪称掀起世界上第三次信息技术浪潮。
- 物联网是通过能够获取物体信息的传感技术来进行信息采集，通过网络进行信息传输与交换，通过信息处理系统进行信息加工及决策。物联网在整个信息获取、传输、处理与应用的过程中展现出融合性、泛在性和创新性。

物联网有五个基本特征

- 一是全面感知，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；
- 二是无缝互联，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；
- 三是可靠传递，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；

- 四是智能处理，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；
- 五是协同互动，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。

- 正是基于对物联网特征的深入认知，业界通常将物联网分为**感知层（全面感知）、网络层（无缝互联、可靠传递）和应用层（智能处理、协同互动）三个层次**。

2. 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。

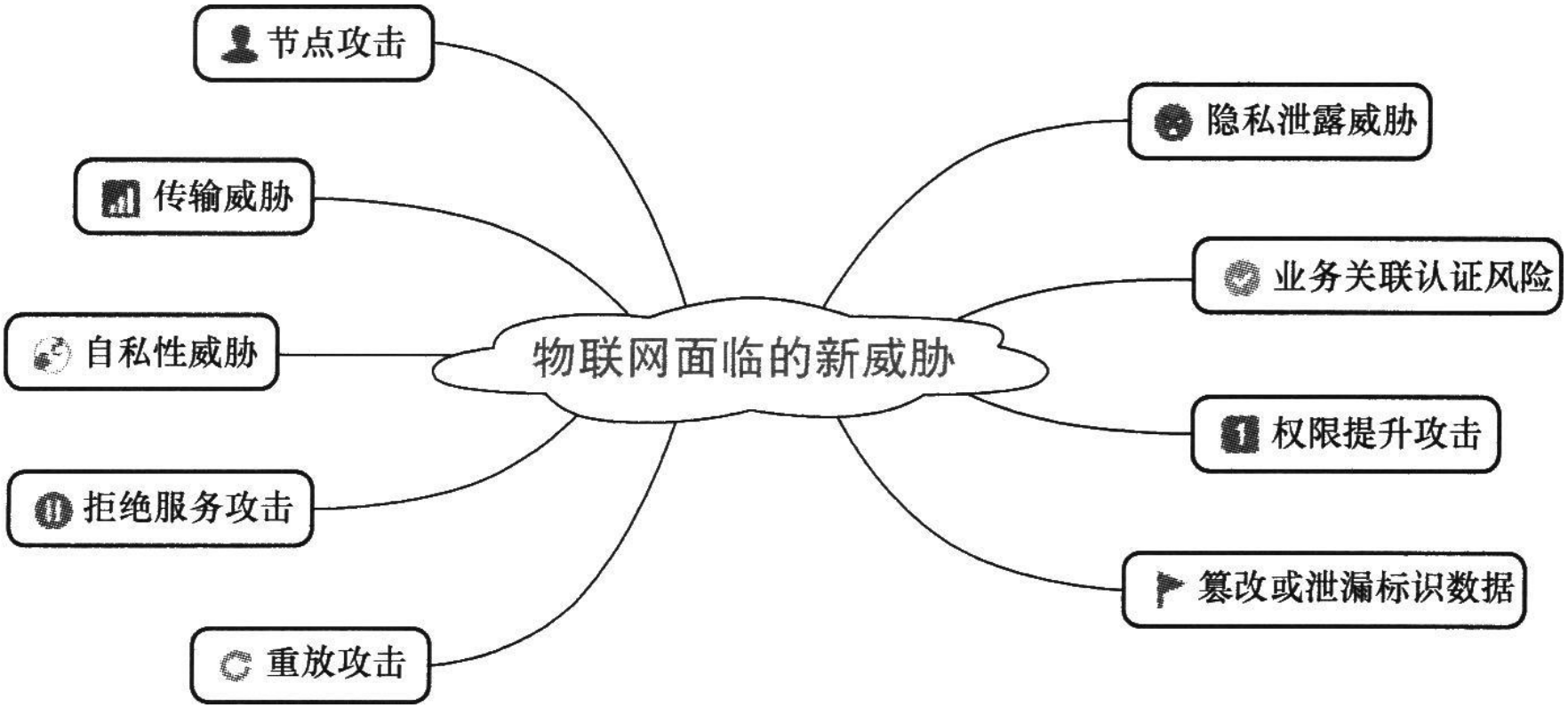
- 物联网尽管超越了传统互联网，但并未脱离互联网，因此，物联网所面临的安全问题既有传统的网络安全威胁，又有不同于互联网的新威胁。

传统的网络安全威胁

详见第1章

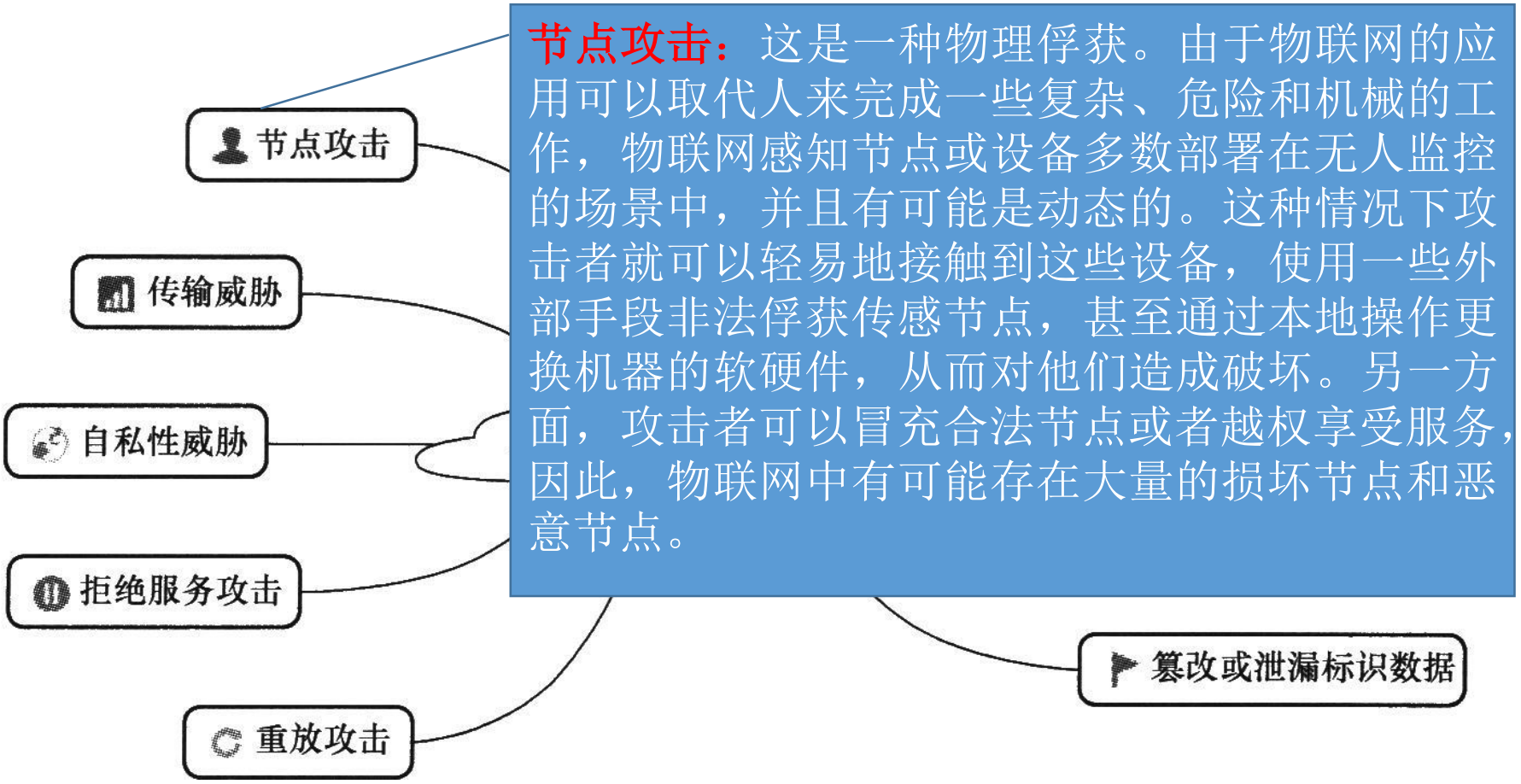
(1) 各种自然因素
(2) 内部窃密和破坏
(3) 信息的截获和重演
(4) 非法访问
(5) 破坏信息的完整性
(6) 欺骗
(7) 抵赖
(8) 破坏系统的可用性。

物联网面临的新威胁



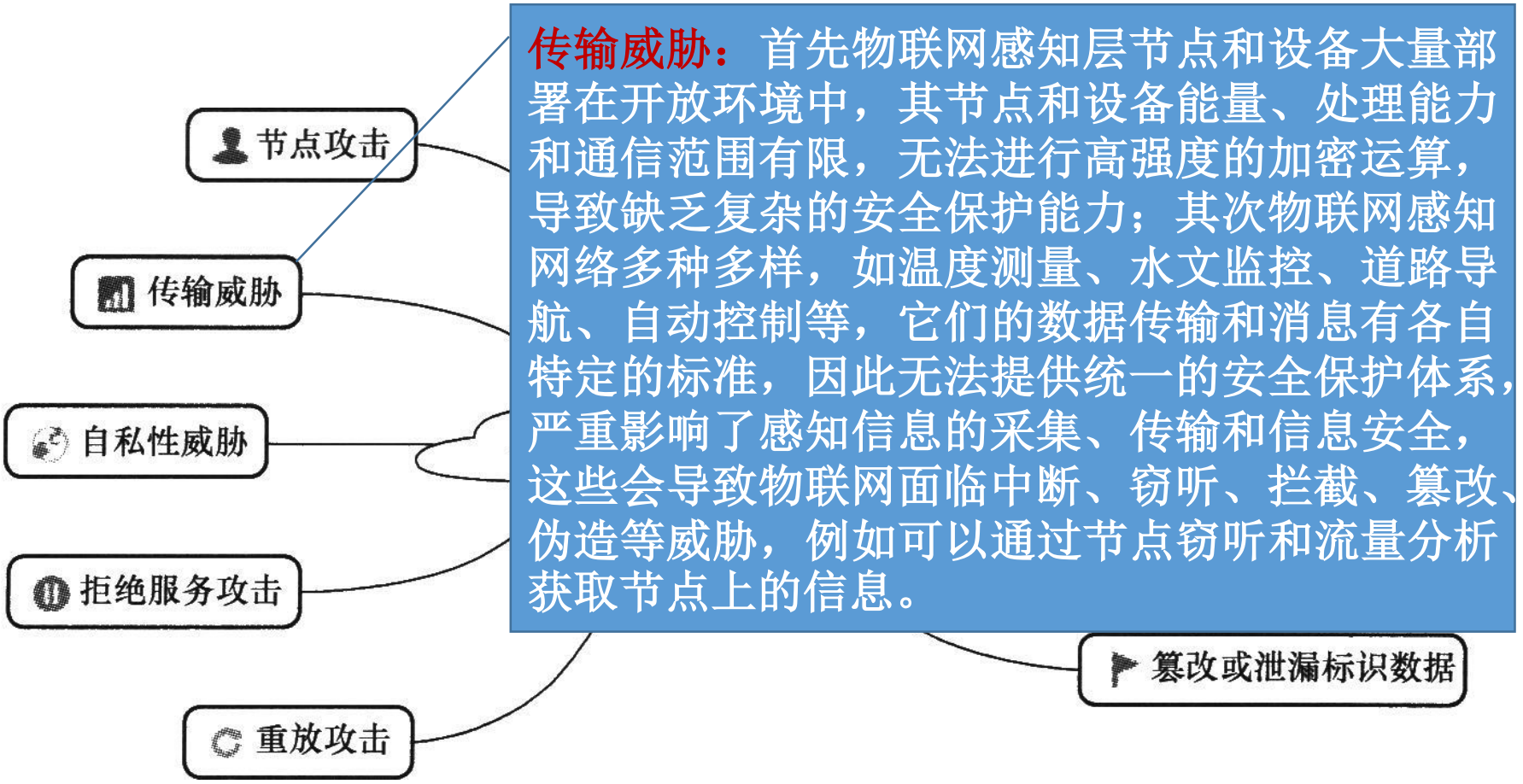
物联网面临的新威胁

物联网面临的新威胁



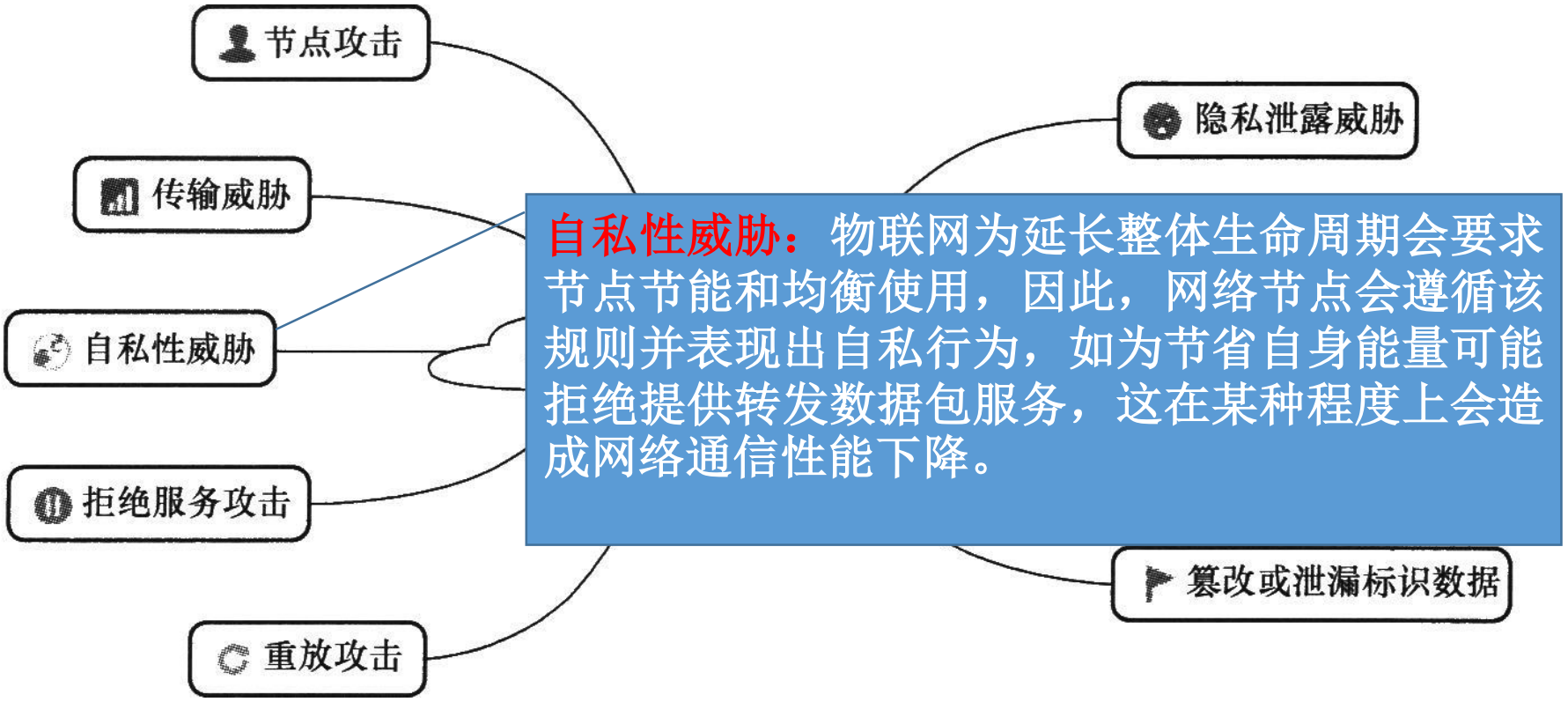
物联网面临的新威胁

物联网面临的新威胁



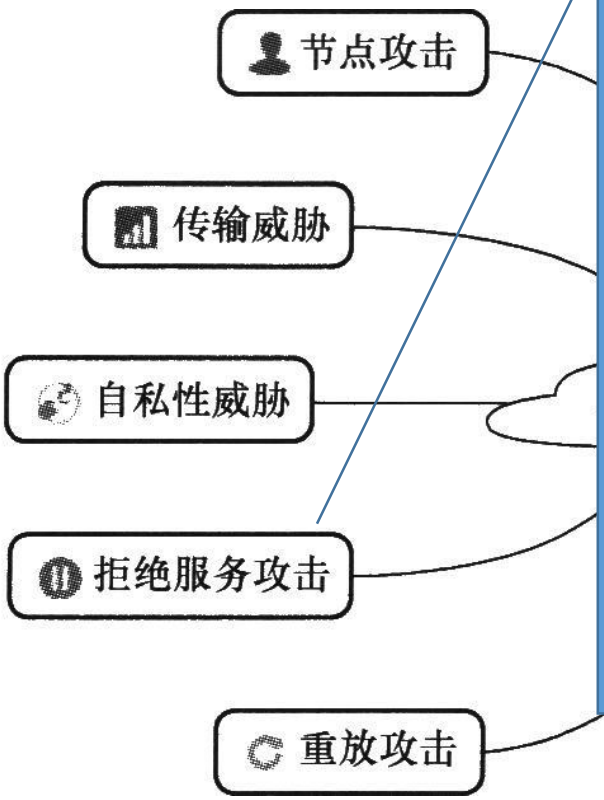
物联网面临的新威胁

物联网面临的新威胁



物联网面临的新威胁

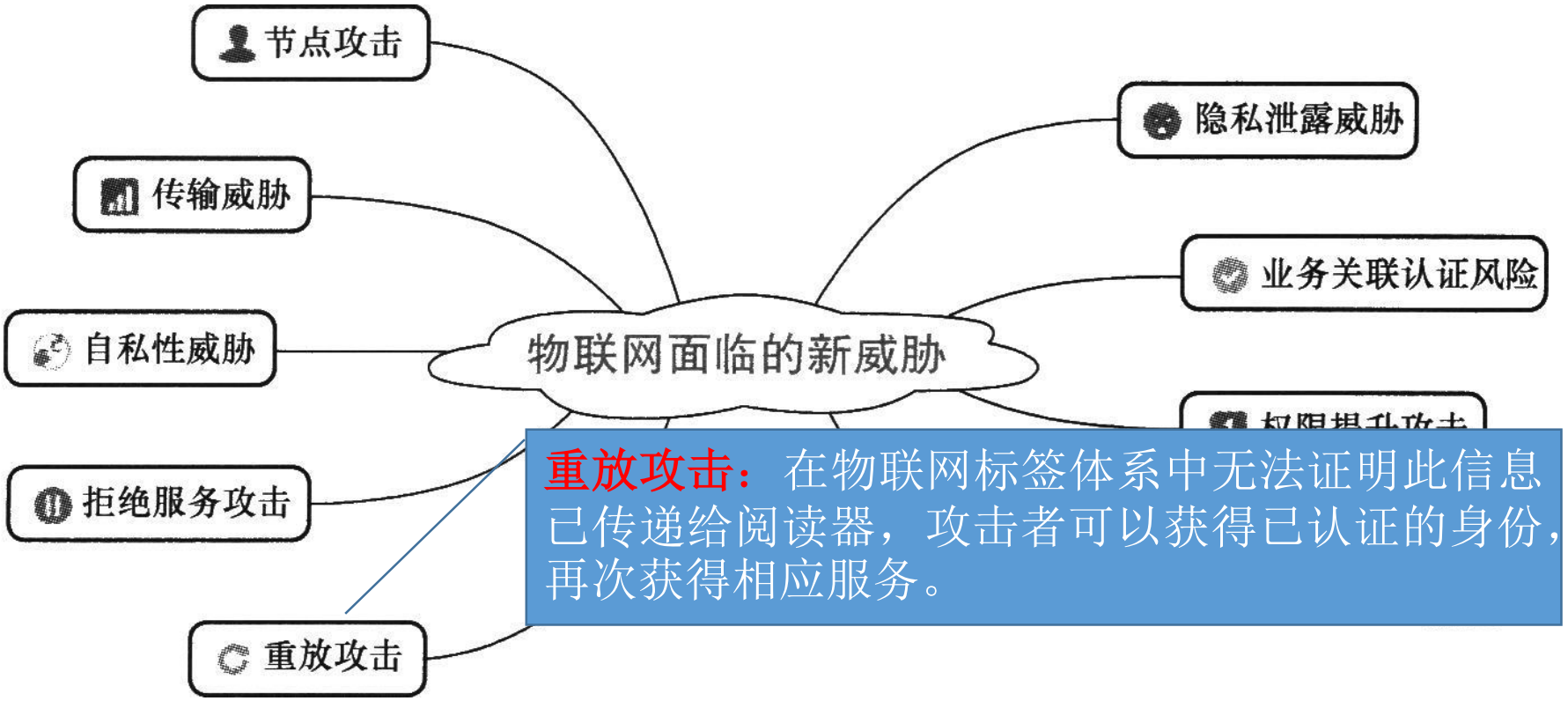
物联网面临的新威胁



拒绝服务攻击：一方面，物联网的对象名解析服务（Object Name Service，ONS）以DNS(Domain Name System)技术为基础，ONS同样也继承了DNS的安全隐患，例如ONS漏洞导致的拒绝服务攻击，利用ONS服务作为中间的攻击放大器去攻击其他节点或主机等；另一方面，由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传输时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。攻击者利用广播Hello信息，并利用通信机制中优先级策略、虚假路由等协议漏洞同样可以产生拒绝服务攻击。

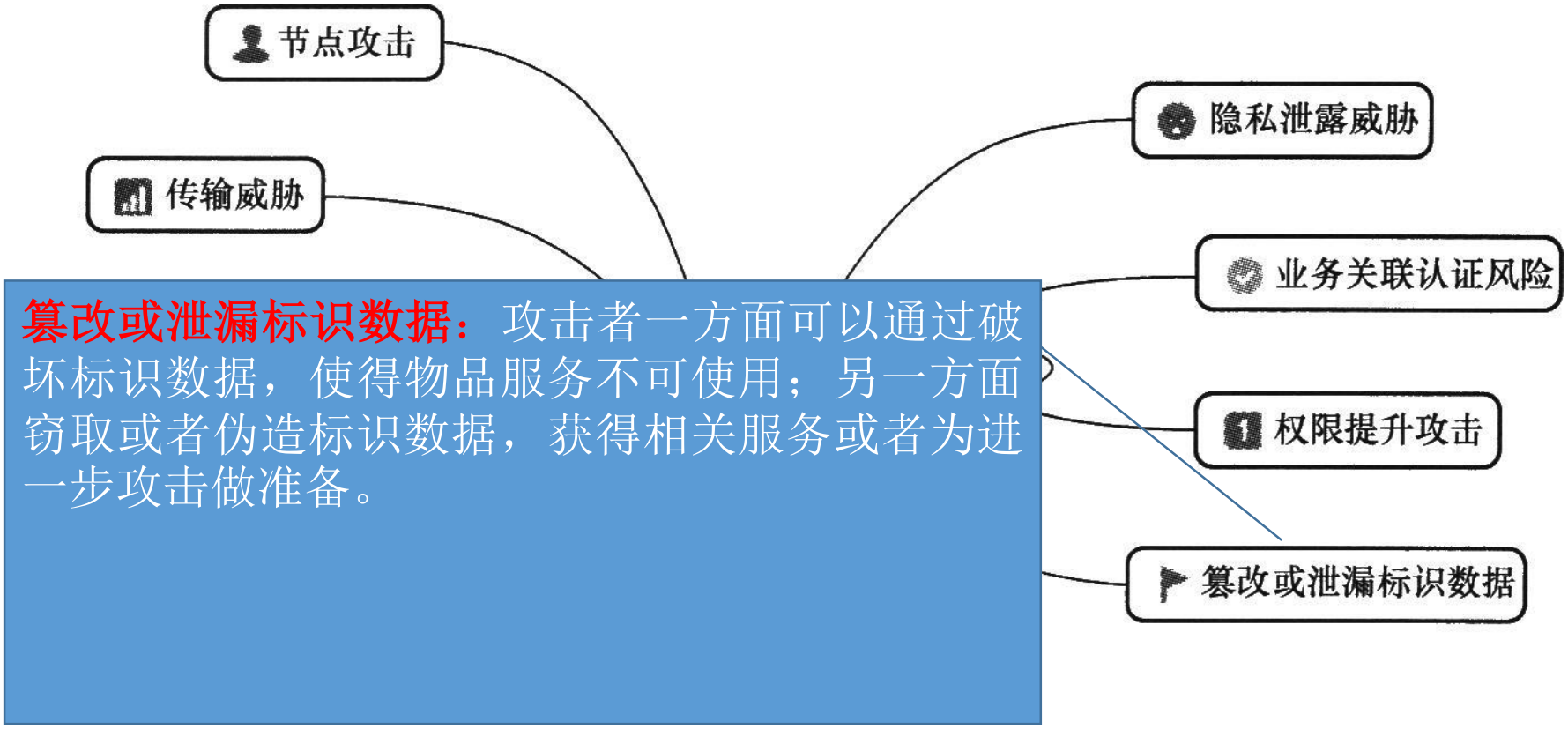
物联网面临的新威胁

物联网面临的新威胁



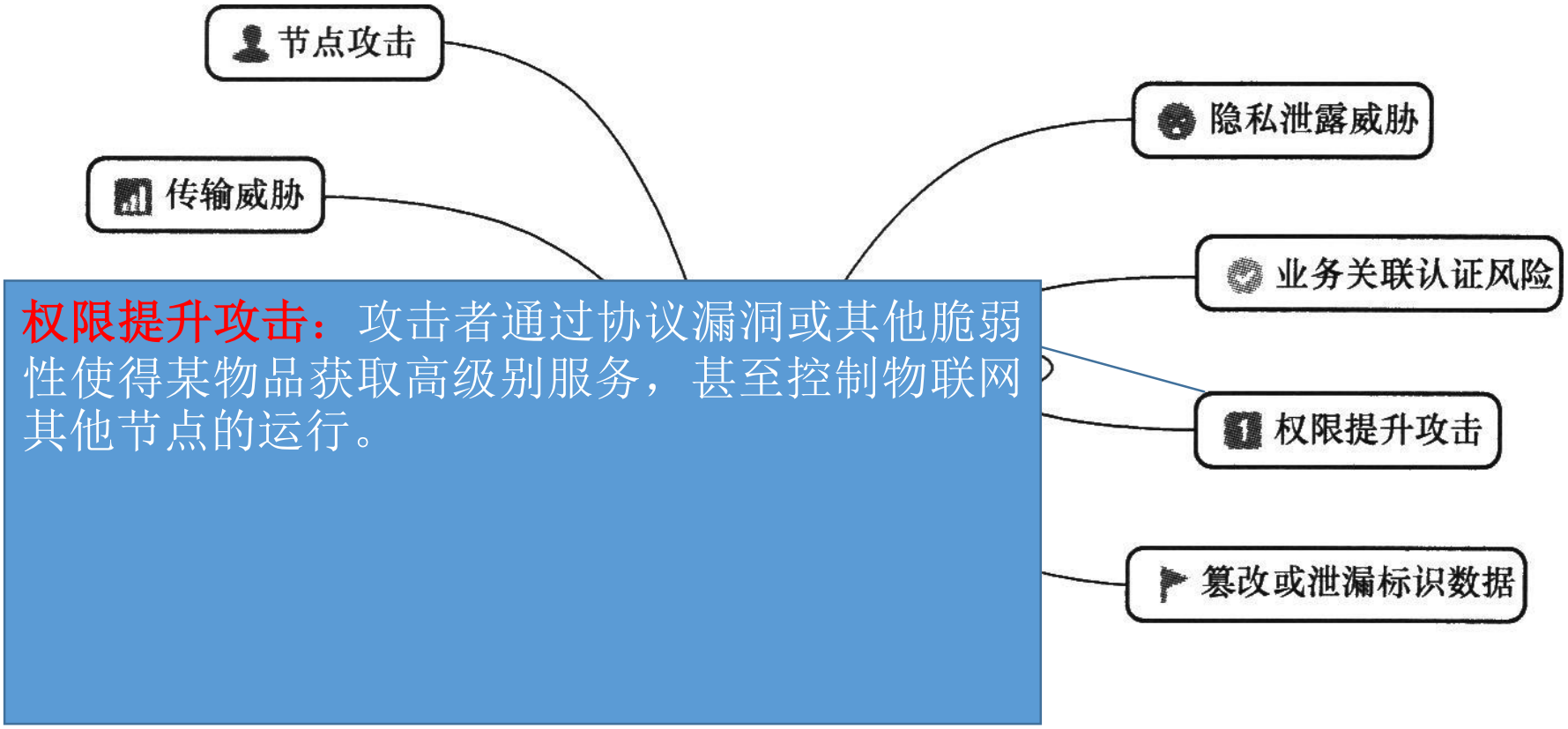
物联网面临的新威胁

物联网面临的新威胁



物联网面临的新威胁

物联网面临的新威胁

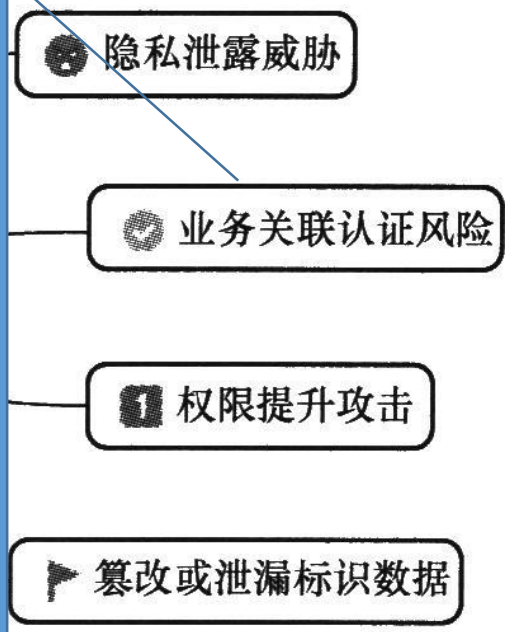


物联网面临的新威胁

物联网面临的新威胁

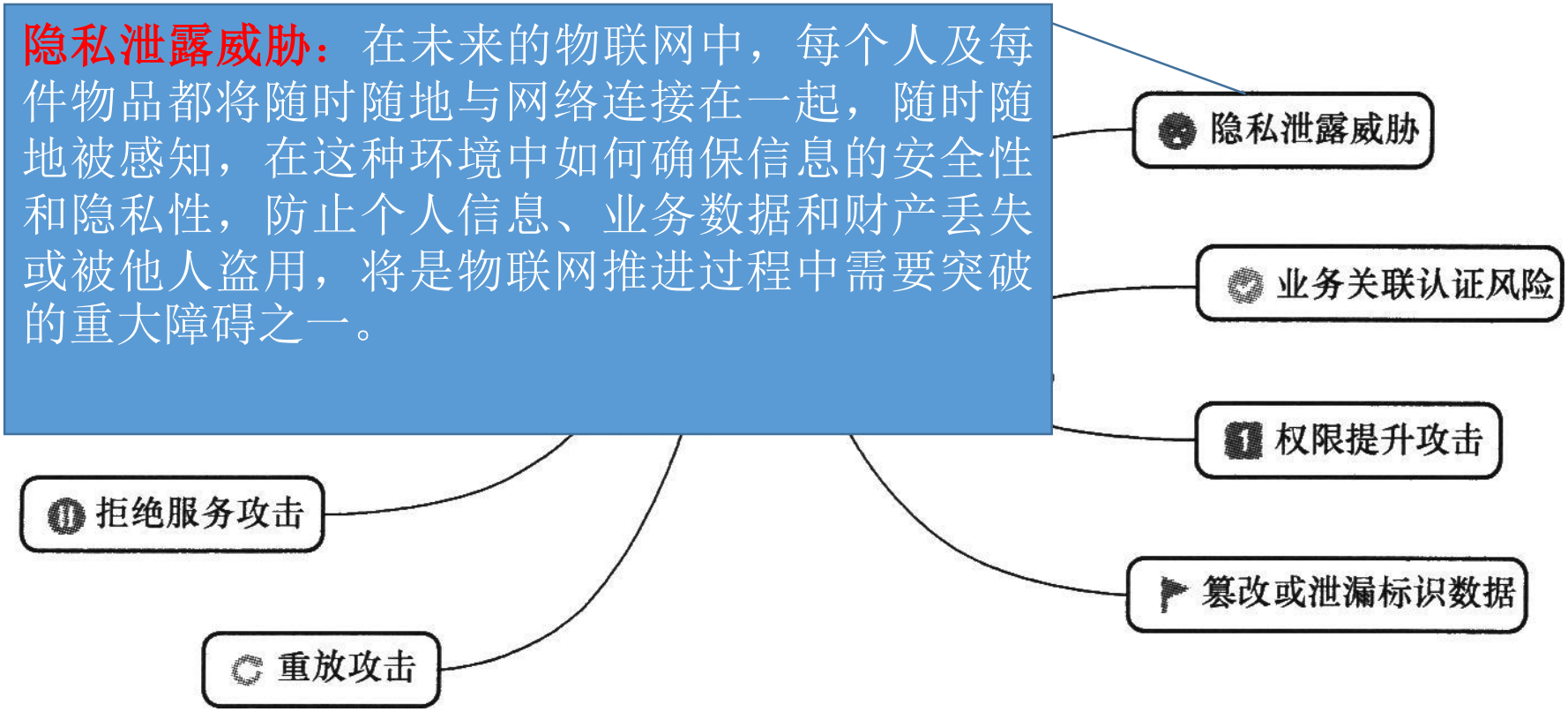
业务关联认证风险：传统的认证是区分不同层次的，网络层的认证就负责网络层的身份鉴别，业务层的认证就负责业务层的身份鉴别，两者独立存在。但是在物联网中，大多数情况下机器都是拥有专门的用途，因此其业务应用与网络通信紧紧地绑在一起。由于网络层的认证是不可缺少的，那么其业务层的认证机制就不再是必需的，而是可以根据业务由谁来提供和业务的安全敏感程度来设计。

例如，当物联网的业务由运营商提供时，那么就可以充分利用网络层认证的结果而不需要进行业务层的认证；当物联网的业务由第三方提供时，就可以发起独立的业务认证而不用考虑网络层的认证；当业务较敏感时，一般业务提供者会不信任网络层的安全级别，而使用业务层认证；对于普通业务（如气温采集等），业务提供者认为网络层认证已经足够，那么就不再需要业务层认证。这在实际操作中可能出现一定的安全风险。



物联网面临的新威胁

隐私泄露威胁：在未来的物联网中，每个人及每件物品都将随时随地与网络连接在一起，随时随地被感知，在这种环境中如何确保信息的安全性和隐私性，防止个人信息、业务数据和财产丢失或被他人盗用，将是物联网推进过程中需要突破的重大障碍之一。

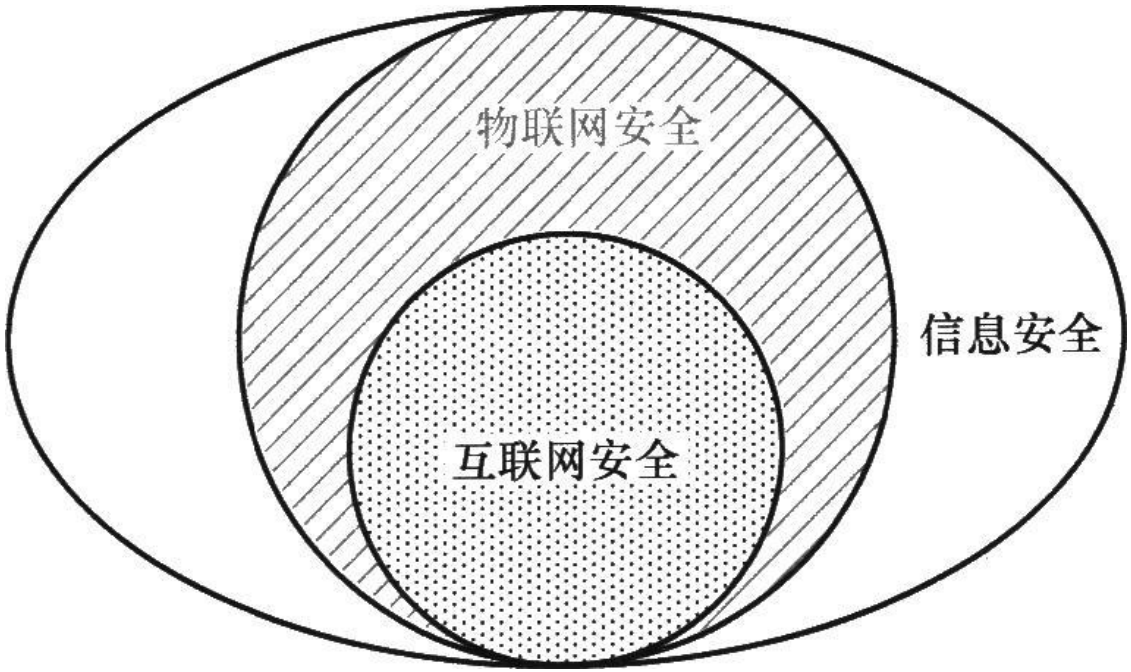


物联网面临的新威胁

3.物联网安全概念

- **物联网安全**是指**物联网**环境下的**网络安全**，是指物联网系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，物联网系统连续可靠正常地运行，网络服务不中断。
- 物联网安全包括**物理安全**（主要表现为对传感器的干扰、屏蔽、信号截获等）、**运行安全**（存在于传感器、信息传输系统和信息处理系统等物联网组成要素中，影响其正常运行）、**数据安全**（要求物联网中的信息不被窃取、篡改、伪造、抵赖等）。

- 信息安全的实质就是保护系统或网络中的信息资源免受各种类型的威胁、干扰、破坏、非法利用或恶意泄露，即保证信息的安全性。
- **物联网安全和互联网安全则是将信息安全的范畴限定于物联网或互联网之内，即保护物联网或互联网中的信息资源免受各种威胁、干扰和破坏。**物联网安全的目标则是达成物联网中的信息安全性，确保物联网能够按需地为获得授权的合法用户提供及时、可靠、安全的信息服务。



物联网安全与互联网安全、信息安全的关系

物联网安全的特点

(1)广泛性

- 与互联网相比，物联网具有更加广泛的地域、领域、对象覆盖性。一方面，大量的物联网感知节点广泛地分布于众多的领域和区域，表现出泛在化的特点；另一方面，物联网与普通大众的联系程度将远远超越互联网，并深刻地影响着人们的职业活动与休闲生活，当每个人都习惯于使用网络来处理每天的事务时，如网上办公、网上购物、智能交通、智能家居等，物联网安全必然与我们每个人紧密联系在一起。物联网将无处不在，物联网安全也将如影随形，这就是物联网安全的广泛性。

物联网安全的特点

(2)复杂性

- 物联网组成的多态性、应用领域的广泛性、所蕴含技术的差异性以及面临安全威胁的多样性等决定了物联网安全的复杂性，物联网安全涉及许多互联网安全所没有的新问题和新技术，物联网安全同时要面对信息感知、信息传输、信息处理和信息应用等多方面的安全问题，并且更加强调用户隐私的保护。

物联网安全的特点

(3)非对称性

- 物联网感知层的节点能力较弱、数量庞大，而网络中心的计算能力很强、数量有限，因此，整个网络表现出明显的非对称性。物联网安全在面向这种非对称结构的网络时，需要兼顾能力较弱的感知节点和能力很强的网络中心的安全处理能力，采用高效的安全管理措施来进行协调，从而形成整体上的安全综合能力。

物联网安全的特点

(4)轻量级

- 物网中有数量巨大的低能节点，物联网面临的安全威胁规模也将是空前的，安全与需求的矛盾将十分突出。物联网安全解决方案中必然有相当一部分是轻量级、低成本的，只有这样才能**适应物联网感知层的特点与物联网大规模分布应用**，也只有这样才可能为普通大众所接受。因此，物联网安全表现出轻量级的特点。

4. 物联网安全需求

物联网感知层安全

- **感知层的出现是物联网区别于传统互联网最重要的特征之一。**物联网感知层由若干的传感器或RFID等感知节点组成，呈现多源异构性，由于受到计算和通信等能力不足、能量等资源有限的约束，难以提供统一的安全保护体系，实施安全方案的选择性较小，且还没有形成标准化的安全机制，可能受到安全威胁的问题较突出，对机密性、节点认证、密钥协商、信誉评估、安全路由、安全数据融合等要求较高。

物联网安全需求—感知层安全

(1)节点本身的安全需求

- 由于往往分布于无人值守的区域，物联网感知层的节点可能受到捕获和拆解等物理攻击，攻击者也可能部署恶意节点加入物联网感知层，进而实施针对节点身份（如假冒）、采集的数据（如伪造）或节点间数据传输（如选择性转发）的破坏活动。故需要对物联网感知层的节点本身加以保护。

物联网安全需求—感知层安全

(2)所采集信息的安全需求

- 物联网感知层的基本功能就是依托感知节点完成对所覆盖区域的相关信息采集，并以多跳的方式传递给汇聚节点或中心站点。攻击者针对感知层信息采集可能实施的攻击行为包括：窃听、篡改、伪造或重放数据；破坏数据的机密性、完整性、真实性、新鲜性等属性；实施针对路由方面的选择性转发攻击、Sinkhole攻击、Sybil攻击、Wormhole攻击、Hello洪泛攻击等，导致节点采集的信息无法到达目标节点。故需要对采集的信息进行保护。

物联网安全需求—网络层安全

(1)大批量接入认证需求

- 接入认证是确保网络中实体身份合法和信息安全的前提。传统的一对一接入认证模式和网关设备难以适应物联网短期内大批量接人的认证需求。

(2)避免网络拥塞和拒绝服务攻击的需求

- 物联网中节点和设备数量众多，传输的连接认证请求、路由等信令流量和采集的数据等信息流量可能十分巨大，任何微小的网络故障或攻击行为都可能导致网络拥塞，或出现服务器拒绝服务的现象。

物联网安全需求—网络层安全

(3)高效的密钥管理需求

- 传统的针对网络终端或通信实体逐个进行认证、产生密钥、分配密钥、使用密钥、更新密钥、销毁密钥等密钥管理模式难以适应物联网的终端众多特征，不仅会带来密钥管理效率低下，还会导致大量的能量和通信资源消耗。

物联网安全需求—应用层安全

- 物联网应用层涉及物联网的信息处理（业务支撑平台）和具体的应用（业务）。
- 信息处理包括云计算、分布式系统、海量信息处理、数据的存储管理、挖掘分析等，要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统，涉及隐私保护等安全问题，如如何根据不同访问权限对同一数据库内容进行筛选，如何兼顾用户隐私保护和认证等。应用业务覆盖的范围十分广泛，是针对不同的行业应用建立相应的安全策略，还是建立一个相对独立的安全架构；如何解决信息泄露追踪，如何进行计算机取证，如何销毁计算机数据，如何保护电子产品和软件的知识产权等，因此，其安全需求具有多样性，内容丰富，包括：身份认证、消息认证、访问控制、数据的机密性与用户隐私保护、数字签名、数字水印、入侵检测、容错容侵等。

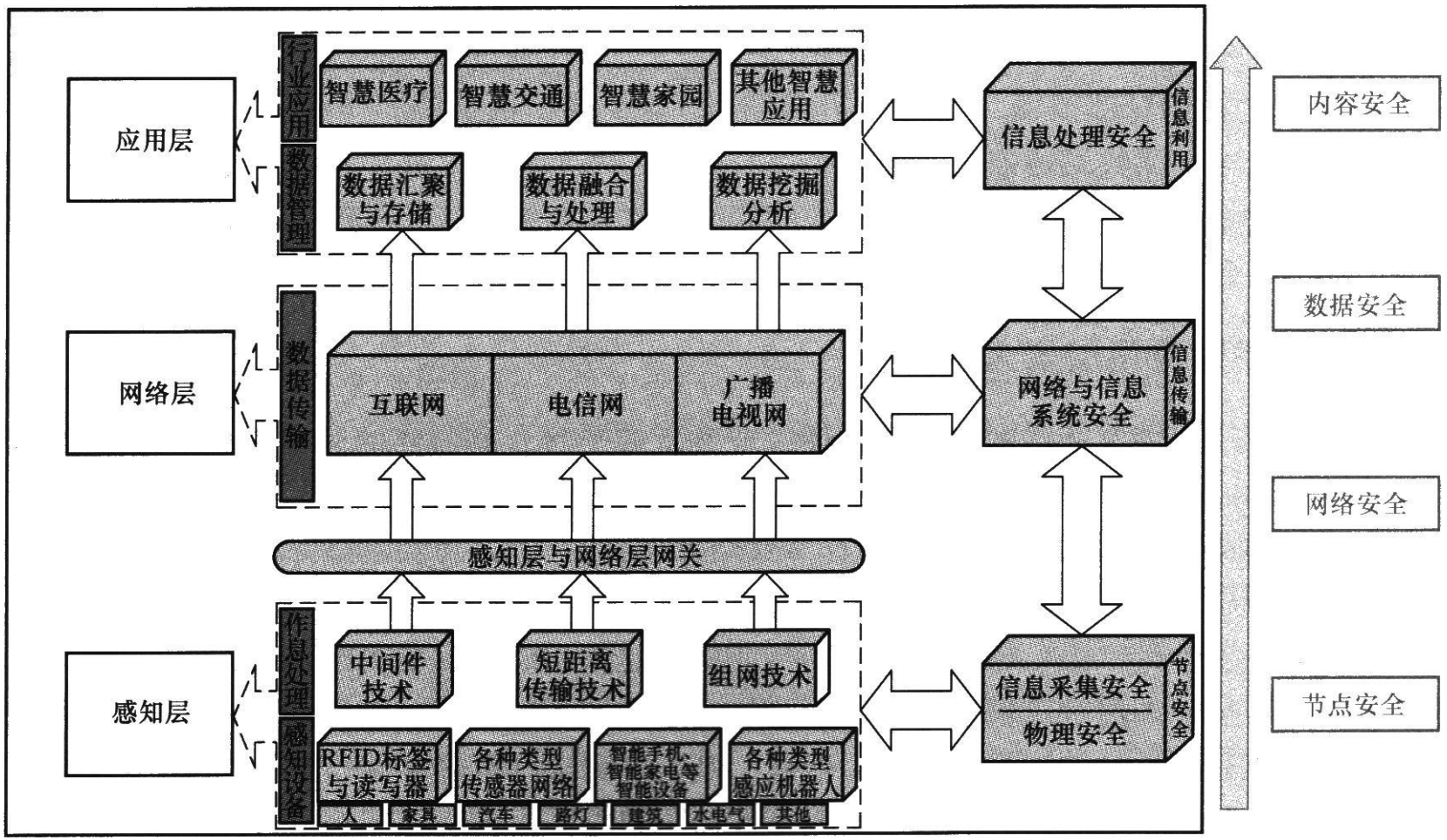
5.物联网安全体系

- 解决物联网安全的总体思路就是技术与管理并重。
- **首先，要以技术为支撑**，构建起物联网安全基础设施，包括研究芯片级的物理安全技术，完善传输级的密码与密钥管理技术，加强接入级的认证与访问控制，实现应用级的风险评估、入侵检测和安全控制；
- **其次，要以管理为保障**，通过强化物联网安全教育管理，完善物联网安全立法，严厉打击物联网安全犯罪。只有技术与管理相互配合，才有实现物联网安全的可能。通常对外部威胁主要采用技术手段，对内部威胁则强化管理措施。构建完备的物联网安全体系是确保技术支撑得力、管理保障有效的核心。

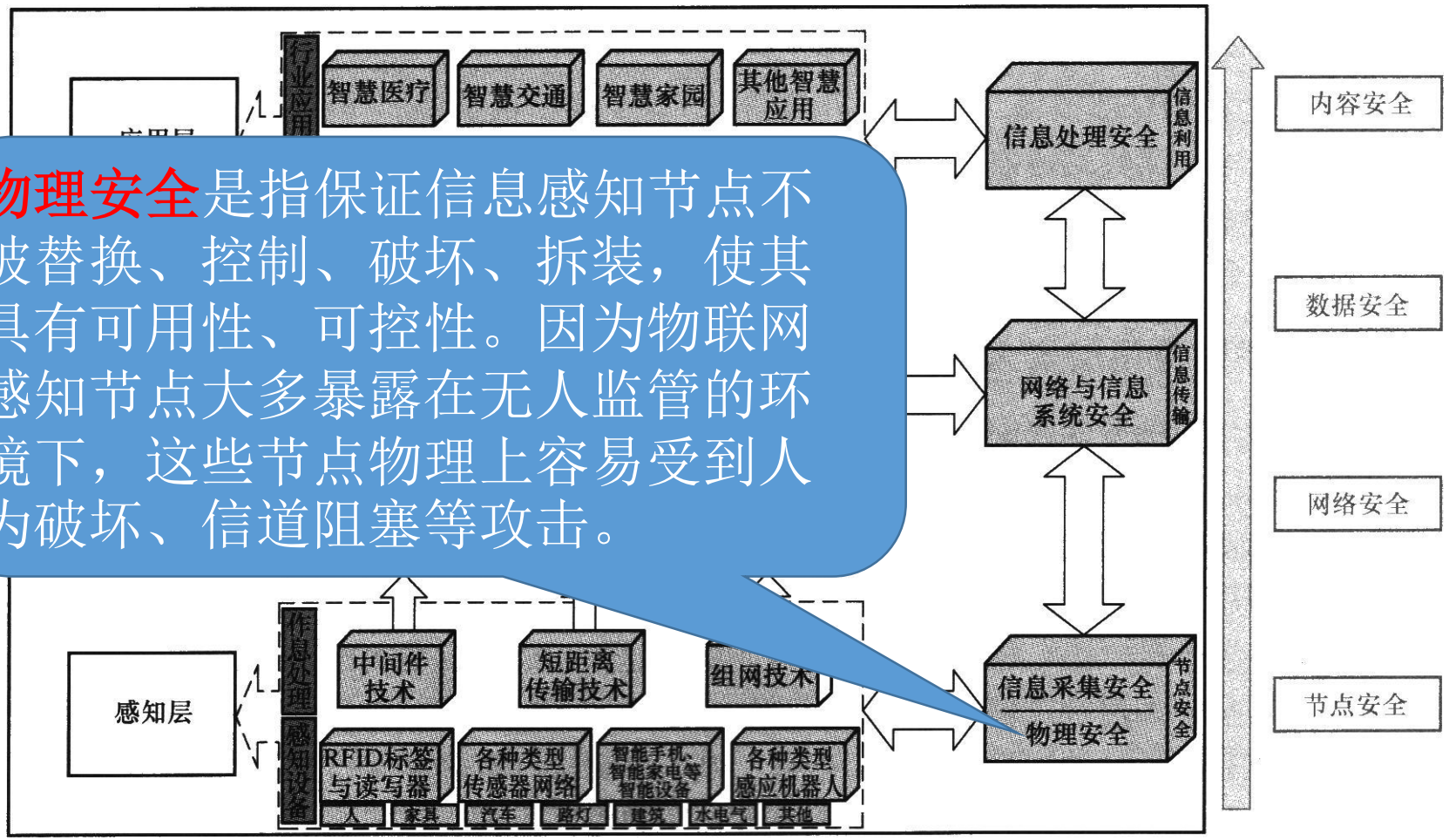
物联网安全体系结构

- 物联网的构成要素包括传感器件、信息传输系统和信息处理系统，从结构上分别位于物联网的感知层、网络层以及应用层，对应着**DCM分层模型的设备(Devices)、连接(Connection)和管理(Management)**。

- 相应地，其安全形态表现为感知层安全（包括物理安全和信息采集安全）、网络层安全（网络与信息系统安全）、应用层安全（信息处理安全）。


应用层
网络层
感知层
行业应用
数据管理
数据传输
信息处理
感知设备
智慧医疗
智慧交通
智慧家园
其他智慧应用
数据汇聚与存储
数据融合与处理
数据挖掘分析
互联网
电信网
广播电视网
感知层与网络层网关
中间件技术
短距离传输技术
组网技术
RFID标签与读写器
各种类型传感器网络
智能手机、智能家电等智能设备
各种类型感应机器人
人
家具
汽车
路灯
建筑
水电气
其他
信息处理安全
信息利用
网络与信息系统安全
信息传输
信息采集安全
物理安全
节点安全
内容安全
数据安全
网络安全
节点安全

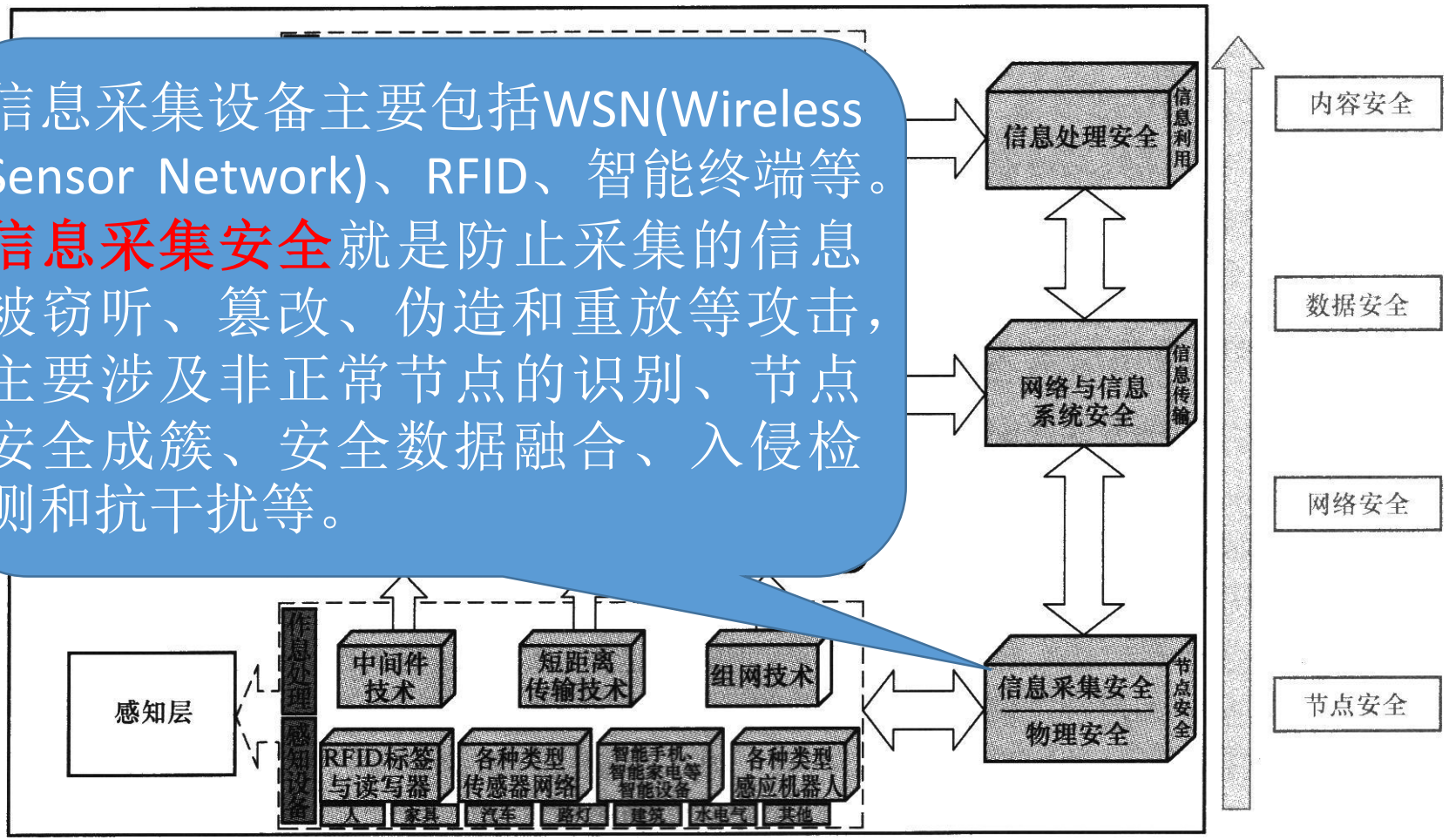
物联网安全体系结构



物理安全是指保证信息感知节点不被替换、控制、破坏、拆装，使其具有可用性、可控性。因为物联网感知节点大多暴露在无人监管的环境下，这些节点物理上容易受到人为破坏、信道阻塞等攻击。

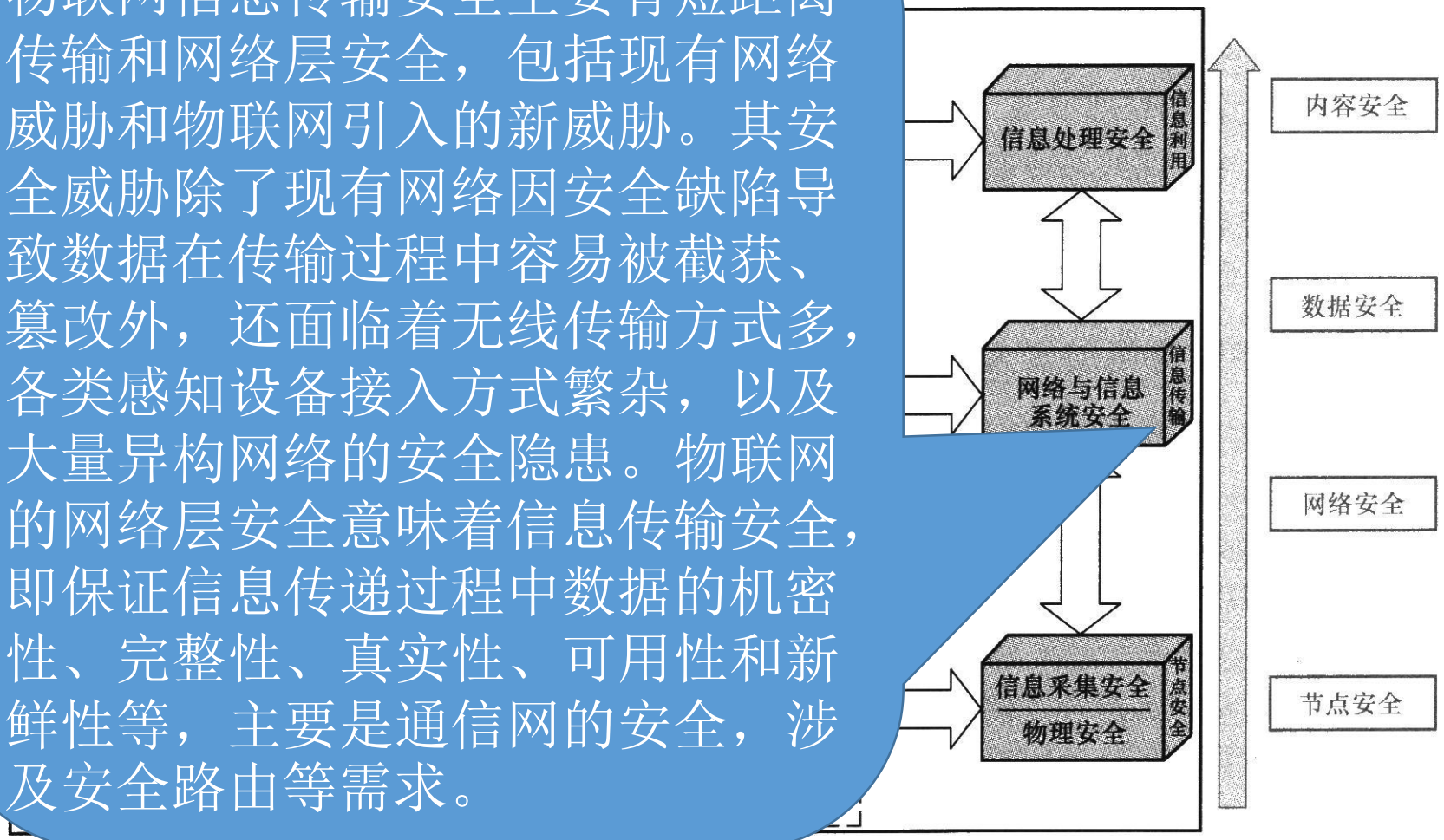
物联网安全体系结构

信息采集设备主要包括WSN(Wireless Sensor Network)、RFID、智能终端等。**信息采集安全**就是防止采集的信息被窃听、篡改、伪造和重放等攻击，主要涉及非正常节点的识别、节点安全成簇、安全数据融合、入侵检测和抗干扰等。

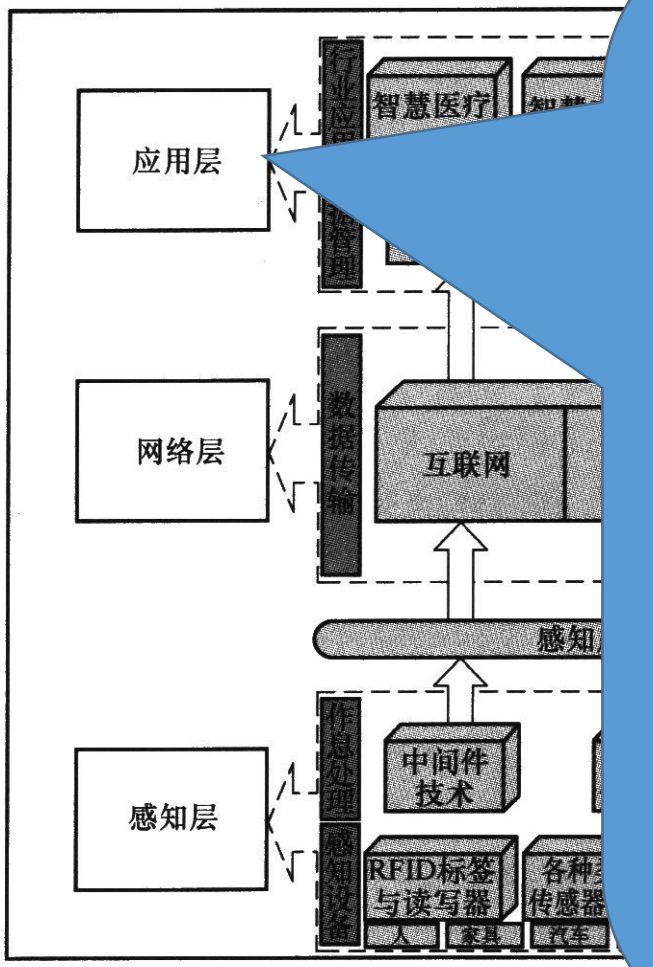


物联网安全体系结构

网络层是物联网信息传输的主干道。物联网信息传输安全主要有短距离传输和网络层安全，包括现有网络威胁和物联网引入的新威胁。其安全威胁除了现有网络因安全缺陷导致数据在传输过程中容易被截获、篡改外，还面临着无线传输方式多，各类感知设备接入方式繁杂，以及大量异构网络的安全隐患。物联网的网络层安全意味着信息传输安全，即保证信息传递过程中数据的机密性、完整性、真实性、可用性和新鲜性等，主要是通信网的安全，涉及安全路由等需求。



物联网安全体系结构

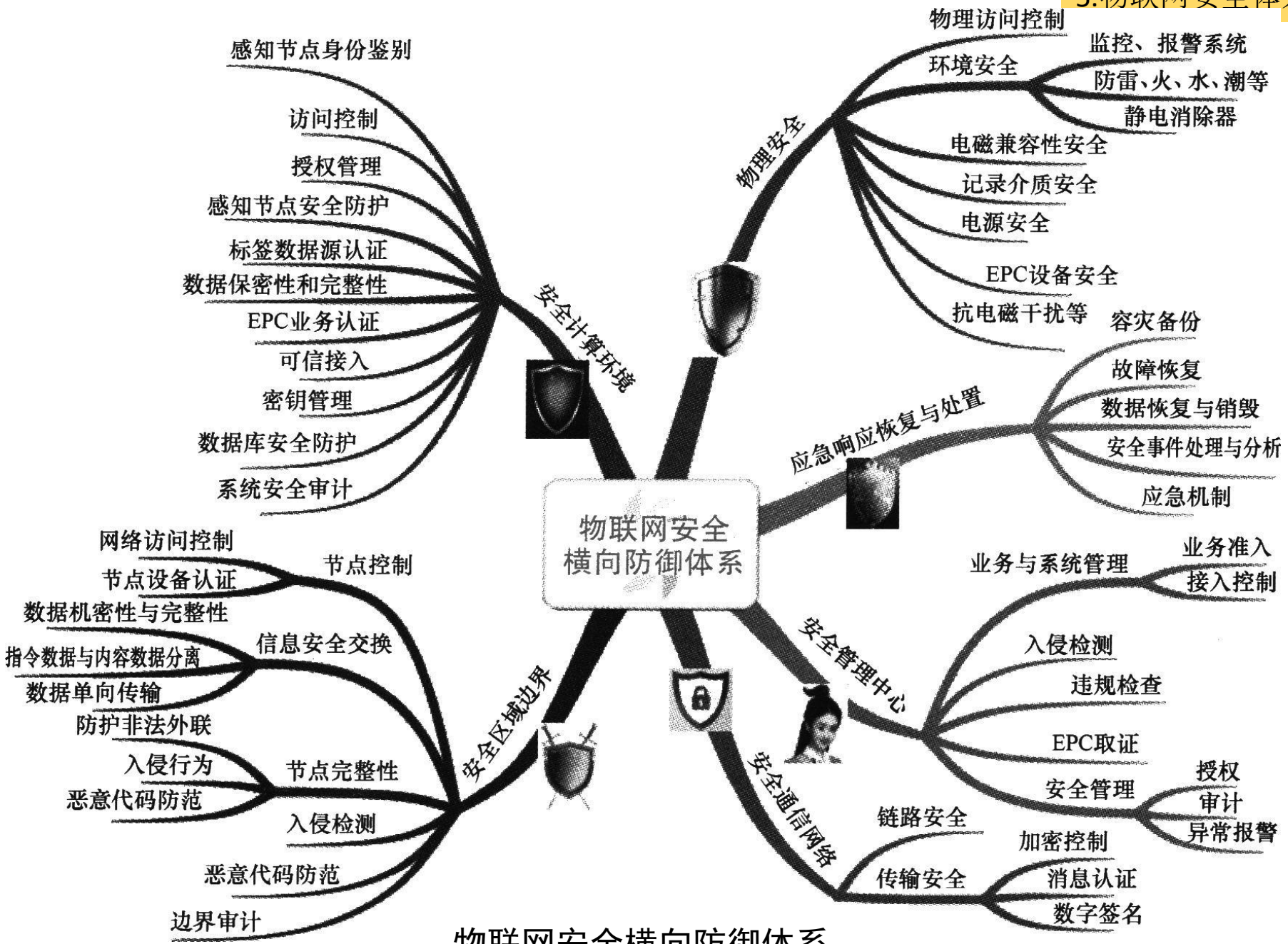


应用层安全对应着物联网的信息处理和应用安全，保证信息的机密性、可鉴别性和储存安全，主要是隐私保护、数据管理安全和应用安全。涉及安全定位、身份认证和访问控制等。数据管理主要包括对数据的存储管理、挖掘分析等，涉及个人或团体的隐私暴露问题。各类智慧型应用的管理不完善、系统自身存在漏洞或设计缺陷，攻击者可利用它们获得权限，执行恶意攻击。

物联

物联网安全技术体系

- 物联网安全技术体系可以从**纵深防御体系和横向防御体系**两个方面来理解。
- 纵深防御体系可分为边界防护（单个应用的边界）、区域防护（单个业务应用区域）、节点防护（如服务器或感知节点）和核心防护（针对一个具体的安全技术，或具体的节点与用户，或操作系统的内核等）。
- 横向防御体系分为物理安全、安全计算环境、安全区域边界、安全通信网络、安全管理中心、应急响应恢复与处置六个层面，以满足物联网密钥管理、点到点消息认证、防重放、抗拒绝服务、防篡改或隐私泄漏、业务安全等安全需求，实现数据或信息在传输、存储、使用过程中机密性、完整性、可追责性、可用性的物联网安全基本目标。



物联网安全横向防御体系

- **物理安全：**主要包括物理访问控制、环境安全（监控、报警系统、防雷、防火、防水、防潮、静电消除器等装置）、电磁兼容性安全、记录介质安全、电源安全、EPC(Electronic Product Code)设备安全、抗电磁干扰等方面。
- **安全计算环境：**主要包括感知节点身份鉴别、访问控制、**授权管理(Public Key Infrastructure，即PKI系统)**、感知节点安全防护（恶意节点、异常节点、失效节点识别）、标签数据源认证、数据保密性和完整性、EPC业务认证、可信接入、密钥管理、数据库安全防护、系统安全审计。
- **安全区域边界：**主要包括节点控制（网络访问控制、节点设备认证）、信息安全交换（数据机密性与完整性、指令数据与内容数据分离、数据单向传输）、节点完整性（防护非法外联、入侵行为、恶意代码防范）、入侵检测、恶意代码防范、边界审计。

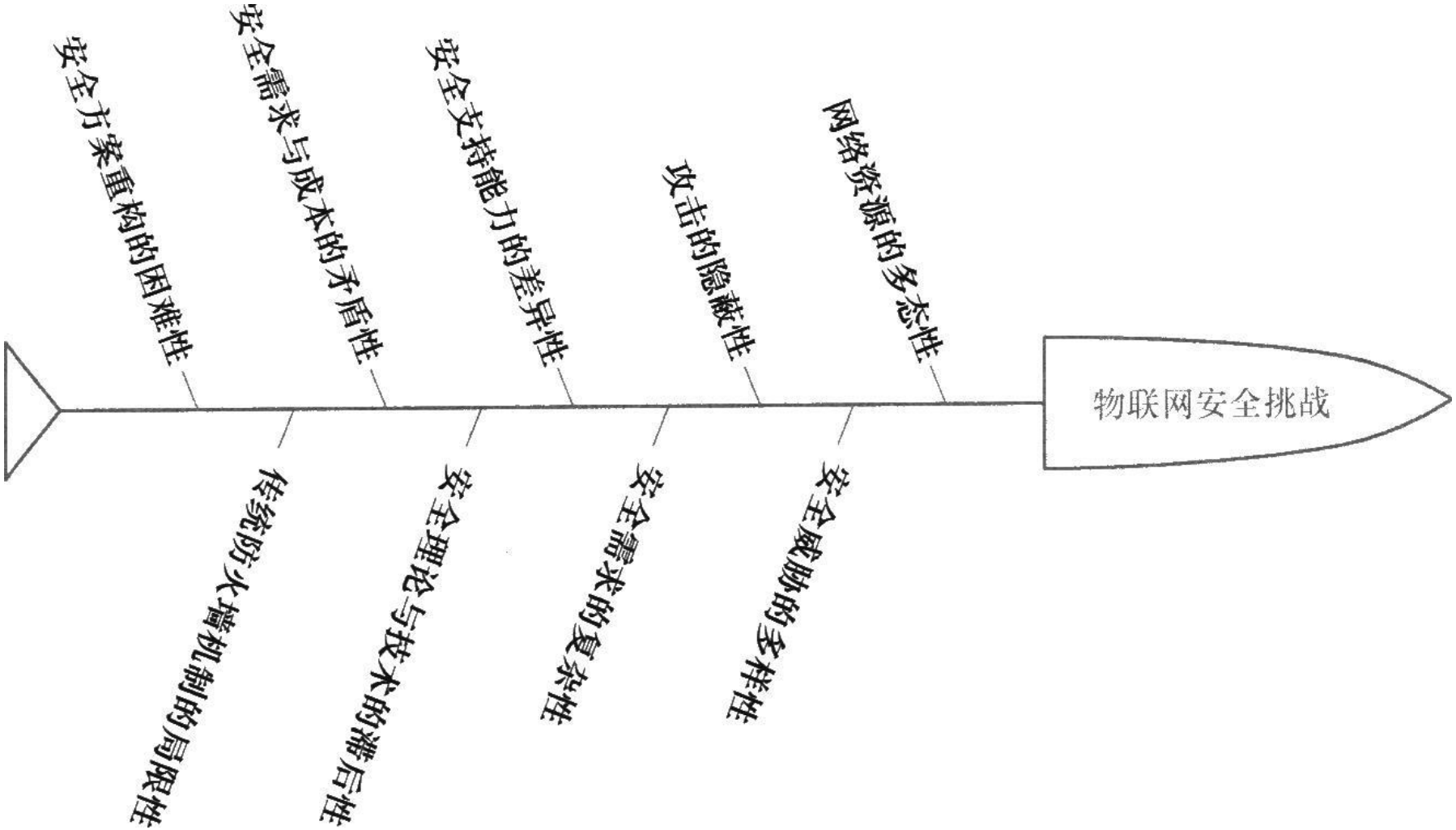
- **安全通信网络：**主要包括链路安全（物理链路专用或链路逻辑隔离）、传输安全（加密控制、消息认证或数字签名）。

- **安全管理中心：**主要包括业务与系统管理（业务准入与接入控制）、入侵检测、违规检查、EPC取证、安全管理（授权、审计、异常报警）。

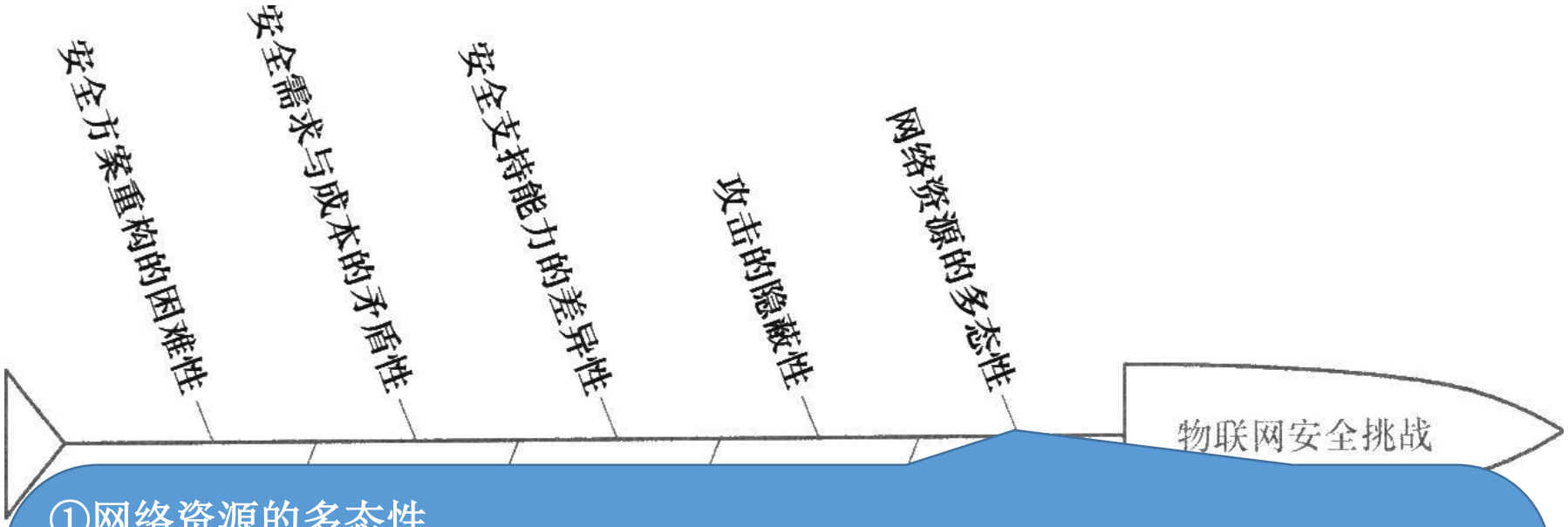
- **应急响应恢复与处置：**主要包括容灾备份、故障恢复、数据恢复与销毁、安全事件处理与分析、应急机制。

6.物联网安全挑战

- 物联网比一般IT系统更容易受到侵扰，面临着更严峻的安全问题。因为在传统互联网基础上发展起来的物联网实现了网络主体和网络形态的拓展，表现出网络组成的异构性、网络分布的广泛性、网络形态的多样性、感知信息和应用需求的多样性，以及网络的规模大、数据处理量多、决策控制复杂等特征。
- 一方面，感知层可自主实现信息感知，而传感器节点通常被部署在无人值守且物理攻击可以到达的区域；另一方面，网络覆盖国民经济、社会发展、人们生产生活的各个方面，故其影响比传统网络更加巨大。这些变化和新的约束条件对密钥建立、保密和认证、隐私、拒绝服务攻击的鲁棒性、安全路由选择及节点俘获提出了新的研究难点，给物联网安全方案的构建带来了困难。



物联网安全面临的9个主要挑战

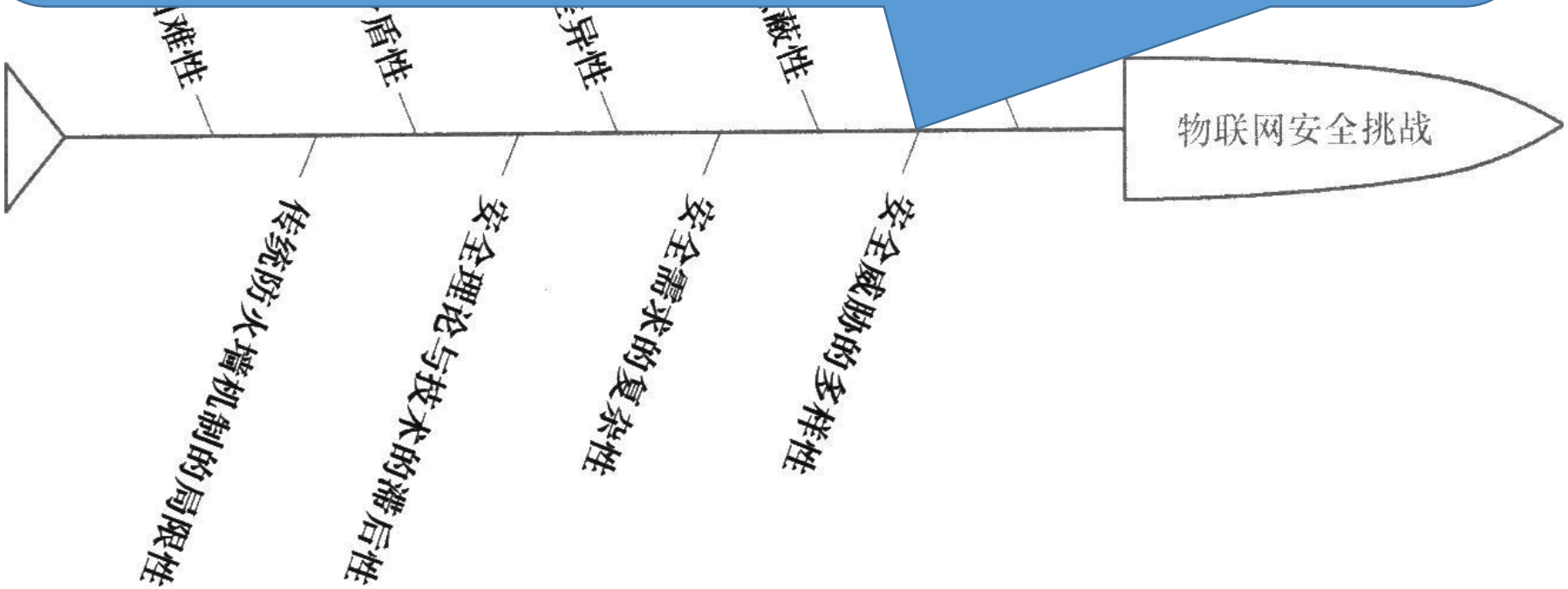


①网络资源的多态性

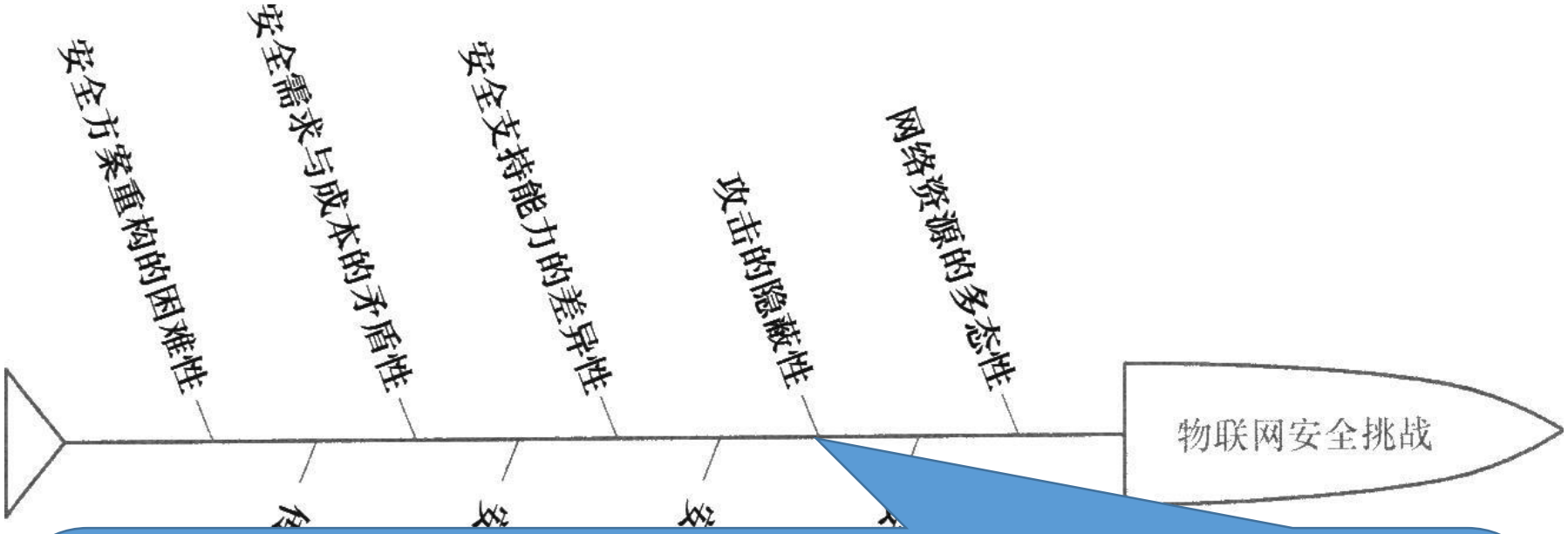
物联网中的资源表现出多态性，如网络组成可能涉及互联网、无线传感网、移动通信网、广播电视网等；四大类网络（有线长、短距离和无线长、短距离）相互连接组成的异构、多级、分布式网络导致统一的安全体系难以实现“桥接”和过渡；感知层中的传感器节点等在计算、存储、通信带宽和能量等方面表现出资源的有限性；网络中不同节点或设备间表现出资源和能力的差异性和非平衡性；网络中不同实体的加入或退出表现出不可预见的动态性，连接也可能时断时续。网络资源的这种多态性、异构性、有限性、差异性、动态性导致安全信息的传递和处理难以统一，使得构建统一的安全方案不再可行，“个性化”的安全方案是物联网安全的基本需求和一个重要特征。

②安全威胁的多样性

物联网组成复杂，对象多样，涉及的技术十分丰富；感知层、传输层和应用层承担的任务不同，所拥有的资源不同，蕴含的技术不同；且不同物联网应用对攻击者的吸引力也不一样。这些差异会导致攻击者在攻击手段和技术途径的选取上有所不同，从而形成不同的安全威胁方式，使得物联网面临的安全威胁具有多样性。如攻击者可以通过拒绝服务攻击严格限制物联网的价值；还有对无线通信链路进行窃听和篡改。



物联网安全面临的9个主要挑战

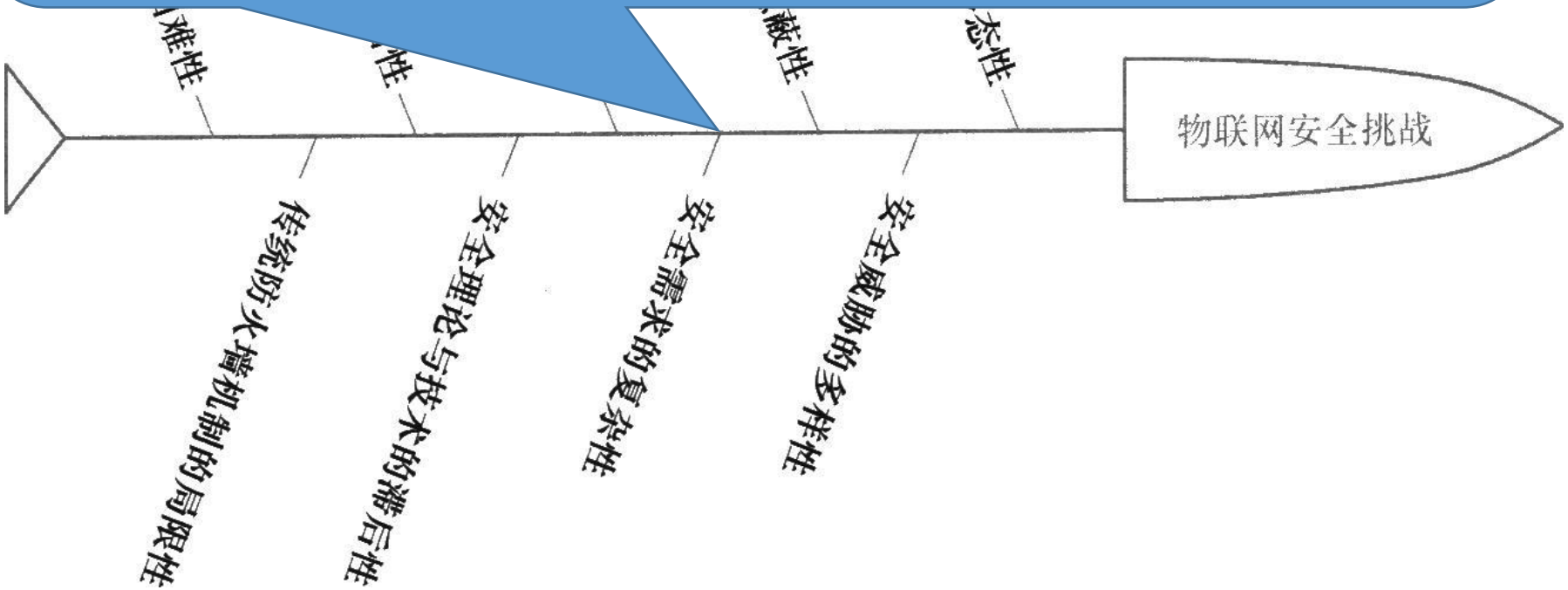


③攻击的隐蔽性

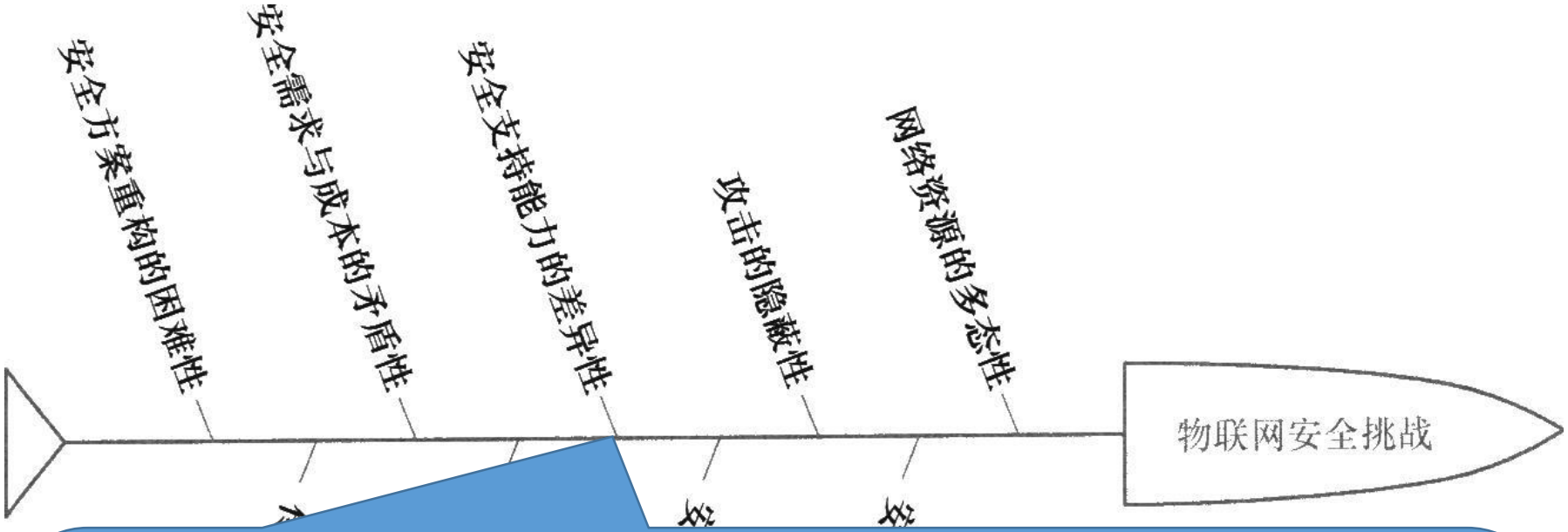
物联网中的信息获取技术不再局限于传统的窃听等技术，呈现出涵盖电、磁、声、光等多种物理信号，结合网络及通信技术的多元化特点，打破了物理隔离的障碍。攻击具有隐蔽性，表现为攻击目标的隐蔽性：被植入恶意代码或硬件的设备一般不影响其正常功能，很难通过常规方法进行检测；攻击时间的隐蔽性：攻击者可远程控制攻击发起时间，在攻击发起前，被攻击目标通常处于静默状态，传统的单次突发性检测不再有效；攻击过程的隐蔽性：为逃避无线信号检测，攻击信息传输过程采用隐蔽传输技术，现有无线信号检测设备尚不具备对这些新型通信技术的检测能力。因此，这就大大增加了攻击检测的难度。

④安全需求的复杂性

由于物联网面临的安全威胁多种多样，要应对这些威胁需要有不同的解决方案；且不同的物联网应用基于所属主体价值追求的偏好、成本投入能力的差异、面临的安全环境的不同，可能有不同的安全保护强度需要；在保证一个智能物体被数量庞大甚至未知的设备识别和接受的同时，又要同时保证其信息传递的安全性和隐私性。这些因素导致物联网安全需求的复杂性。



物联网安全面临的9个主要挑战

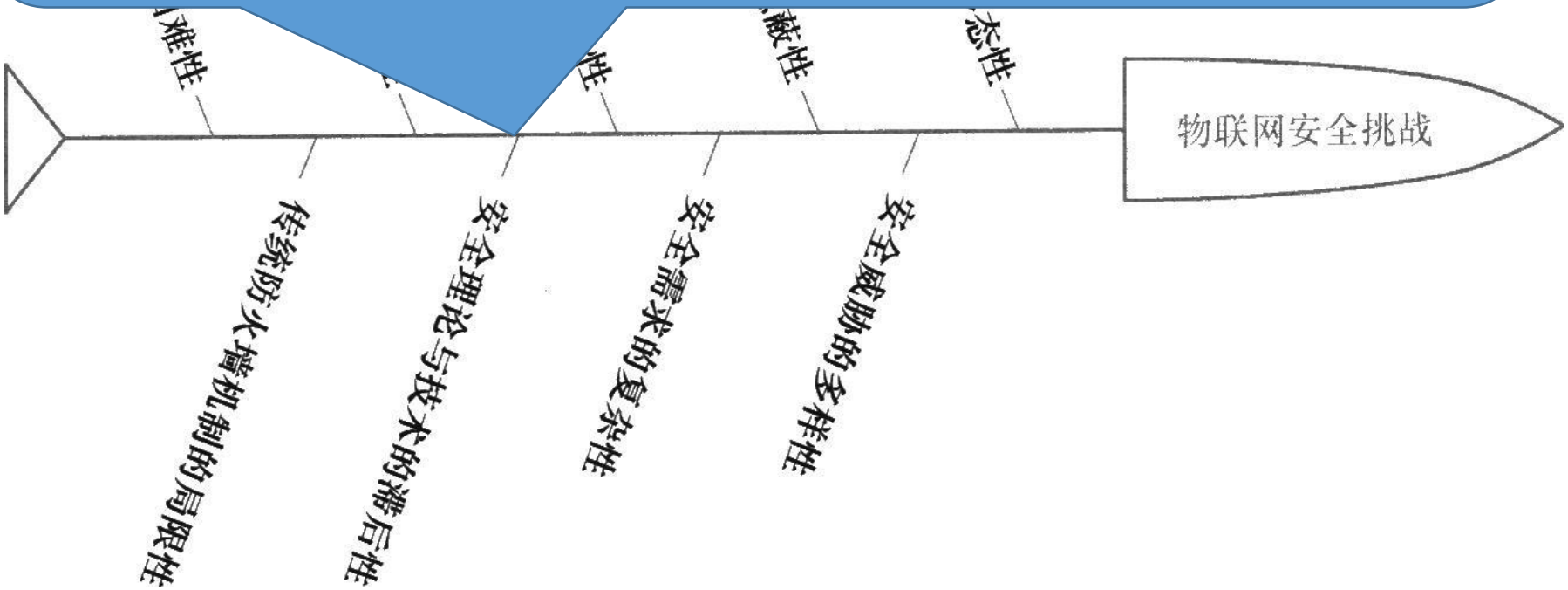


⑤安全支持能力的差异性

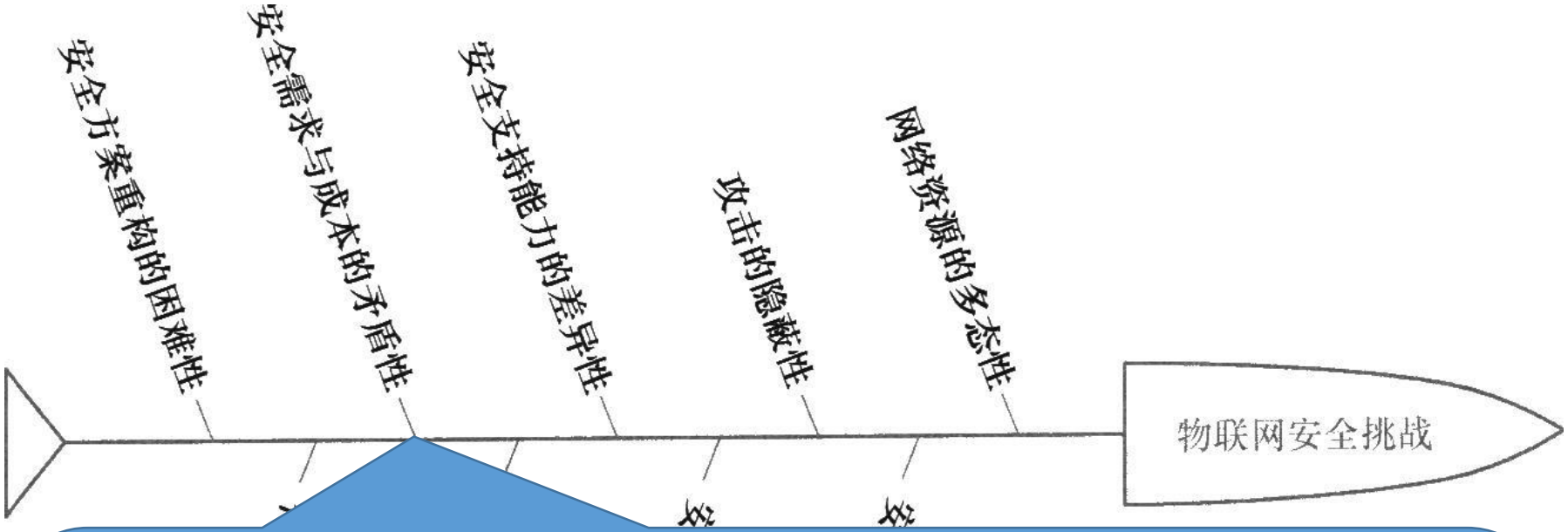
由于物联网中的资源具有多态性，这些资源在计算能力、存储能力和通信能力等方面不尽相同，甚至具有能量的不可补充性并影响节点的生命力，从而表现出对安全方案的承载能力和实施条件要求不同，以及安全支持能力的差异性。特别是物联网感知层的轻量级安全需求十分突出。

⑥安全理论与技术的滞后性

物联网作为一个刚出现十余年的新生事物，表现出不同于传统网络的一些新特征，其复杂程度远超现有网络，要确保这类网络的安全可靠，涉及新的安全理论和技术的应用。目前，针对物联网的安全理论与技术的研究才刚刚起步，还远远不能满足实际应用需要，表现出安全理论和技术的滞后性。



物联网安全面临的9个主要挑战

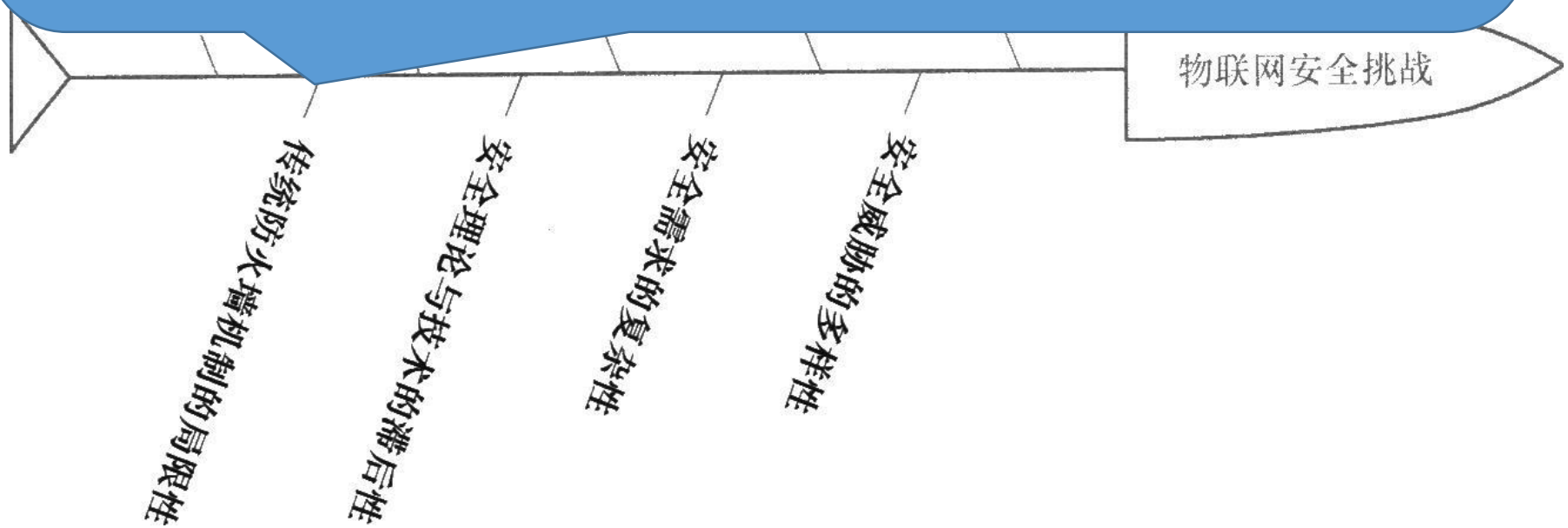


⑦安全需求与成本的矛盾性

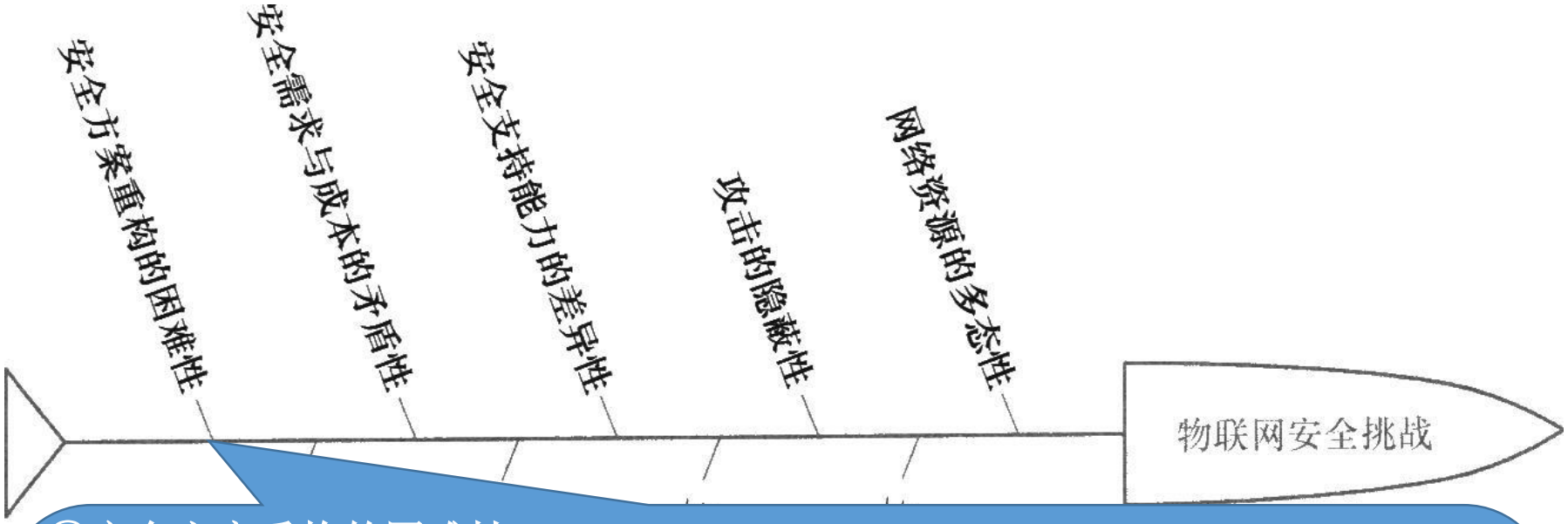
由于物联网不仅能够将“人”与“物”基于信息的纽带逻辑地联系在一起，而且还具有“物理”上的关联性，物联网既与人的身体健康和生命财产安全息息相关，又可能影响国家安全和社会稳定，**物联网集“平民化”与“高大上”于一体**，因此，安全对于物联网具有特别重大的意义，安全是物联网应用的核心需求，“没有安全就没有应用”。物联网安全方案的构建和实施离不开人、财、物的投入，而物联网潜在应用十分广泛、安全需求十分强劲，同时对应的成本投入将十分巨大，这是一对显而易见的矛盾。

⑧传统防火墙机制的局限性

配置防火墙机制是传统网络安全方案的一种基本思路，以此实现内外网的隔离和访问过滤。但物联网突破了传统网络的边界，物联网设备会彻底跳过防火墙建立与第三方服务的长期连接，有的甚至表面上都不为企业所知。如果物联网设备被盗用，大多数组织基本上不要指望能知道发生了什么。因为对物联网软件和硬件的内部工作机制的了解非常有限，大部分这些物联网设备都能给可危害单台设备的攻击者提供很大的能力，然后再逐步渗透到整个网络。如果网络没有正确保护或者分段的话，无论是视频、音频、环境或其他敏感信息，往往都可以通过入侵物联网设备盗取出去，可能还会为犯罪分子提供有价值的信息。**保护物联网最大的不同在于要跳出传统防火墙方案去思考，因为物联网意味着网络边界的模糊。**



物联网安全面临的9个主要挑战



⑨安全方案重构的困难性

物联网特有的安全问题可概括为如下几种：①略读(Skimming)：在末端设备或RFID持卡人不知情的情况下，信息被读取；②窃听(Eavesdropping)：在一个通信通道的中间，信息被中途窃取；③哄骗(Spoofing)：伪造复制设备数据，冒名输入到系统中；④克隆(Cloning)：克隆末端设备，冒名顶替；⑤破坏(Killing)：损坏或盗走末端设备；⑥拥塞(Jamming)：伪造数据，导致设备阻塞不可用；⑦屏蔽(Shielding)：用机械手段屏蔽电信号，让末端无法连接。

针对上述问题，传统网络中没有对应的安全解决方案，因此，需要针对物联网的特殊需求和问题进行安全方案的重构，这种重构意味着没有先例可供借鉴，在创新过程中将面临前所未有的困难。

7. 物联网安全现状与发展趋势

- **物联网安全现状**

(1)感知层的安全

- 感知层面临的威胁主要包括：RFID电子标签不受控制地被扫描、定位和追踪，导致隐私泄漏；智能感知节点的自身物理安全问题及继发性破坏；无线信号易被干扰；针对智能传感终端、RFID电子标签等的假冒攻击；缓冲区溢出、格式化字符串、输入验证、同步漏洞、信任漏洞等数据驱动攻击；蠕虫等恶意代码攻击；大量节点数据传输导致网络拥塞的DoS攻击等。
- 目前，对于感知层的安全威胁提出了一些相应的解决方案，很多借鉴了传统的信息安全防御策略。

1)加密机制

- 感知层的加密机制主要有两种类型：针对隐私加密和防恶意跟踪加密。
- 目前针对隐私加密的研究主要包括：美国MIT的Sarma等人提出基于哈希锁方法以及S．Weis等人进一步提出基于随机哈希锁进行隐私保护的方法。德国的Henrici等人提出基于杂凑的ID变化方法。
- 针对防恶意跟踪的研究主要包括：瑞士洛桑理工大学的M．Ohkubo教授提出基于哈希链的方法，A．Machanavajjhala等人提出一种在不损失统计正确性的情况下有效防止身份信息泄露的匿名化方法。

2)认证机制

- 认证使得通信的数据接收方能够确认数据发送方的真实身份，以及数据在传送过程中是否遭到篡改。
- 就物联网感知层而言，身份认证是确保节点的身份信息真实可信，并阻止非授权的用户窃取通信数据。
- Carlo Maria Medaglia等人提出在WSN中运用PKI方法来使得各个设备之间建立信任关系；Divyan M．Konidala等人提出在EPCglobal中使用相互认证机制来确保阅读器与标签(Tag)相互信任。

3)访问控制技术

- 物联网环境下的访问控制被拓展到在机器与机器之间进行访问授权，由于访问对象大量增加，其实现变得更加复杂。
- Carlo Maria Medaglia等人提出在WSN中每个节点上定义一个访问控制列表(Access Control List，ACL)，使得每个节点只接受其ACL中节点的信息而达到安全目的。Yong Ki Lee等人在分析现有国际标准和工业标准采用基于密码的访问控制方法的缺点基础上，提出一种EC-RAC(ECDLP based Randomized Access Control)的访问控制方法。

4)物理机制

- 主要是采用一些物理方法来保证设备的安全。
- Christoph P. Mayer等人提出使用杀死标签、法拉第罩以及使用阻塞标签等方法使得入侵者无法读取RFID电子标签的信息。
- Olivier Savry等人提出了使用RFID干扰信号使入侵者无法连接到正常的标签。

2. 网络层的安全

- 物联网的网络层依赖于传统的互联网，因此物联网面临传统网络的安全问题，例如病毒、木马、DDoS攻击、假冒、中间人攻击、跨异构网络攻击等传统互联网的网络安全问题。
- 物联网网络层的安全技术研究目前主要还是在传统的互联网安全方面，可以使用的技术有传统的认证技术、数据加密技术等。
- 网络层的安全机制可分为端到端机密性和节点到节点机密性。对于端到端机密性，需要建立端到端认证机制、端到端密钥协商机制、密钥管理机制和机密性算法选取机制等安全机制。在这些安全机制中，根据需要可以增加数据完整性服务。

对于节点到节点机密性，需要节点间的认证和密钥协商协议，这类协议要重点考虑效率因素。
机密性算法的选取和数据完整性服务则可以根据需求选取或省略。

考虑到跨网络架构的安全需求，应建立面向不同网络环境的认证衔接机制。

另外，**根据应用层的不同需求，网络传输模式可能区分为单播通信、组播通信和广播通信**，针对不同类型的通信模式有相应的认证机制和机密性保护机制。

3．应用层的安全

- 应用层面临的安全挑战主要表现为：如何针对不同权限的用户进行不同的访问控制；如何保护用户隐私信息；如何防止信息被泄露或跟踪；如何进行计算机取证等。
- **(1)访问控制技术**
- 访问控制是网络安全防范和保护的主要策略，它可以限制对关键资源的访问，防止非法用户的侵入或合法用户的越权操作所造成的破坏。Eberhard Grummt等人设计了一种专门用于描述大规模EPCIS（EPC Information Services，EPCglobal网络服务）事件中访问权限的上下文感知策略语言，并提出一种新的基于规则的访问协议，通过定义访问规则来限制用户访问权限，加强了信息的安全性。

(2)匿名签名与认证技术

- 匿名签名与认证技术是一种保护用户的身份和位置信息不被泄露的有效解决方案。Joaquin Garcia - Alfaro等人针对现有ONS服务中隐私泄漏的问题，实现了匿名的ONS查询服务，为解决ONS查询中的隐私信息泄漏问题提供了一种途径。
- 总之，整体上物联网安全的研究仍处于初始阶段，还没有形成一套完整、系统、标准化的解决方案，现有的许多方法离实际应用还有一定的距离，特别是传感器网络的资源局限性和多跳自组织网络环境下的大规模数据处理，使其安全问题的研究难度增大。

物联网安全发展趋势

安全是物联网得以进一步发展和推广应用的关键，没有安全保障为前提，物联网不可能得到大的发展，这是物联网未来发展的必然要求！

- 种种体验和现有信息网络平台的使用经验告诉人们物联网安全的重要性，但还没有谁能清楚说明物联网安全的整体规划、发展思路与技术路线。
- 到目前为止，能够满足物联网安全新挑战及体现物联网特点的安全技术还不成熟，物联网安全技术还将经过相当长一段时间的发展才可能走向相对完备，并在“攻”与“防”的对抗式发展过程中“螺旋式上升”，呈现出融合创新、跨学科综合、智能化集成、新技术涌现、安全标准体系的建立和安全技术模块化等趋势。

(1)融合创新

- 物联网尽管是新事物，但它并非凭空产生，可以认为物联网是传统互联网的拓展升级，物联网中蕴含着许多有关互联网的既有技术，同时，又引入了许多传统互联网未涉及的新技术。因此，物联网安全技术的发展一定不能抛开传统网络安全技术，应在相关网络安全技术融合的基础上，结合物联网的新特点和新需求，催生出某些新的安全技术，与原有网络安全技术相互配合，表现出融合创新的特点。
- 物联网的安全防护技术必然是针对不同攻击技术的应用，融合不同的安全技术来为用户提供较为完善的安全解决方案。物联网安全不但依赖单一安全技术自身的性能，还依赖于各种安全技术之间的协作所发挥的综合功效。

物联网安全技术融合创新发展趋势还表现为相关安全技术与物联网设备的融合。

因为物联网是一个与应用紧密相关的概念，不同的应用其安全的内涵不同，涉及的系统设备不同，实现安全的途径不同，要达成的安全目标也可能不同。因此，物联网安全具体化后，一定与应用相关联，物联网安全技术的融合创新离不开与物联网设备的结合。

如将物联网安全技术与安全策略置入物联网的路由器、终端等网络设备中，并**采用集成化管理软件，可能引入的安全机制包括防火墙、入侵检测、流量分析与监控、内容过滤等**，形成与应用需求相对应的、完备的、一体化的网络安全体系，避免安全与应用相分享、安全设备与网络设备不协调。

(2) 跨学科综合

- 物联网的产生源于通信、计算机、网络、感知和控制等多学科交叉融合，涉及信息的获取、传输、处理及应用等完整信息链。物联网安全方案的提供自然离不开跨学科综合，特别是近年来行为学、心理学、经济学等在信息安全领域的应用，产生了信息（或网络）安全行为学、网络心理学、信息安全经济学等新的学科分支，丰富了物联网安全方案的内容和设计思路。比如，分析物联网环境下攻击者的行为特征、行为模式和行为规律，以及产生攻击行为的原因、攻击行为的影响、影响攻击行为的因素等，有助于遏制攻击行为对物联网安全的危害。

类似地，从经济活动的视角考察信息安全，以信息安全活动的经济规律为研究对象，分析物联网安全活动的效益规律和安全事故的损失规律，有助于提升物联网安全方案的经济性；

网络心理学研究有助于准确分析攻击者实施攻击行为的心理动机和心理需求，为制定有针对性的物联网安全防护方案提供源于网络心理学方面的指导，也为引导用户正确使用网络、合法利用网上资源和有效管理网络提供帮助。

(3)智能化集成

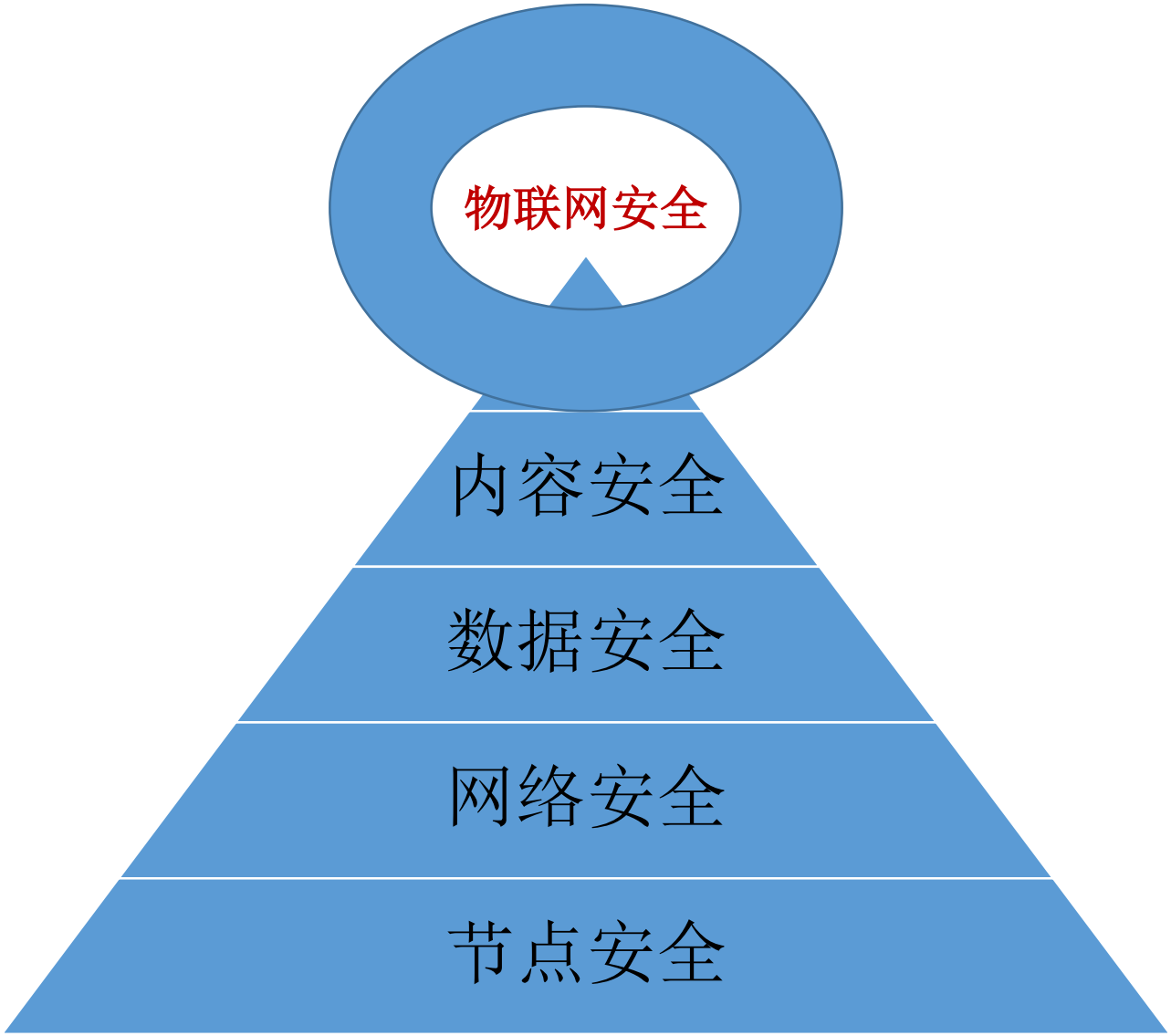
- 物联网本质上是一个多学科交叉融合的复杂巨系统，物联网面临的安全威胁和面对的安全问题错综复杂，传统的安全技术串联、并联或混合运用及静态的安全解决方案对物联网整体的安全保障很难再取得满意的效果。一种可行的途径就是提高物联网安全防护系统的智能化水平，通过人工智能技术的运用，将现有成熟的安全技术和一些适合物联网应用环境的新安全技术集成起来，并**具有自适应的动态安全状态感知与应对能力**。人工智能作为一种模仿高级智能的推理和运算技术，具有推理、逻辑判断、思考和学习等功能，人工智能技术所具有的许多特殊能力可以使其成为物联网安全管理最强有力的支持工具。

(4)新技术涌现

- 随着时间的推移，任何事物都是发展变化的，作为复杂巨系统（复杂网络）的物联网也不例外。物联网本身在发展，资源越来越丰富、组成越来越异构、实体越来越多元、技术越来越庞杂，具有无穷包容性的物联网在“攻”“防”对抗过程中，按照“问题牵引”的动态应对模式，会不断推陈出新地发展出前所未有的安全技术，新的物联网安全技术将在层出不穷的关联技术支撑下不断涌现，用以确保物联网安全。
- 如**节点安全基因化技术、量子密码技术、轻量级密码算法与安全协议技术、微功率安全无线通信技术、数字水印技术、生物识别技术、自动取证技术、可信计算技术、信誉评估技术、智能拦截技术、故障隔离技术、容错容侵技术**等都可能取得新的进展并在未来的物联网安全领域实现广泛的应用。

5．安全标准体系的建立和安全技术模块化

- 物联网安全是一个复杂的概念，物联网安全问题因应用而不同，不同的安全服务提供商提供的安全解决方案通常不一样，一个复杂的物联网也不太可能由单一的安全服务提供商提供全部的安全解决方案。为了快速高效地构建起物联网特定安全问题的解决方案，当安全解决方案需要更新时能够快速高效地找到替代方案，物联网安全标准体系的建立和物联网安全技术模块化是必由之路。
- “模块化”的思路是物联网安全方案实现与维护的最佳选择。模块化的前提是标准化，只有形成统一的安全技术规范、统一的安全模块标准，才能更好地对各个物联网安全服务提供商进行规范，来自于不同服务提供商的模块才可能相互对接和兼容，才可能避免已有投资的浪费、市场的混乱和产业的垄断等。


物联网安全
内容安全
数据安全
网络安全
节点安全