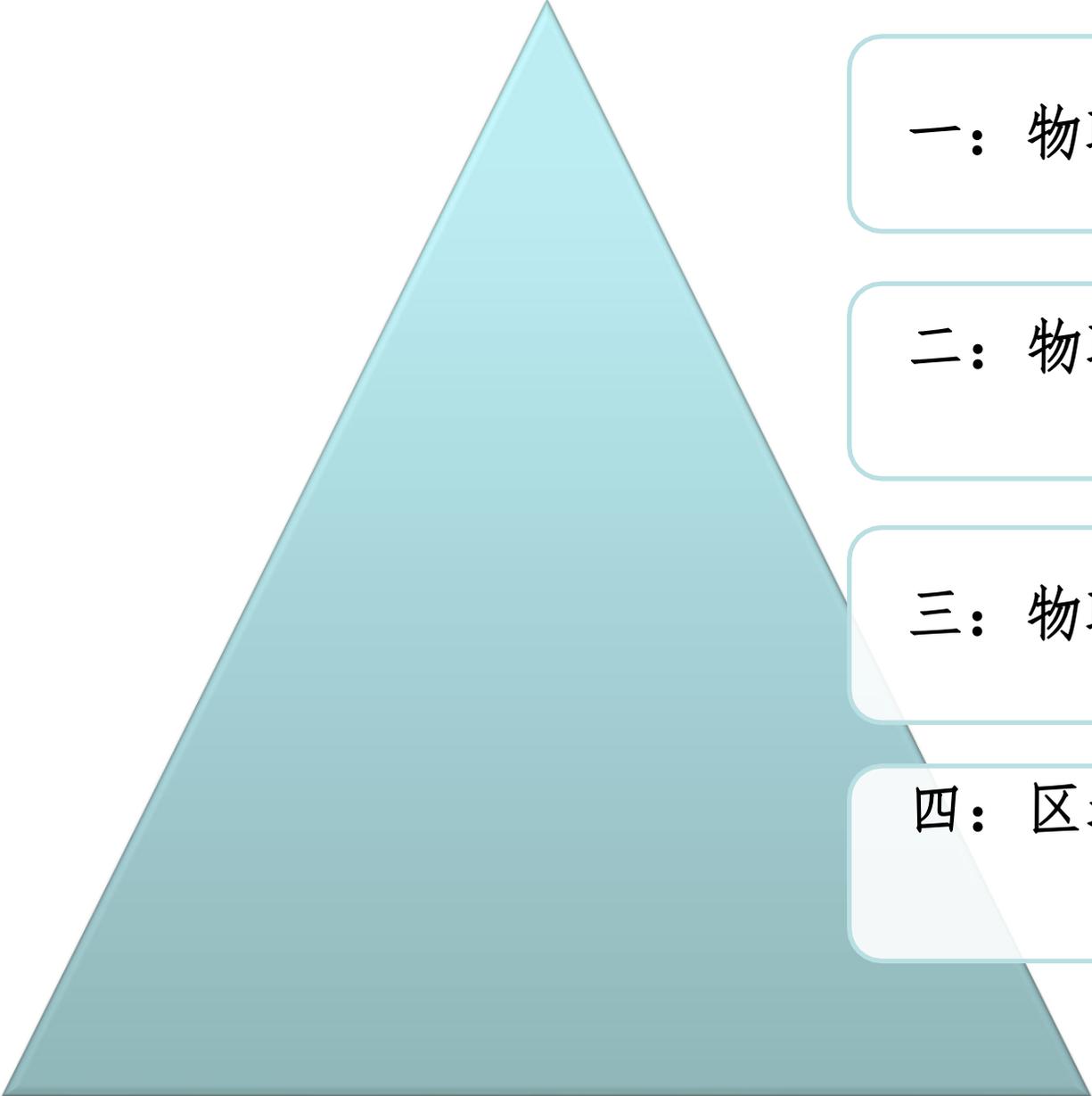


物联网安全技术-导论

物联网的安全与隐私保护问题直接关系到物联网服务能否得到真正的实际推广应用，物联网安全问题已成为热点。在本章中分析了物联网安全特征和面临的安全威胁，讨论了物联网安全的体系架构、物联网安全管理和一些安全关键技术，如密钥管理、安全路由、隐私保护、认证与访问控制等。同时，也探讨了基于IPv6的物联网的安全问题，以及安全管理。

| 知识要点 | 能力要求 |
|-----------------|--|
| 物联网安全概述 | <ol style="list-style-type: none"> 1 了解物联网的安全特征 2 理解物联网安全威胁 3 了解物联网安全体系结构 |
| 物联网安全关键技术 | 掌握本章中物联网安全的关键技术 |
| 基于IPv6的物联网的安全技术 | <ol style="list-style-type: none"> 1 了解IPv6协议引入带来的安全需求 2 掌握安全技术 |
| 物联网的安全管理 | 了解物联网安全管理以及引入IPv6后物联网安全管理 |
| 区块链技术与物联网安全 | <ol style="list-style-type: none"> 1 了解区块链技术特性 2 理解基于区块链技术的物联网安全保护 |



一：物联网的安全概述

二：物联网的安全关键技术

三：物联网的安全管理

四：区块链技术与物联网安全

一：物联网的安全概述

(1) 大众化

(3) 非对称

物联网安全特征

(2) 轻量级

(4) 复杂性



物联网安全体系结构

感知层安全威胁

感知层普遍的安全威胁是某些普通节点被攻击者控制之后，其与关键节点交互的所有信息都将被攻击者获取。攻击者的目的除了窃听信息外，还可能通过其控制的感知节点发出错误信息，从而影响系统的正常运行。

网络层安全威胁

网络层很可能面临非授权节点非法接入的问题。互联网或者下一代网络将是物联网网络层的核心载体，互联网遇到的各种攻击仍然存在。

应用层安全威胁

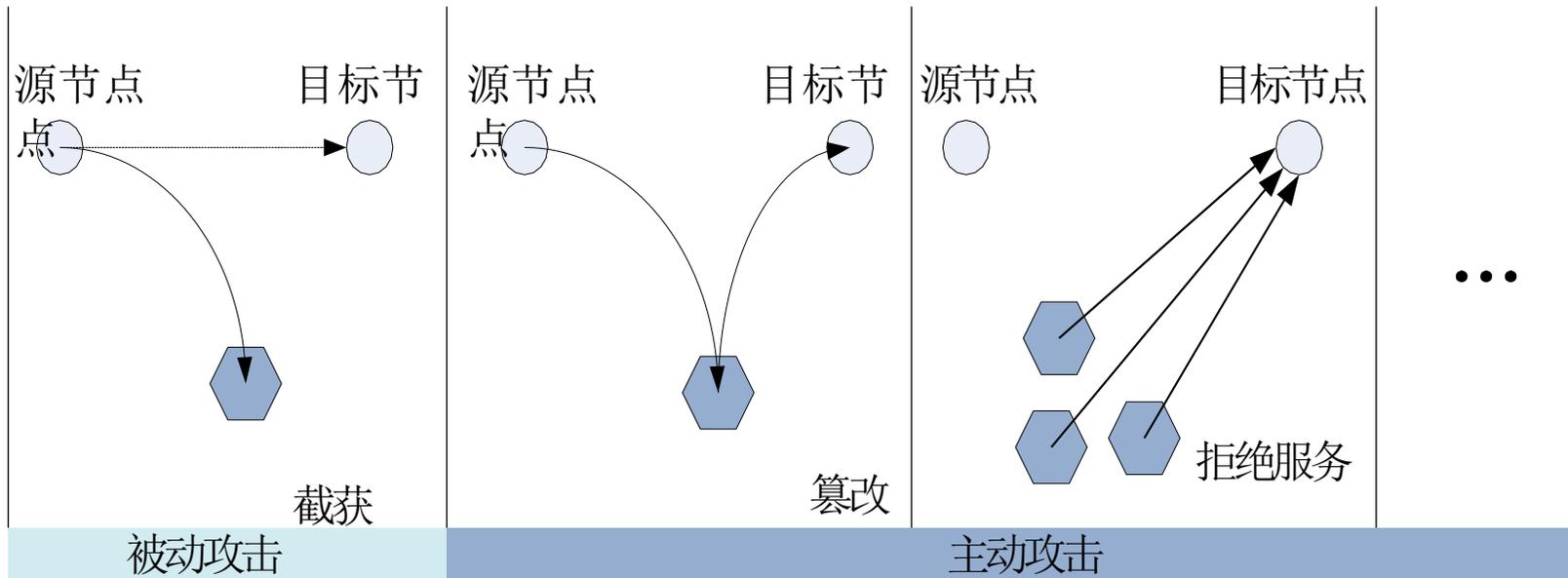
云计算等新兴技术的使用会给攻击者提供截取、篡改数据的机会，同时会利用软件系统的漏洞、缺陷，并对密钥进行破解，达到非法访问数据库系统的目的，造成重大损失。

物联网面临的安全威胁

目前，物联网的通信面临着以下两大类安全威胁，即**被动攻击**和**主动攻击**。

被动攻击：

攻击者从物联网通信网络上窃听正常节点间的通信内容的这种攻击方式称为截获。在被动攻击中，攻击者只是观察和分析某个协议数据单元PDU而不干扰信息流。即使这些数据对攻击者来说是不易理解的，它也可以通过观察PDU的协议控制信息部分，来了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换的数据的某种性质。这种攻击又称为流量分析。



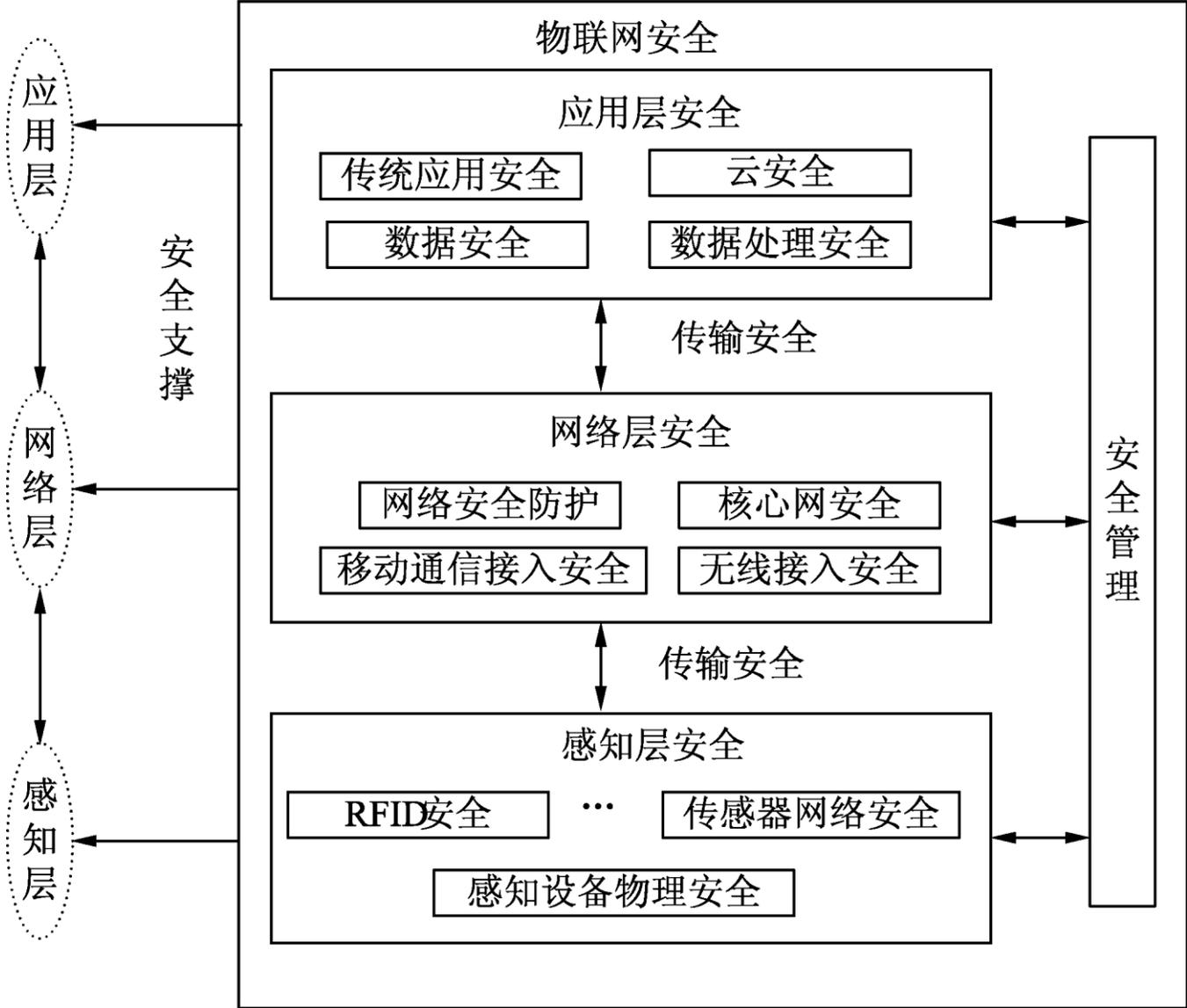
物联网面临的安全威胁

主动攻击：

主动攻击方式较多，下面列举2种常见的主动攻击方式。

- ① **篡改**：攻击者故意篡改正常节点间传送的报文。这里包括彻底中断传送的报文，甚至把完全伪造的报文传送给目标节点。这种攻击方式也称为“更改报文流”。
- ② **拒绝服务Dos (Denial of Service)**：攻击者向目标节点发送大量分组，导致目标节点一直处于“忙”状态而无法完成与正常节点的通信。Dos攻击将会耗尽节点电量以及占用带宽资源，使系统运行变得缓慢甚至无法继续工作。

物联网安全体系结构



物联网安全架构

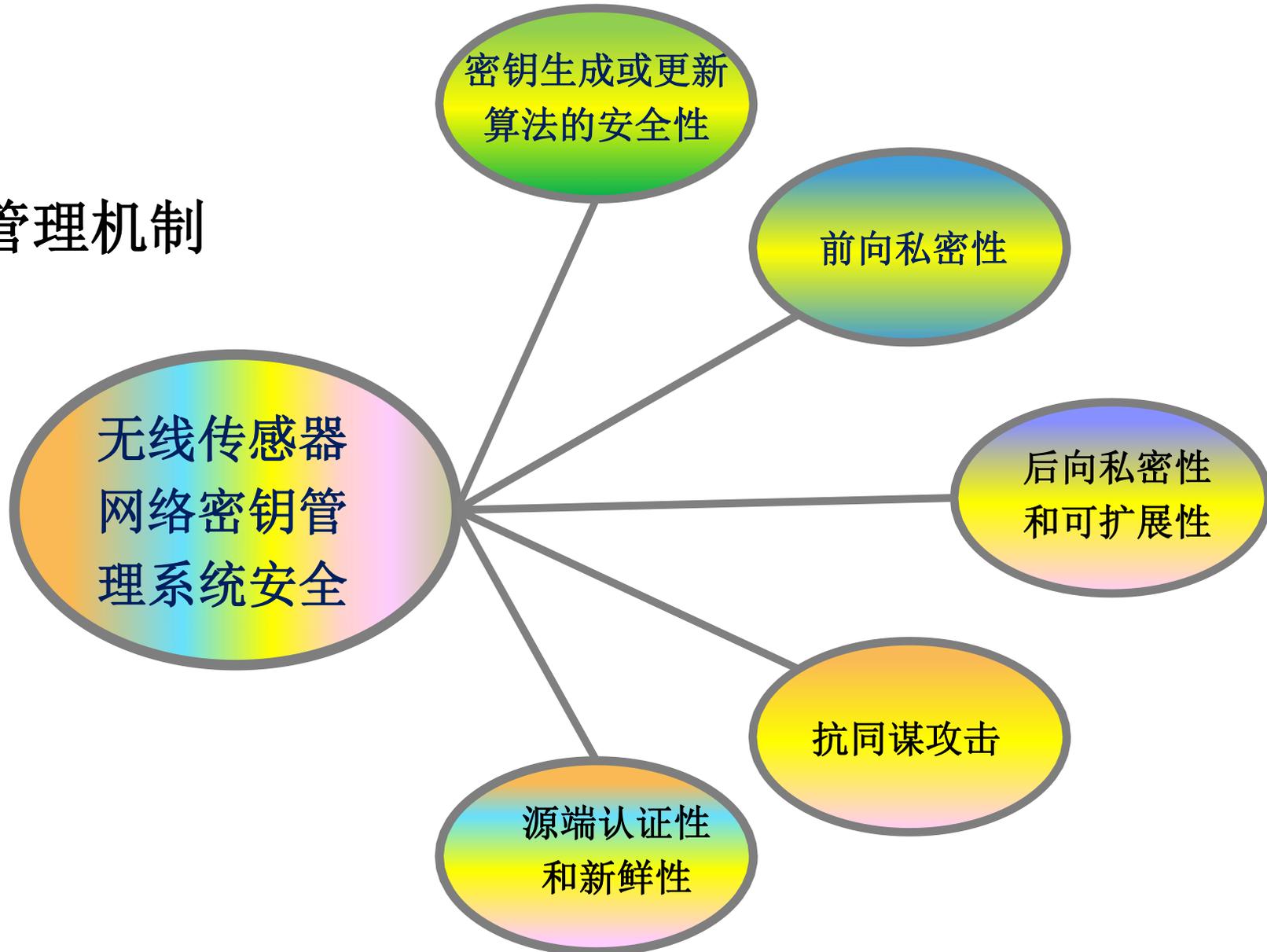
感知层安全主要分为设备物理安全和信息安全两类。

网络层安全主要包括网络安全防护、核心网安全、移动通信接入安全和无线接入安全等。

应用层安全除了传统的应用安全之外，还需要加强处理安全、数据安全和云安全。因此应用层需要一个强大而统一的安全管理平台。

二：物联网的安全关键技术

密钥管理机制

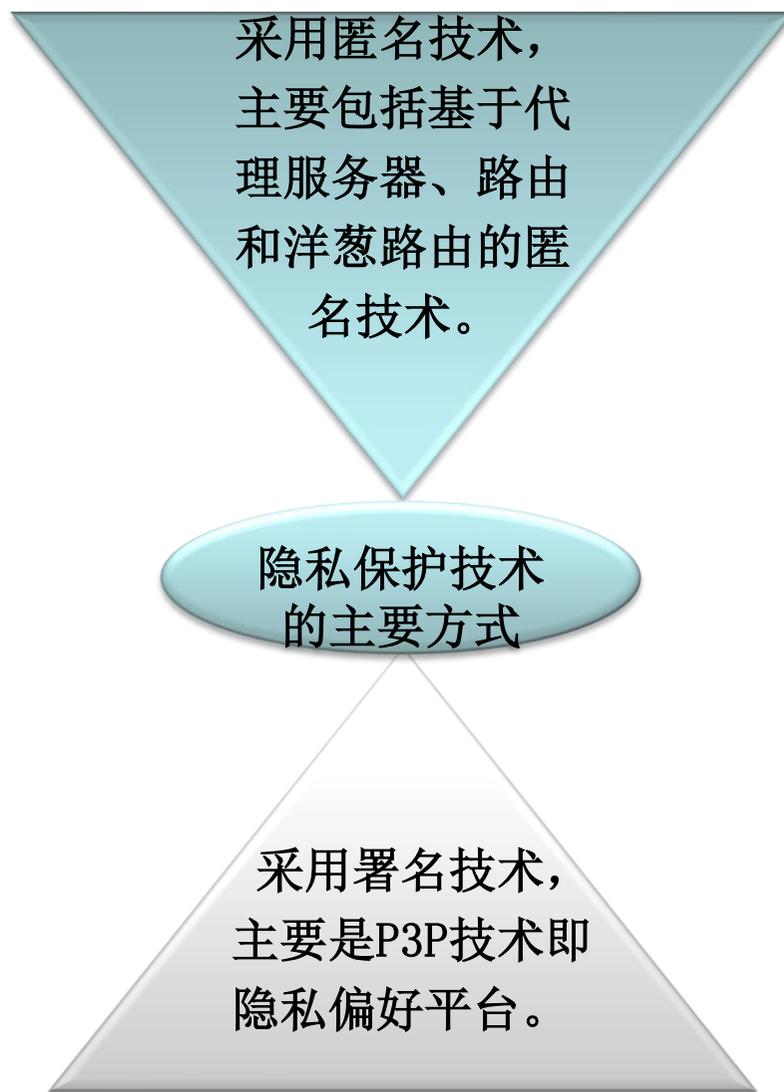


物联网的安全关键技术

在密钥管理系统的实现方法中，人们提出了基于**对称密钥系统**的方法和基于**非对称密钥系统**的方法。在基于对称密钥的管理系统方面，从分配方式上也可分为以下三类：**基于密钥分配中心方式、预分配方式和基于分组分簇方式**。

典型的解决方法有**SPINS协议**、基于密钥池预分配方式的**E-G方法**和**q-Composite方法**、单密钥空间随机密钥预分配方法、多密钥空间随机密钥预分配方法、对称多项式随机密钥预分配方法、基于地理信息或部署信息的随机密钥预分配方法、低能耗的密钥管理方法等。与非对称密钥系统相比，对称密钥系统在计算复杂度方面具有优势，但在密钥管理和安全性方面却有不足。例如邻居节点间的认证难于实现，节点的加入和退出不够灵活等。特别是在物联网环境下，如何实现与其他网络的密钥管理系统的融合是值得探讨的问题。为此，人们将非对称密钥系统也应用于无线传感器网络。近几年作为非对称密钥系统的基于身份标识的加密算法（**Identity-Based Encryption, IBE**）引起了人们的关注。该算法的主要思想是加密的公钥不需要从公钥证书中获得，而是直接使用标识用户身份的字符串。最初提出这种基于身份标识加密算法的动机是为了简化电子邮件系统中证书的管理。

数据处理与隐私性



安全路由

无线传感器网络路由协议常受到的攻击主要有以下几类：
虚假路由信息攻击、选择性转发攻击、污水池攻击、女巫攻击、虫洞攻击、Hello洪泛攻击、确认攻击等。

| 攻击类型 | 解决方法 |
|------------|-----------------------------|
| 外部攻击和链路层攻击 | 链路层加密认证 |
| 女巫攻击 | 身份认证 |
| HELLO洪泛攻击 | 双向链路认证 |
| 虫洞和污水池 | 很难防御，必须在设计路由协议时考虑，如基于地理位置路由 |
| 选择性转发攻击 | 多径路由技术 |
| 认证广播和洪泛 | 广播认证 |

认证与访问控制

网络中的认证主要包括身份认证和消息认证

身份认证可以使通信双方确信对方的身份并交换会话密钥。

消息认证中主要是接收方希望能够保证其接收的消息确实来自真正的发送方。

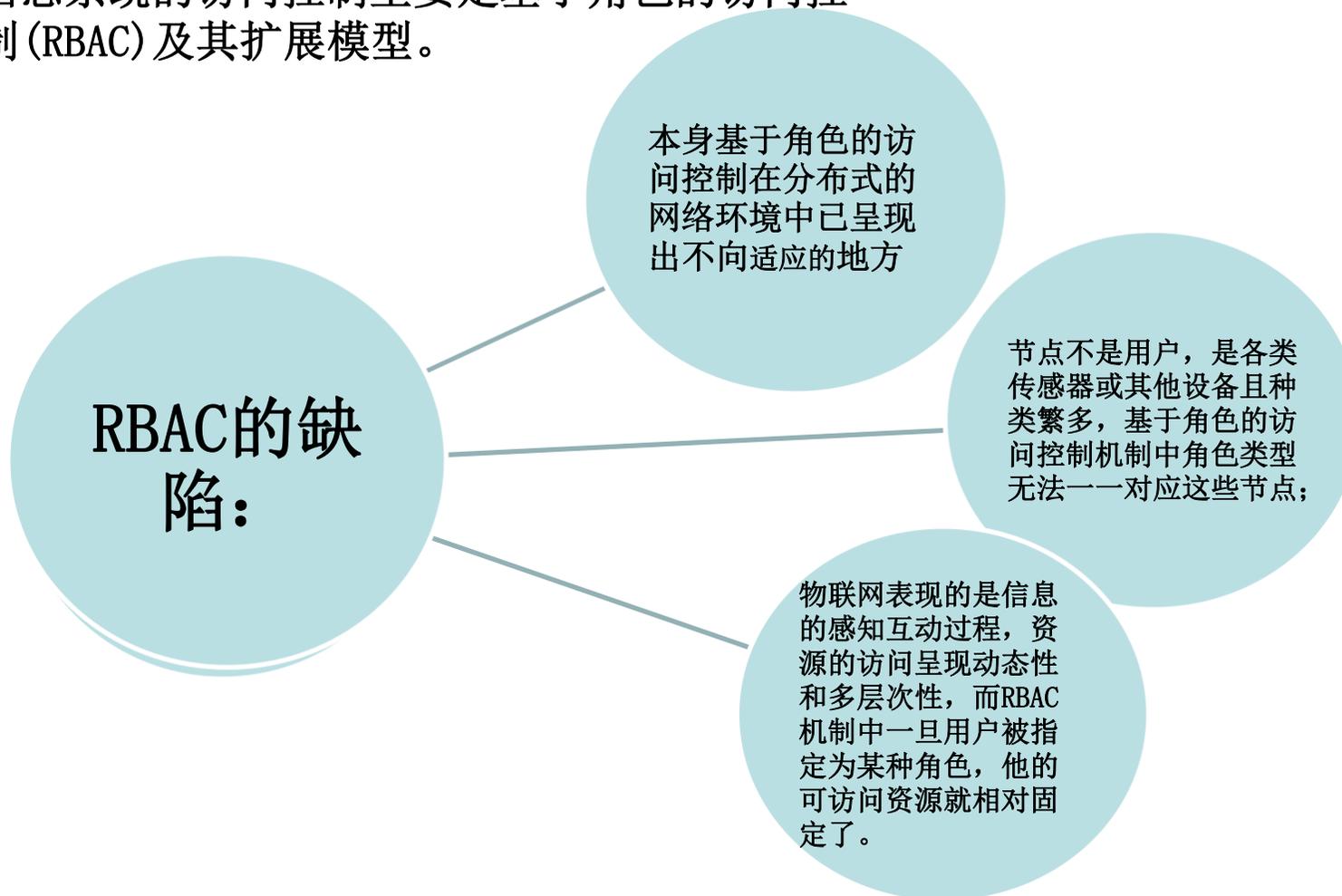
在物联网中，业务应用与网络通信紧紧地绑在一起，认证有其特殊性。

基于单向散列函数的认证方法。

基于轻量级公钥算法的认证技术。

基于预共享密钥的认证技术。

访问控制是对用户合法使用资源的认证和控制，目前信息系统的访问控制主要是基于角色的访问控制机制 (RBAC) 及其扩展模型。



基于属性的访问控制 (ABAC) 是近几年研究的热点，ABAC方法的问题是对较少的属性来说，加密解密的效率较高。目前有两个发展方向：基于密钥策略和基于密文策略。

恶意代码防御

恶意代码防御可采用基于现有网络中的恶意代码防御机制，并结合分层防御的思想，从而加强物联网中的恶意代码防御能力。

1. 分层防御的思想，即在传感器网络层或M2M终端部署入侵检测机制检测异常流量及恶意代码，以便从源头控制恶意代码的复制和传播；
2. 传感器网关可作为防御机制中的第二层控制节点，负责恶意代码、异常流量的简单分析和上报处理；
3. 核心网为恶意代码防御服务器作为恶意代码防御机制的第三层防御控制节点，负责恶意代码的分析、处理。

入侵检测与容侵容错技术

分布式入侵检测通过设置自治Agent（代理人）：入侵检测 Agent（IDA）、通信服务Agent（TSA）和状态检查Agent（SDA）来实现对网络数据的入侵检测。

容侵就是指在网络中存在恶意入侵的情况下，网络仍然能够正常地运行。现阶段物联网的容侵容错技术主要体现为无线传感器网络的容侵容错技术。

基于IPv6物联网的安全技术

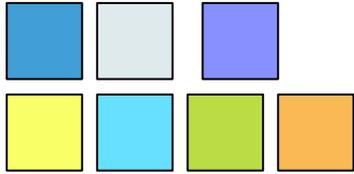
无线传感器网络在引入IPv6协议以后，给传感网带来了新的安全问题：

(1)IPv6网络层数据传输安全问题及需求分析。

①IPv6网络中的IPSec（网络协议安全性）安全关联，需要六次以上的消息交互，且密钥协商采用非对称ECDH算法，开销大幅增加；

②ESP同时满足加密和认证，需要采用IPSec的ESP报头，但是ESP报头的长度至少为10字节（传感网应用），报文负载太大。

③IPSec作为IPv6网络强制的数据安全机制，传感网中一对多的保密性和完整性无法通过IPSec的加密和校验来完成。



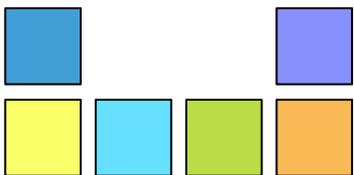
(2)IPv6路由安全问题及需求分析。

RPL路由协议中，Rank的主要功能是创建最优的网络拓扑，避免环路和管理控制开销。攻击节点可以通过篡改自己的Rank值在攻击者附近构建一个sinkhole，吸引周围节点向其发送数据。

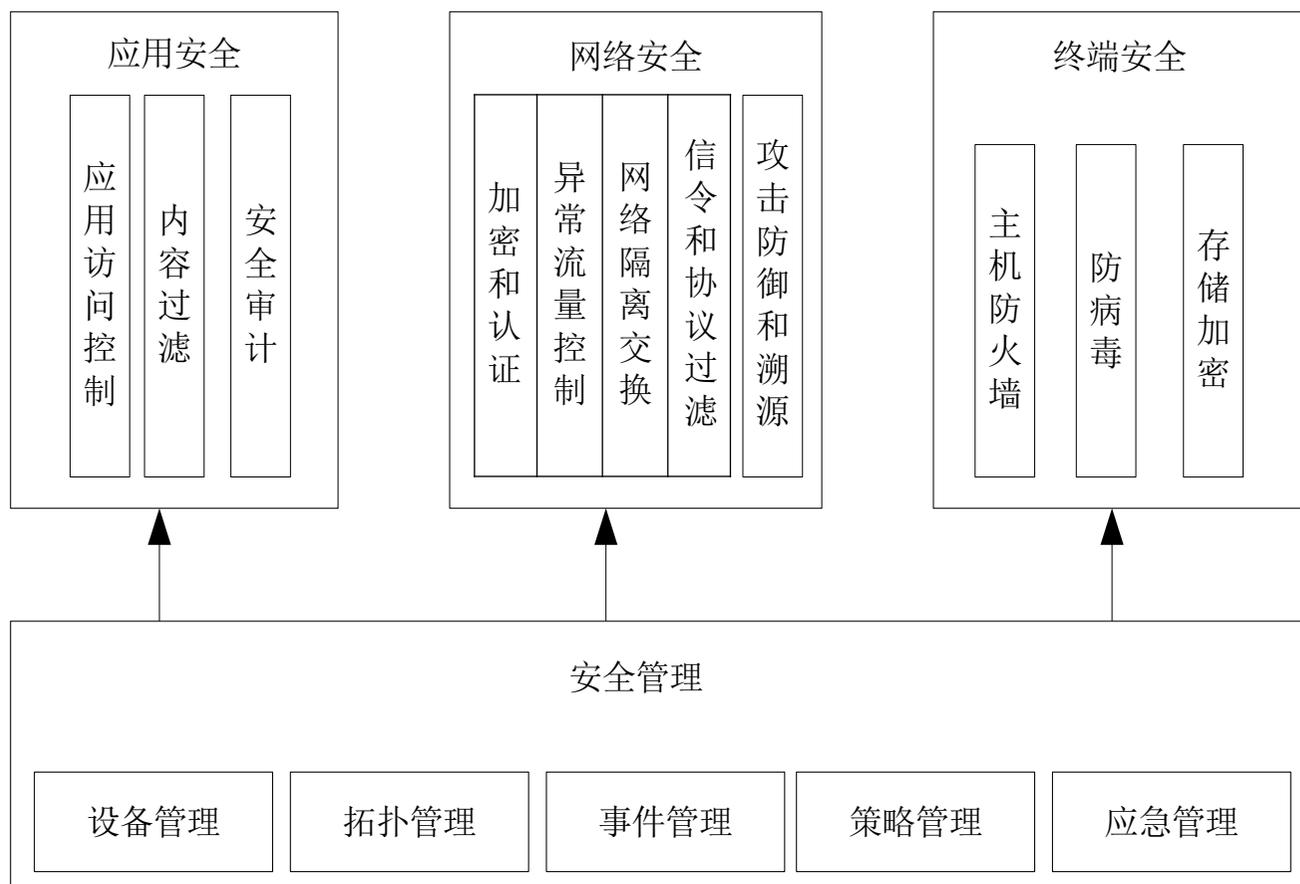
(3)互联互通系统安全问题及需求分析

①非法Internet访问用户随意的访问传感器网络，不采取认证机制对访问用户进行身份认证，将造成传感器网络网络管理中心的崩溃，同时传感器网络大量的私密信息遭到泄露。

②合法Internet访问用户，如果没有合理的方案控制其访问规则，大量的访问操作将对传感器网络网络管理带来负担，也造成传感器网络敏感信息的泄漏，无法保障高机密性信息的安全性。

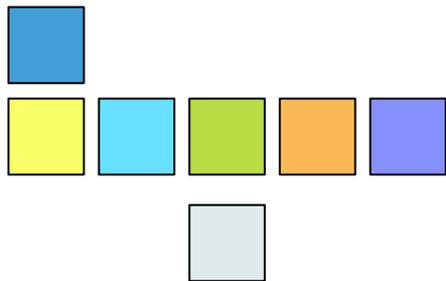


三：物联网的安全管理



具体来讲，安全管理包括设备管理、拓扑管理、事件管理、策略管理和应急管理。





IPv6传感网的安全管理

节点身份鉴别

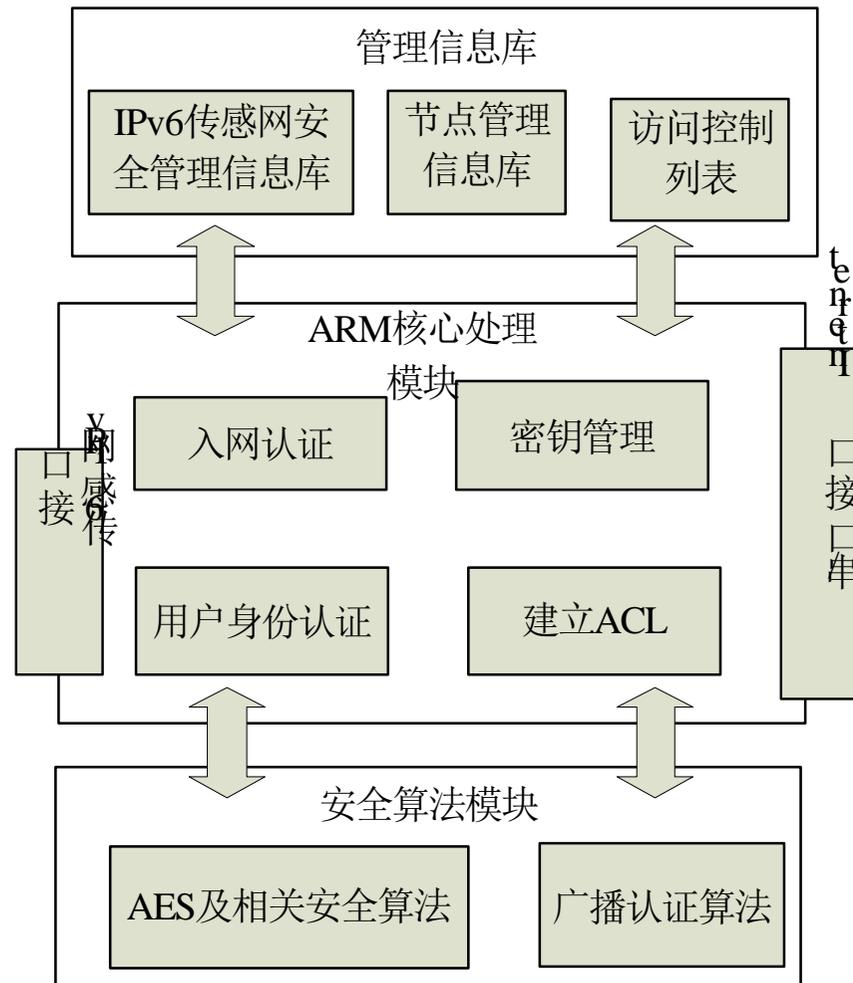
密钥管理

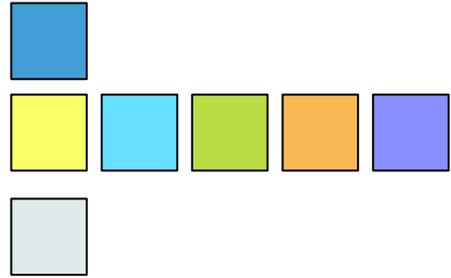
访问控制

访问控制列表

安全管理信息库

网关安全管理使用IPv6传感网接口和Internet用户接口对传感网数据和Internet用户访问信息进行处理，其功能结构如下图所示。





安全管理者由管理信息库、核心处理模块和安全算法模块构成。

①管理信息库完成数据存储功能

②核心处理模块传感网接口和用户接口分别处理IPv6传感网和转发用户信息。

③安全算法模块集成标准IPSec SAD库、轻量级IPSec采用的轻量级密码算法和AES加解密等安全算法。

四：区块链技术与物联网安全

区块链技术

区块链技术 (Blockchain technology) 是一种记录交易数据的计算机数据库，它并非是一项新技术，而是一个新的技术组合。其关键技术包括P2P动态组网、基于密码学的共享账本、共识机制、智能合约等技术。区块链原本是比特币等加密货币存储数据的一种独特方式，用来存储大量交易信息，每条记录信息按照时间顺序链接起来，并以密码学方式保证交易信息不可篡改和不可伪造，因此具备公开透明、无法篡改、方便追溯的特点。

四：区块链技术与物联网安全

区块链技术

区块链是一种共享的分布式数据库技术。主要包括4个技术特性：去中心化，去信任，集体维护，可靠数据库。

1 去中心化。众多节点组成端到端的网络形成了一个区块链，因此在区块链中不存在中心化的设备和管理机构，这些数据信息存储在所有节点中，而不是存储在唯一的中心化机构。任一节点停止工作都不会影响系统整体的运作。去中心化弥补了传统中心设备集中管理而容易招致攻击的缺陷。

2 去信任。系统中所有节点之间通过数字签名技术和哈希算法进行验证，只要按照系统既定的规则进行交易，不需要节点信任，节点之间不能也无法欺骗其它节点。

四：区块链技术与物联网安全

区块链技术

- 3 集体维护。所有具有维护功能的节点参与系统维护。
- 4 可靠数据库。在区块链中，相邻的两个区块利用密码学与每一笔交易相串联，因此可以通过这种方式追溯每一笔交易记录；系统中每个节点都有完整的数据库拷贝，所以单个节点或者数个节点对数据库的更改并不会引起系统数据库的更改。

四：区块链技术与物联网安全

区块链技术

从架构设计上来说，区块链可以简单的分为三个层次，基础网络层，协议层、和应用层。其中，它们相互独立但又不可分割。

(1) 基础网络层。主要有数据层和网络层组成。数据层中主要有4个核心技术：区块 + 链，哈希函数，Merkle树，非对称加密算法。网络层主要实现去中心化，包含P2P网络。

① 区块 + 链。区块是一种记录交易的数据结构，反映了一笔交易的资金流向，完成了交易的区块则会形成主链。一个区块包含：交易信息、前一个区块形成的哈希散列、随机数。区块结构主要有区块头和区块体组成。

四：区块链技术与物联网安全

区块链技术

交易信息：包括交易双方的私钥、交易的数量、电子货币的数字签名。

前一个区块形成的哈希散列：用来将区块连接起来，实现交易的顺序排列。

随机数：所有矿工节点竞争计算随机数的答案，最快得到答案的节点生成一个新的区块，并广播到所有节点进行更新，如此完成一笔交易。
如图9-7 区块+链结构。

② 哈希函数。基于密码学的单向哈希函数，用 $y = \text{hash}(x)$ 的方式进行表示。易被验证，但却很难破解。实现将任意长度的资料经由Hash算法转换为一组固定长度的代码。

四：区块链技术与物联网安全

区块链技术

③ Merkle树。也称为哈希二叉树，其主要功能是用于校验大规模数据的完整性。Merkle树归纳所有交易信息并生成统一的哈希值，若区块中任意一交易信息被更改都会使得Merkle树改变。

④ 非对称加密算法。密钥产生器产生一对密钥，公钥是向外公开的，并且发送方用公钥对原信息加密，只有接收方用自己的私钥才能解密，保证了数据不被窃取。若用私钥进行数字签名，则只有公钥才能验证数据是由私钥持有者所发出，因此具有不可抵赖性。

四：区块链技术与物联网安全

区块链技术

⑤ P2P网络。实现点对点的技术交流，而不经中心服务器。因此P2P网络具有无需中心服务器介入的去中心化、容错性高，健壮性好的特点。

四：区块链技术与物联网安全

区块链技术

(2) 中间协议层。中间协议层由共识层、激励层、合约层组成。

① 位于共识层的共识机制。为了所有节点能够达成对于一笔交易的共识，包括交易记录的有效性，真实性，因此需要利用共识机制来实现。目前主要有四大类共识机制：PoW（Proof of work工作量证明）、PoS（Proof of Stake，权益证明）、DPoS（Delegated Proof-Of-Stake，股份授权证明）和分布式一致性算法。

② 位于激励层的发行机制和激励机制。如比特币系统会根据新建的区块奖励矿工，但根据时间规则每四年奖励会减半，所以比特币总量固定而不会继续增加。

四：区块链技术与物联网安全

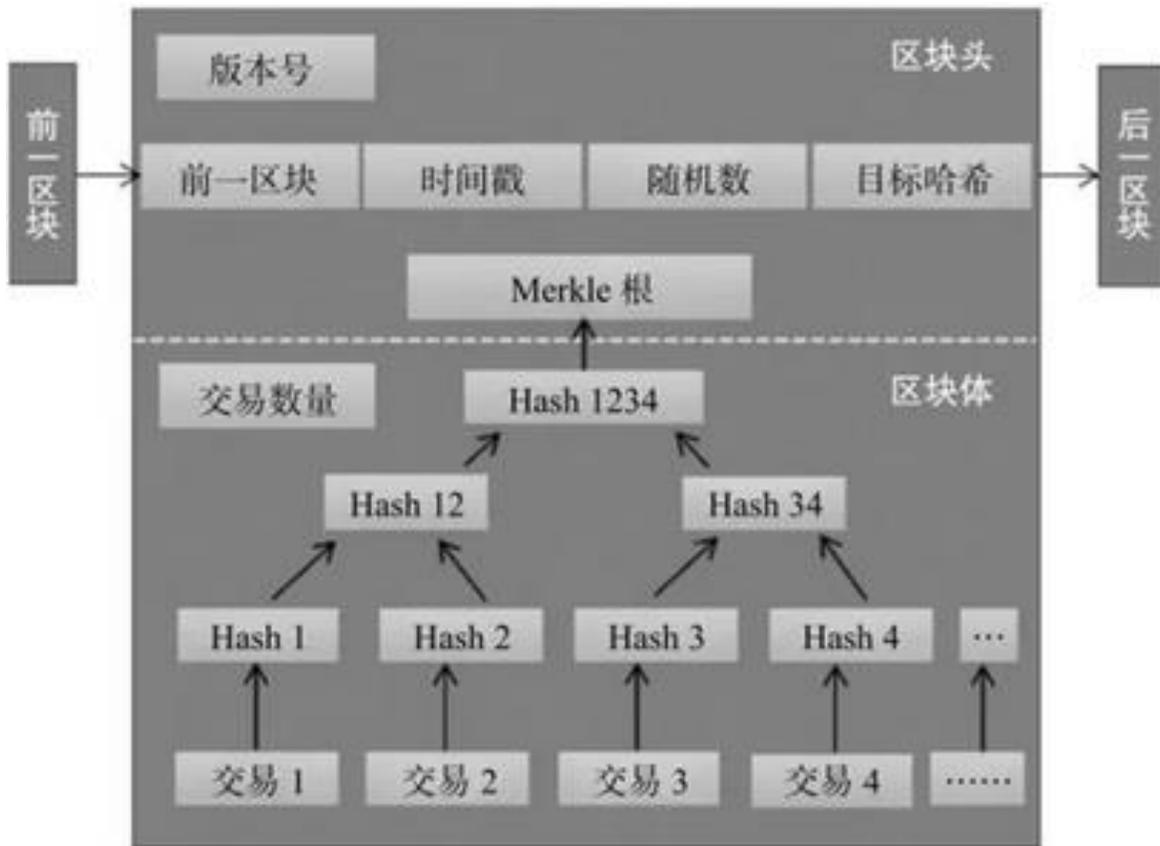
区块链技术

③ 位于合约层的智能合约。智能合约是一组规则和逻辑选择。各方签署了智能合约，并通过代码的形式附着在区块数据上，再经由P2P传递。当满足了智能合约的触发要求，则区块链激活并执行智能合约内容。

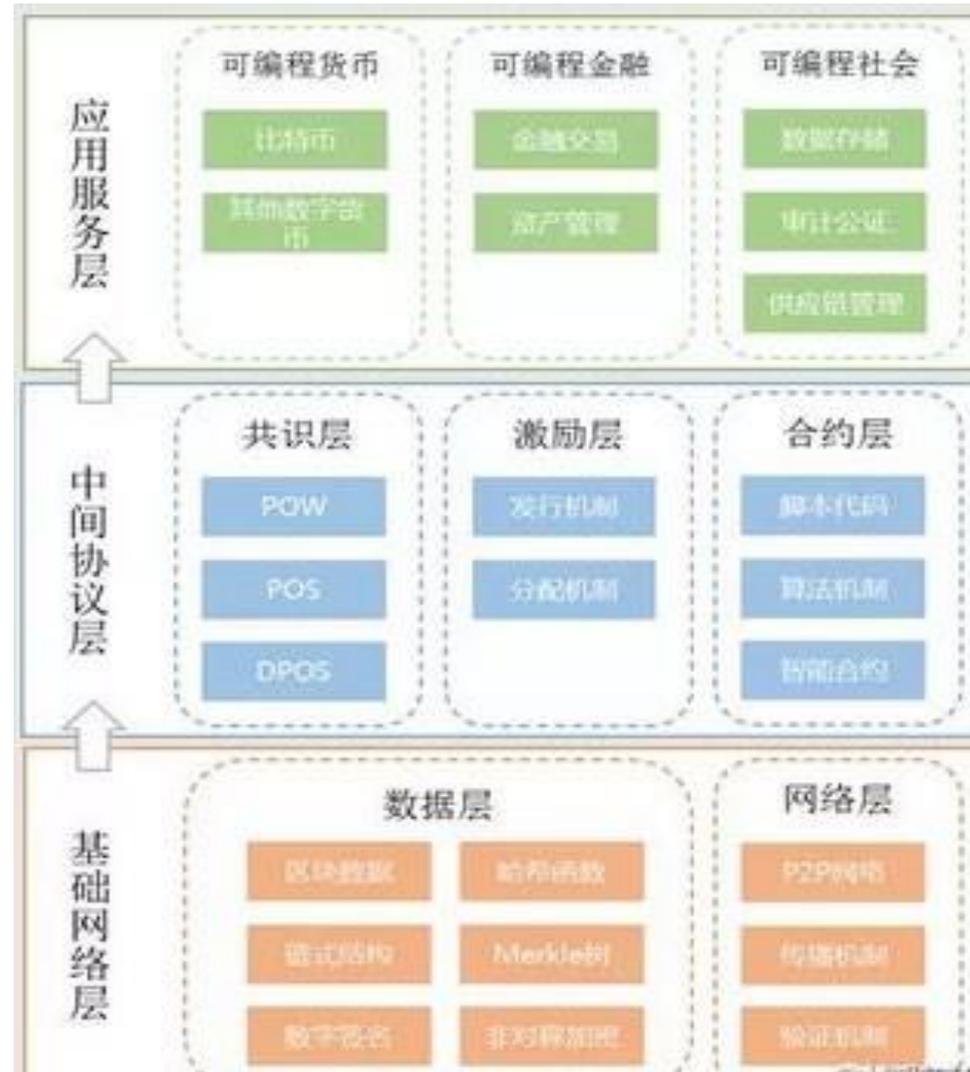
(3) 应用层。应用服务层作为区块链产业链中最重要的一环，则包括区块链的各种应用场景和案例，包括可编程货币、可编程金融和可编程社会。

四：区块链技术与物联网安全

区块链技术



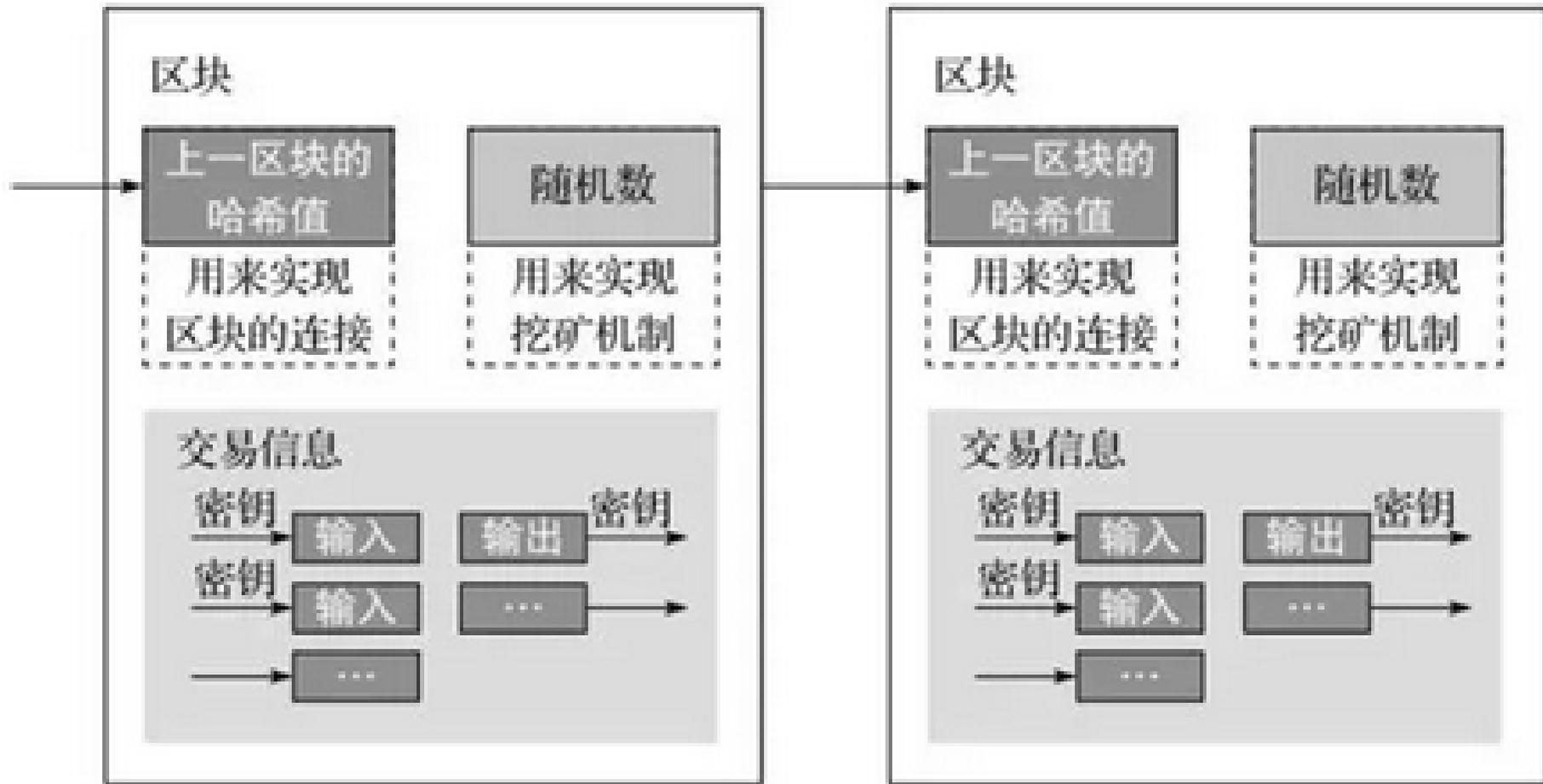
区块结构



区块链架构图

四：区块链技术与物联网安全

区块链技术



区块+链结构

四：区块链技术与物联网安全

利用区块链保障物联网安全

区块链与物联网具有许多相似的地方，如区块链与物联网都具有去中心化的特点。区块链系统网络是典型的 P2P 网络，而物联网的拓扑结构也属于分布式，两者的网络特性决定了物联网可以利用区块链技术在网络安全的优势，为物联网安全问题提供解决途径；区块链系统通过智能合约来进行智能化执行，而在物联网应用中，可以利用区块链的智能合约来实现目前的物联网应用如智能家居，智能交通等等；在保证安全方面，物联网可以利用区块链的非对称加密算法，实现信息加密和数字签名，利用私钥加密信息，公钥解密验证信息来源的真实性。

四：区块链技术与物联网安全

利用区块链保障物联网安全

随着物联网设备数量的增长，传统的中心化设备的管理与数据处理容易招致物联网安全攻击，而基于区块链的物联网安全模式将得以改善。

物联网设备鉴权。在新的物联网设备接入网的时候，需要向接入平台和网络设备节点发送接入请求和设备鉴权。此时物联网利用区块链中的非对称加密算法以及P2P网络，实现无需额外建设第三方平台和设备而直接进行新设备入网和身份验证的功能。

物联网共识网络。为了数据的安全和隐私保护，利用区块链的共识验证机制。部署特定节点进行工作量证明验证，保证在物联网环境下智能设备节点不承担数据计算工作等，而只是对数据进行加密和传输，并把数据传输作为区块链交易向整个网络广播。

四：区块链技术与物联网安全

利用区块链保障物联网安全

设备追踪。利用区块链技术可以通过记录用户和设备之间的数据账本，物联网系统就可以跟踪单个设备并能够查找其历史记录。通过设备追踪，实时了解设备的使用状态，一旦出现异常，立即响应，能够最大限度地保护设备安全，从而保证整个物联网网络的安全。

Thank

you!

