第 1 章　物联网工程概要

1.1　概　　要

本章概述以无线传感器网络（Wireless Sensor Networks，WSNs）为核心载体的物联网（Internet of Things）工程的基本概念和支撑技术。重点介绍基于 ZigBee 标准的无线传感器网络技术特征及网络架构，使读者了解物联网基本体系构架、重要支撑技术和广阔的应用前景。

1.2　物联网概念与基本特征

1．物联网概念

进入 21 世纪以来，随着传感器技术、微机电技术、嵌入式计算技术、分布式信息处理技术和无线通信技术的快速发展，信息系统从传统的人工合成单信道模式转变为人工生成和自动生成的双信道模式，并实现信息系统与物理系统的相互融合，表现为信息虚拟世界与物理实体世界的交互作用，使得物理世界可以被全面感知和智慧操控；同时，以传感器、射频模块和智能识别终端为代表的信息自动生成设备和射频通信设备联网，共同构成了实时准确地感知、测量和监控物理世界的硬件支撑平台。从而在以上系统融合和硬件支撑的基础上，信息世界的扩展需求和物理世界的联网需求，共同催生了一类新型网络——物联网（Internet of Things，IoT）。物联网是新一代信息技术的重要组成部分，顾名思义，“物联网就是物物相联的互联网”。这有两层含义：第一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信。IoT 通过无线传感器网络（Wireless Sensor Networks，WSNs）、射频识别（Radio Frequency Identification，RFID）等信息传感设备，按约定的协议，把任何物品与互联网连接起来进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理等具体工程应用。

物联网将逻辑上的信息世界与客观上的物理世界融合在一起，成为改变人类与自然界交互方式的信息感知、采集和传输领域的一场革命，极大地扩展了现有网络的功能和人类认识世界的能力。作为物联网的核心载体，WSNs 是信息获取、信息传输与信息处理三大子领域技术相互融合的产物，具有数据中心、自组织、多跳路由、动态拓扑、密分布集等特点，代表了更小、更廉价的低功耗计算设备的“后 PC 时代”。目前世界上大约有 60 亿个具有通信能力的微处理器和微控制器，且该数字还在不断攀升，同时网络终端和接入技术的触角不断延伸到人类生产和生活的各方面，并成为物联网感知物理世界的“神经末梢”。物联网通过 WSNs 这个核心载体，将物与物的智慧互联技术及人类感知自然界的水平提高到一个革命性的崭新阶段，其通过智慧感知、射频通信、识别技术与普适计算、泛在网络的融合应用，被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。物联网工程的应用目的是实现物与物、物与人，以及所有的物品与网络的连接，方便识别、管理和控制。目前，物联网涉及的工程领域越来越广，已经融入了工业制造领域、互联网及移动通信等传统 IT 领域。可寻址、可通信、可控制、数字化、信息化、网络化、泛在化与开放模式正逐渐成为物联网发展的演进目标。物联

网的众多优势，使其在军事侦察、环境科学、医疗卫生、工业自动化、商业应用及地质灾害的预测等领域具有广泛的应用前景，表 1-2-1 所示为其中的典型应用领域。

表 1-2-1 物联网的典型应用领域

领域		用途
军事		兵力和装备的监控、战场情况实时监视和评估、目标定位、情报获取等功能；战场情况监视和占领区的侦察等；协助智能弹药对目标的攻击以及战场破坏情况的评估；核武器、生物武器的成分以及攻击后的监测和侦察等
环境		监视农作物灌溉情况、土壤情况、空气情况；大面积的地表监测和行星探测；气象和地理研究；地质灾害监测；生物环境的研究；森林火灾的监测等
医疗		通过传感器节点可对病人的心跳速率、血压等进行实时检测，提供对人体状况远程监控与诊断；用于医院里的药品管理，对药品种类进行分类、辨识药品等
家居及城市管理	智能家居	通过布置于房间内的温度、湿度、光照、空气成分等无线传感器，感知居室不同部分的微观状况，从而对家庭环境进行自动控制，提供智慧、舒适的居住环境
	桥梁建筑安全	通过布置于建筑物内的图像、声音、气体检测、温度、压力、辐射等传感器，发现异常事件及时报警，自动启动应急措施
工业自动化		大型设备的监控
反恐和公共安全		通过特殊用途的传感器如生物化学传感器，监测有害物、危险物的信息，准确判定生化物质的成分以及泄漏源位置，可用于反恐袭击，提高对突发事件的应变能力

物联网的基本概念可以从多重角度加以理解。表 1-2-2 分别从技术理解、应用理解、狭义理解和泛在理解的角度来定义物联网。

表 1-2-2 物联网多角度定义

技术理解	应用理解	狭义理解	泛在理解
关键词：智能网络	关键词：服务应用	关键词：物物相联	关键词：融合架构
综合运用传感器、微机电、嵌入式计算、分布式信息处理和无线通信等技术，将物体的信息通过传输网络到达指定的信息处理中心，最终实现物与物、人与物之间的自动化信息交互与处理的智能网络	架构在网络基础上的应用层面的各种服务的总和。为用户提供生产、生活的远程监控、指挥调度、采集测量、智能识别、定位跟踪等方面的应用服务，达到以更加精细和动态的方式管理生产和生活的目标	通过无线射频识别、感应设备、定位系统等技术手段和载体，按约定的协议把世界上所有的物体都连接起来，并与现有的“互联网”结合，实现人类社会与物理世界的普遍联系	联系各类物理基础设施与信息功能的融合体系。将物联网理解为一种基于多类型网络和基础设施，进行联网应用、通信交流和信息处理的融合体系架构，而非一个物理上独立存在的实体网络

2．物联网基本特征

从物联网定义的技术理解角度来看，物联网和传统的互联网相比有其自身鲜明的特征。物联网的基本特征可概括为全面感知、可靠传输和智能处理。

（1）全面感知。物联网广泛应用各种感知技术。物联网上部署了海量的多种类型传感器，整体构成了分布式异构信源系统，并且因为物联网应用领域的广泛性、分布环境的复杂性和工作时空的差异性，不同类型的传感器所捕获的信息内容、信息格式及时空变化规律都存在差异性，使得物联网内信息呈现海量性、多源性、分布式性等多样性的特征，如图 1-2-1 所示。

（2）可靠传输。物联网通过各种有线和无线网络与互联网融合，将物体的信息实时准确地传递出去。在物联网上的传感器定时采集的信息需要通过网络传输，由于其数量极其庞大，形成了海量信息，在传输过程中，为了保障数据的正确性和及时性，必须适应各种异构网络和协议。

（3）智能处理。物联网不仅提供了传感器的连接，其本身也具有智能处理的能力，能够对物体实施智能控制。物联网将传感器技术、无线通信和微机电技术与智能处理机制相结合，利用云计算、模

式识别等各种智能技术，扩充其应用领域。从传感器获得的多样性特征信息中分析、加工和处理出有意义的数据，适应用户的不同需求并拓展新的应用领域和应用模式。物联网的智能处理过程，从功能结构角度可分解为射频通信系统和信息网络系统。依据信息科学的视点，围绕信息流动过程，可抽象出图 1-2-2 所示的物联网信息处理功能模型，该模型的每步信息管理过程都可融合智能处理的技术手段。

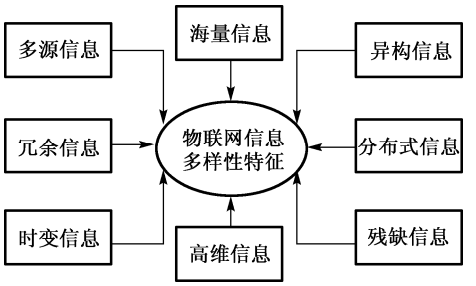

图 1-2-1　多样性信息的全面感知

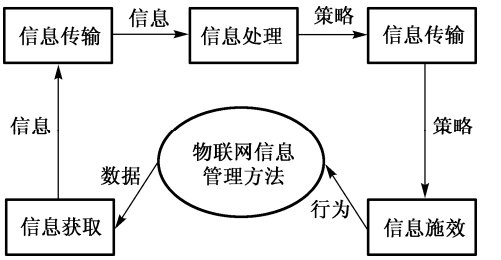

图 1-2-2　物联网信息处理功能模型

1.3　物联网支撑技术特点

1．主要支撑技术

基于已有的各种通信标准和网络服务，物联网支撑技术具有以下几个特点。

（1）感知识别普适化

作为物联网的末梢，自动识别和传感网技术近年来发展迅猛、应用广泛，仔细观察就会发现人们的衣食住行都能折射出感知识别技术的发展。无所不在的感知与识别将物理世界信息化，将传统上分离的物理世界和信息世界高度融合。传感器是机器感知物质世界的“感觉器官”，为物联网系统的处理、传输、分析和回馈提供最原始的信息。随着电子技术的不断发展，传统的传感器正逐步实现微型化、智能化、信息化和网络化。

（2）异构设备互联化

尽管物联网应用中的硬件和软件平台千差万别，各种异构设备（即不同型号和类别的 ZigBee 模块、RFID 标签、蓝牙模块、传感器、手机和笔记本电脑等）利用无线通信模块和标准通信协议，构建成自组织网络，在此基础上运行不同协议的异构网络之间通过网关互联互通，实现网络间的信息共享及融合。

（3）联网终端规模化

物联网时代的一个重要特征是物品触网，每一件物品均具有通信功能，成为网络终端。据预测，未来联网终端的规模有望突破百亿大关。

（4）管理调控智慧化

物联网将大规模数据高效、可靠地组织起来，为上层行业应用提供智能的平台，数据存储、组织及检索成为行业应用的重要基础设施。与此同时，各种决策手段，包括运筹学理论、机器学习、数据挖掘、专家系统等广泛应用于各行各业。面向物联网的传感网，主要涉及以下几项技术：测试及网络化测控技术、智慧化传感网节点技术、传感网组织结构及底层协议、对传感网自身的检测与自组织、传感网安全。

2．未来技术发展方向

物联网技术在不断地发展、深化，并和多领域技术交叉融合，未来将重点从硬件系统和软件体系的革新方面来确立物联网技术发展方向。

（1）硬件系统方面的未来发展方向侧重于物联网的末梢网络技术发展，未来将与新材料和智能传感器设备的研究紧密结合，将包含微缩事物的纳米材料技术和智能化的微机电技术引入物联网的硬件系统，降低网络系统的功耗并提高系统感知终端技术的智能性。

（2）软件系统方面的未来发展方向主要涉及协议规范、体系结构、算法设计三个方面的技术革新。其中，在协议规范发展方面，其自身协议在网络时间同步、容量极限、安全机制、能效利用、抗干扰性等方面仍存在亟待研究和发展的问题，特别是 ZigBee 协议与其他协议标准无线网络（如蓝牙网络、WiFi 网络）的技术共存问题的研究，是其未来协议标准发展的一个重要方向；在体系结构发展方面，主要涉及物联网环境下处理海量多样性信息的软件系统层次结构设计、体系结构组成、子系统相互作用机制构建、可重构技术拓展及并行开发与测试管理等；在算法设计研究方面，主要涉及物联网感知复杂事件语义模型建模算法、传感器节点感知跟踪、行为建模及感知交互算法，以及资源控制、优化和调度算法。

1.4 ZigBee 标准介绍

1.4.1 ZigBee 技术特征

近年来，以传感器、无线通信和微机电技术为核心的物联网技术高速发展，其在环境监测、物流跟踪、医疗监护、家庭娱乐等领域的大量工程运用中，要求实现技术具备低成本、低功耗、自组织等特点。以传感器和自组织网络为代表的无线应用具有传输带宽占用小、传输延时和功率消耗低、组网灵活等众多特点，符合物物联网的自身特点，并且在物联网的广泛应用中需要一种符合低端传感器的、面向控制的、应用简单的专用标准，而 ZigBee 的出现很好地满足了这一系列物联网应用的技术需求。

ZigBee 技术是一种短距离、低复杂度、低功耗、低数据传输速率、低成本的无线通信标准，以 IEEE 802.15.4 无线通信技术为基础，涉及网络、安全、应用方面的软件协议。ZigBee 技术被 IEEE 确定为低速率无线个人局域网标准，其作为低成本、低功耗、双向近距离无线通信标准，已经成为物联网研究领域的核心支撑技术，ZigBee 技术自身所具备的优势特点，使其与物联网领域的开发应用完美结合，成为物联网的重要支撑技术。

（1）工作频段灵活。已经可以使用的频段有 2.4GHz、868MHz（欧洲）及 915MHz（美国），都是可以免除执照的频段。

（2）速率低。ZigBee 虽然根据不同的工作频段，其数据传输速率也会不同，但是都处在较低的速率上。在 868MHz 频段上，有一个数据传输速率为 20kbps 的传输信道；在 915MHz 频段上，有 10 个数据传输速率为 40kbps 的传输信道；在 2.4GHz 频段上，有 16 个数据传输速率为 250kbps 的传输信道。

（3）功耗低。ZigBee 的时间分为工作期和非工作期。由于 ZigBee 技术的数据传输速率较低，传输的数据量很小，因此在工作时的信号收发时间短。而在非工作时，ZigBee 节点处于休眠模式。在低功耗的待机模式下，一般 ZigBee 节点由两节普通 5 号干电池供电，可使用 6 个月以上，从而免去了充电或频繁更换电池的烦琐。

（4）通信范围有限。ZigBee 低功耗的特点决定了设备较小的发射功率，一般两个 ZigBee 节点有效的通信距离为 10～75m，基本可以覆盖普通家庭和办公室。

（5）成本低。由于 ZigBee 的数据传输速率较低，协议简单，使成本降低。然而其协议不收取专利费。ZigBee 降低了其自身对通信控制器的要求，因此可以采用 8 位单片机进行控制，从而大大降低了硬件成本。

（6）时延短。ZigBee 的通信时延和从休眠状态到启动的时延都很短。该特征对时间敏感的信息是至关重要的，此外还可以减少能量消耗。

（7）数据传输可靠。ZigBee 采用了 CSMA/CA 防碰撞机制，给需要带宽固定的通信业务预留专用时隙，避免在发送数据时产生冲突与竞争。在 MAC 层采用了确认数据传输机制，传输过程中出现了问题可以重新发送，从而建立起可靠的数据通信模式。

（8）网络容量大。ZigBee 设备有协调器、路由器和终端三种类型。每个 ZigBee 网络最多可支持 255 个设备，通过网络协调器的连接，整个网络可扩展至 64000 个 ZigBee 网络节点的规模，可以满足大面积无线传感器网络的布建需求。

（9）组网方式灵活。ZigBee 组网方式较为灵活，除了可以组成星形网、簇形网和网状网等方式，网络也可以随节点设备的加入或退出呈现动态变化。

（10）自配置。在有效的通信范围内，ZigBee 可以通过网关自动建立自己的网络，其采用的是载波侦听/冲突检测（CSMA/CA）的方式接入信道；它的节点设备可随时接入或退出，拥有一种自组织的、自配置的组网连接模式。

（11）安全模式。ZigBee 支持认证与鉴权，并在数据传输过程中提供了三个等级的安全处理。第一等级是无安全模式：例如，在某些应用中安全问题并非重要或上层已经给予足够多的安全保护，设备就可以选择这种方式来传输数据。第二级安全模式：设备通过使用接入控制列表（ACL）来防止非法设备获取数据，这级安全模式不采取加密措施。第三级安全模式：在数据传输过程中采用高级加密标准（AES.128）的对称密码，AES 可以保护数据净荷和防止攻击者冒充合法的设备。

ZigBee 技术具有的上述优点，使之可以和物联网完美地结合在一起，成为物联网应用的重要支撑技术。

1.4.2　ZigBee 网络架构

ZigBee 网络存在全功能设备（Full-Function Device，FFD）和精简功能设备（Reduced-Function Device，RFD）两种类型的物理设备，其中，全功能设备 FFD 具备 IEEE 802.15.4 协议标准所指定的所有功能和特征，承担网络控制器的作用并担任网络协调器的角色，提供信息的双向传输并支持网络构建。而精简功能设备 RFD 只具备 IEEE 802.15.4 协议标准所指定的部分功能和特征，在网络中通常作为路由器和终端设备。ZigBee 具有强大的组网能力，可由功能设备构成星形网（Star）、网状网（Mesh）和簇形网（ClusterTree）在内的多种类型的拓扑架构。图 1-4-1 所示的三种节点分别是：协调节点（每个 ZigBee 网络中必须有一个），用于初始化网络信息；路由节点（路由功能），用于存储转发网络中的路由信息；终端节点，根据实用网络的需要携带各种不同信息。

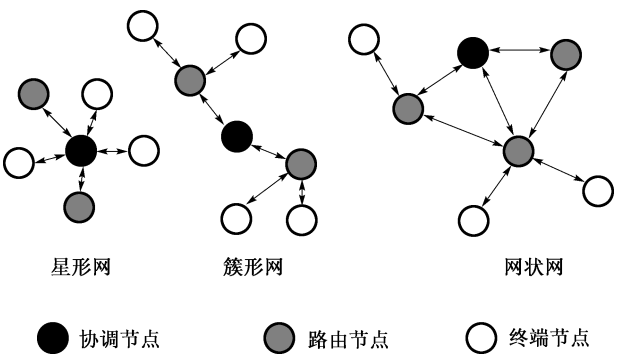

图 1-4-1　ZigBee 的三种网络拓扑架构

1.4.3　ZigBee 技术层次

IEEE 802.15.4 标准定义了开放式系统互联参考模型最下面的两层：物理层（PHY）和介质接入控

制子层（MAC）。该标准描述了低速率无线个人局域网中物理层和媒体访问控制层标准，并把低功耗、低速率传输、低成本作为重点目标，旨在为个人或家庭范围内不同设备之间的低速互连提供统一的标准。IEEE 802.15.4 提供三种物理层的选择（868MHz、915MHz 和 2.4GHz），并且都采用直接序列扩频（DSSS）技术和使用相同的包结构，以降低作业周期、运作功耗和数字集成电路成本。IEEE 802.15.4 标准促使物理层与 MAC 层的协作，从而扩大了网络应用的范畴。ZigBee 联盟提供了网络层和应用层（APL）框架的设计。其中，应用层的框架包括应用支持子层（APS）、ZigBee 设备对象（ZDO）及由制造商指定的应用对象，应用层可基于应用目标由用户灵活地开发利用。ZigBee 技术层次如图 1-4-2 所示。

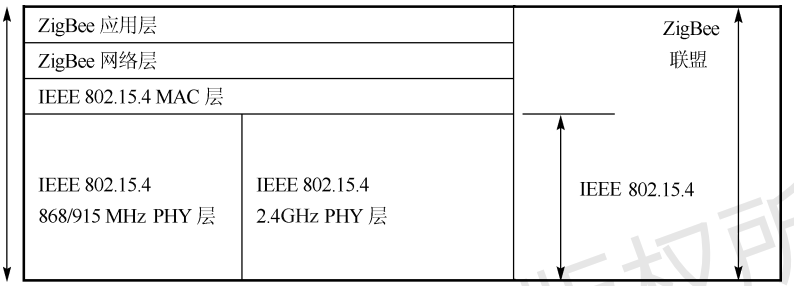

图 1-4-2 ZigBee 技术层次

● 物理层 PHY（Physical Layer）

物理层定义了物理无线信道和与 MAC 层之间的接口，提供物理数据服务物理层管理服务，实现对数据的传输和物理信道的管理。数据传输包括数据的发送与接收，管理服务包括信道能量监测（ED）、链路质量指示（LQI）和空闲信道评估（CCA）等。

● 介质访问层 MAC（Media Access Control）

MAC 层提供两种服务：MAC 层数据服务和 MAC 层管理服务，前者保证 MAC 数据单元在数据服务中的正确收发，后者实现 MAC 的管理活动。IEEE 802.15.4 MAC 子层实现包括设备间无线链路的建立、维护与断开，确认模式的帧传送与接收，信道接入与控制，帧校验与快速自动请求重发，预留时隙管理及广播信息管理等。MAC 子层处理所有物理层无线信道的接入。MAC 层通用的帧结构如表 1-4-1 所示。

表 1-4-1 MAC 层通用的帧结构

信标帧结构							
字节：2	1	4～10	2	K	M	N	2
帧控制	序列号	地址域	超帧描述字段	GTS 分配字段	带转发数据目标地址	信标帧负荷	帧校验
MAC 帧头			MAC 数据服务单元				MAC 帧尾

数据帧结构				
字节：2	1	4～20	N	2
帧控制	序列号	地址域	数据帧负荷	帧校验
MAC 帧头			MAC 数据服务单元	MAC 帧尾

确认帧结构		
字节：2	1	2
帧控制	序列号	帧校验
MAC 帧头		MAC 帧尾

续表

命令帧结构					
字节：2	1	4~20	1	N	2
帧控制	序列号	地址域	命令类型	数据帧负荷	帧校验
MAC 帧头			MAC 数据服务单元		MAC 帧尾

MAC 协议是在 ZigBee 的底层驱动程序基础上实现的，主要包括芯片射频模块接口和一个操作系统抽象层。ZigBee 协议 MAC 层逻辑模型机构如图 1-4-3 所示。

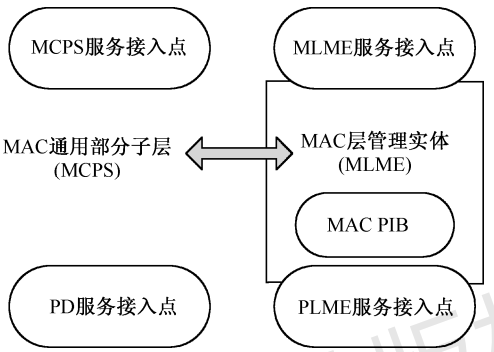

图 1-4-3　ZigBee 协议 MAC 层逻辑模型机构

● 网络层框架

网络层负责拓扑结构的建立和维护、命名和绑定服务，它们协同完成寻址、路由及安全这些必须的任务。网络层管理实体提供网络管理服务，允许应用与堆栈相互作用。网络层数据实体为数据提供服务，在两个或多个设备之间传送数据时，它将按照应用协议数据单元的格式进行传送，并且这些设备必须在同一个网络中，即在同一个内部无线个域网中。网络层数据实体可提供生成网络层协议数据单元、指定拓扑传输路由、确保通信的真实性和机密性等服务。网络协议数据单元即网络层帧结构如表 1-4-2 所示。

表 1-4-2　网络层帧结构

字节：2	2	2	1	1	0/8	0/8	0/1	变长	变长
帧控制	目的地址	源地址	广播半径域	广播序列号	IEEE 目的地址	IEEE 源地址	多点传送控制	源路由帧	帧的有效负荷
网络层帧报头									网络层的有效负荷

● 应用层框架

ZigBee 应用层框架包括应用支持层（APS）、ZigBee 设备对象（ZDO）和制造商所定义的应用对象。应用支持层的功能包括：维持绑定表、在绑定的设备之间传送消息。所谓绑定，就是基于两台设备的服务与需求将它们匹配地连接起来。APS 数据包格式如表 1-4-3 所示。

表 1-4-3　APS 数据包格式

Frame Control	DstEndpoint	Cluster ID	Profile ID	SrcEndpoint	Data
帧类型、传输模式、非直接地址模式、安全有无、ACK 有无等信息	接收节点的 ID	用来判断所传输的数据包	应用的标识 ID	发送节点的 ID	数据负荷

ZigBee 设备对象的功能包括：定义设备在网络中的角色（如 ZigBee 协调器与终端设备），发起和

响应绑定请求，在网络设备之间建立安全机制。ZigBee 设备对象还负责发现网络中的设备，并且决定向它们提供何种应用服务。

1.5 思考与扩展

（1）简述物联网体系的基本特征，参照以下“技术定义”角度，从“服务应用”的角度来总结分析物联网的特征。

从技术定义的角度来看，物联网体系有三个基本特征：①全面感知，即利用射频识别技术（RFID）、传感器、二维码等随时随地获取物体的信息；②可靠传递，通过各种电信网络与互联网的融合，将物体的信息实时准确地传递出去；③智慧处理，利用云计算、模糊识别等各种智慧计算技术，对海量的数据和信息进行分析和处理，对物体实施智能化的控制。

（2）从多种内涵角度简述物联网基本概念的定义，并参照以下思路提示来总结说明：物联网内“物”类型的广泛性和联系“物”的技术手段多样性。

思路提示：物联网是通过射频识别、红外传感器、全球定位系统、激光扫描仪等信息传感设备，按约定的协议，把各种物体与互联网相连接，进行信息交换和通信，以实现对物体的智能化识别、定位、跟踪、监控和管理的一种网络。特别注意，物联网中的“物”，不是普通意义的万事万物，这里的“物”要满足以下条件：①要有相应信息的接收器；②要有数据传输通路；③要有一定的存储功能；④要有处理运算单元（CPU）；⑤要有操作系统；⑥要有专门的应用程序；⑦要有数据发送器；⑧遵循物联网的通信协议；⑨在网络世界中有可被识别的唯一编号。