第2章 物联网环境下的信任模型相关研究

物联网环境是一种新型的网络形势，通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，把现代最新传感技术和网络的便利条件结合起来，使所有智能的一切物体联合成一个网络，从而极大的方便人们的生活。物联网是在互联网的基础上进行了延伸和扩展，将客户端延伸至任何物品与物品之间，使其可以进行信息交换和通信。物联网技术在大规模、异构化、分布式的物联网环境下已经逐渐成型，并日趋完善，但是也存在着很多问题，其中安全问题是物联网技术发展和推广过程中最严峻的问题。利用信任模型对于物联网环境中的管理域及实体进行信任评估，建立跨域实体间的信任关系是目前物联网环境中解决安全问题的有效方法，本章主要介绍了物联网环境的概念及特点，叙述了信任的相关概念，并分析了物联网环境下现有信任模型的优缺点。

2.1 物联网环境下的信任

2.1.1 物联网发展情况概述

随着生活智能化的发展，互联网以及各类传统的分布式网络已经不能满足人们的生活需求了，此时针对物联网环境的发展就成为了当今世界上一个重点的研究课题。2005年信息社会世界峰会上，国际电信联盟发布了《ITU互联网报告2005：物联网》，自此物联网的定义和范围已经发生了变化，覆盖范围有了较大的拓展，不再只是指基于[RFID](https://baike.baidu.com/item/RFID" \t "https://baike.baidu.com/item/%E7%89%A9%E8%81%94%E7%BD%91/_blank)技术的物联网[1]。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，就是把现代最新传感技术和网络的便利条件结合起来，把所有智能的一切物体联合成一个网络，从而极大的方便人们的生活，其安全体系结构可分为三层：感知层、网络层和服务层。感知层中实现了对物理世界的智能感知识别、信息采集处理和自动控制，包括传感器、执行器、[RFID](http://iot.ofweek.com/CAT-132201-RFID.html" \o "RFID" \t "http://iot.ofweek.com/2017-02/_blank)、[二维码](http://iot.ofweek.com/CAT-132205-erweima.html" \o "二维码" \t "http://iot.ofweek.com/2017-02/_blank)和智能装置；网络层中实现了不同的网络连接方式；应用层中包涵了应用基础设施、中间件和[物联网应用](http://iot.ofweek.com/tag-%E7%89%A9%E8%81%94%E7%BD%91%E5%BA%94%E7%94%A8.HTM" \o "物联网应用" \t "http://iot.ofweek.com/2017-02/_blank)。物联网技术体系图如图2.1所示。物联网是在互联网的基础上进行了延伸和扩展，将客户端延伸至任何物品与物品之间，使其可以进行信息交换和通信。如今，物联网技术在大规模、异构化、分布式的物联网环境下已经逐渐成型，并日趋完善。



图2.1 物联网技术体系图

物联网是新一代信息技术的高度集成和综合运用，对新一轮产业变革和经济社会绿色、智能、可持续发展具有重要意义。因其具有巨大增长潜能，已是当今经济发展和科技创新的战略制高点，成为各个国家构建社会新模式和重塑国家长期竞争力的先导[31]。为此，发达国家纷纷出台政策进行战略布局，抢抓新一轮信息产业的发展先机。美国以物联网应用为核心的“智慧地球”计划、欧盟的十四点行动计划、日本的“U－Japan计划”、韩国的“IT839战略”和“u－Korea”战略、新加坡的“下一代I－Hub”计划、台湾的U－Taiwan计划等都将物联网作为当前发展的重要战略目标[32]。自2009年8月温家宝总理提出“感知中国”以来，物联网被正式列为国家五大新兴战略性产业之一，并写入“政府工作报告”，物联网在中国受到了全社会极大的关注，其受关注程度是在美国、欧盟、以及其他各国不可比拟的。近年来在中国制造2025、互联网+双创等带动下，中国物联网产业发展取得长足进步。目前，中国三家基础电信企业都已启动NB-IoT(窄带物联网)网络建设，将逐步实现全国范围广泛覆盖，2017年全网基站规模超过40万站[32]。

2.1.2 信任的概念及特征

信任概念由于其抽象性和结构复杂性，在社会学、心理学、营销学、经济学、管理学等不同的领域定义信任是不同的，至今仍没有一个统一的定义，但是达成共识的观点是：信任是涉及交易或交换关系的基础。在社会科学中，信任被认为是一种依赖关系。相互依赖表示双方之间存在着交换关系，无论交换内容为何，都表示双方至少有某种程度的利害相关，己方利益必须靠对方才能实现。而在计算机网络环境下，信任被用来作为解决可信问题，因此在计算机科学中，信任被认为是一个节点和另一个节点在产生信息交互时对于对方的能力、信誉和可靠性的一种认知和期望。Grandison在文献[33]中，根据分析总结出信任的定义为：“对某个实体能在给定的上下文环境下采取可靠、安全和可依赖行动能力的坚定信念”。也有文献认为，信任是根据主体在具体环境下的不同属性所组成的概念。文献[34]中，将信任分为四类：信任倾向，组织信任，信任信心，信任意向。文献[35]对信任在网络环境的定义为：“信任是对一个实体能力的坚定信念。但是这种坚定信念对于实体来说不是固定不变的，在给定的时间内，在某些方面，随着实体行为变化而变化”。以上对信任的定义，都蕴涵着对实体过去行为的评价，这种评价是随着实体行为能力的改变而动态变化的。综合和归纳以上文献中对于信任的定义，本文将物联网环境下信任的相关概念归纳定义为：

定义2.1 信任：在物联网环境中的特定时刻和上下文背景下，实体间进行交互活动时，交互响应实体对于交互请求实体的交互行为进行满意度评价，并根据物联网环境中的实体属性及相关的信任度评价参数计算出交互请求实体的信任度，作为该实体再次进行交互活动的评价依据。

定义2.2 信任度：信任度是交互响应实体对于交互请求实体信任程度的量化表示，也是实体间信任关系的量化表示，也可以称为信任值、信任关系与可信度。

定义2.3 管理域：在物联网环境下将所有为用户提供资源服务的产品划分为多个管理域，每个管理域中包含多个实体，每个实体包含不同的数据资源。在物联网环境下利用管理域对于实体进行安全管理。

通过长期的研究，专家学者们对于信任的特性达成了一致的观点，参考相关文献[付思源]，本文归纳出信任具有以下特征：

(1)信任的主观性[36]：信任是一种主观的想法，信任评估通常由需要获取信任度的实体节点发起。

(2)信任的不完全的传递性[37]：在物联网环境下不能单纯使用递推原则，如果实体Ea信任实体Eb，实体Eb信任实体Ec，则实体Ea信任实体Ec，这个推论是错误的。在物联网环境下，对于信任的传递性计算应该进行量化处理。具体表示如图2.2所示。

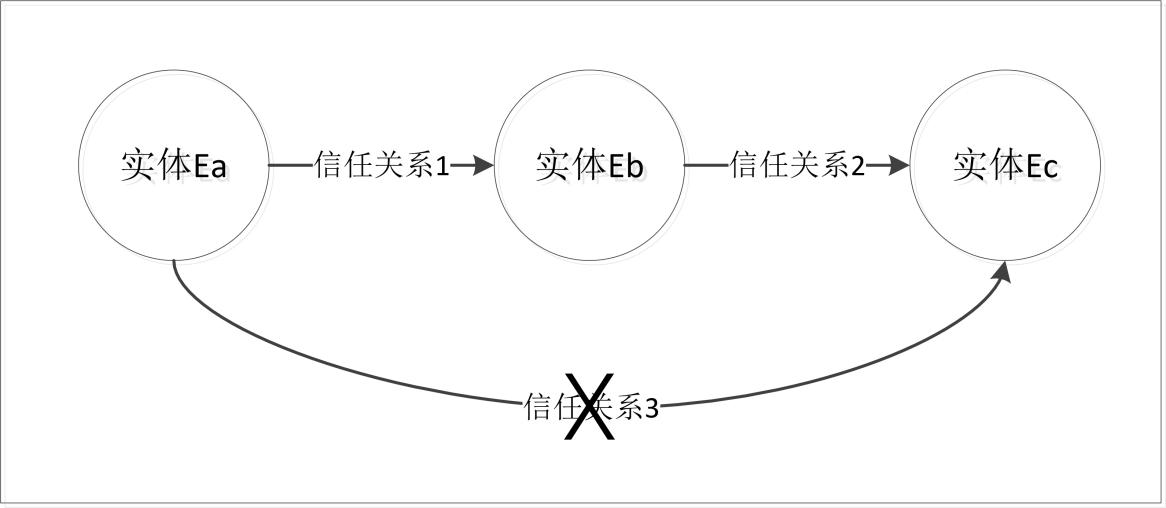


图2.2 信任不完全传递性关系图

(3)信任的时效性[38]：在物联网环境中所有实体的行为以及状态都是动态变化的，因此评估的信任度也会随着时间的改变而动态变化。

(4)信任的非对称性[39]：在物联网环境下信任关系具有方向性，实体Ea信任实体Eb，但实体Eb并不一定信任实体Ea。因此跨域实体间的信任度一般具有不可逆的关系。具体表示如图2.3所示。

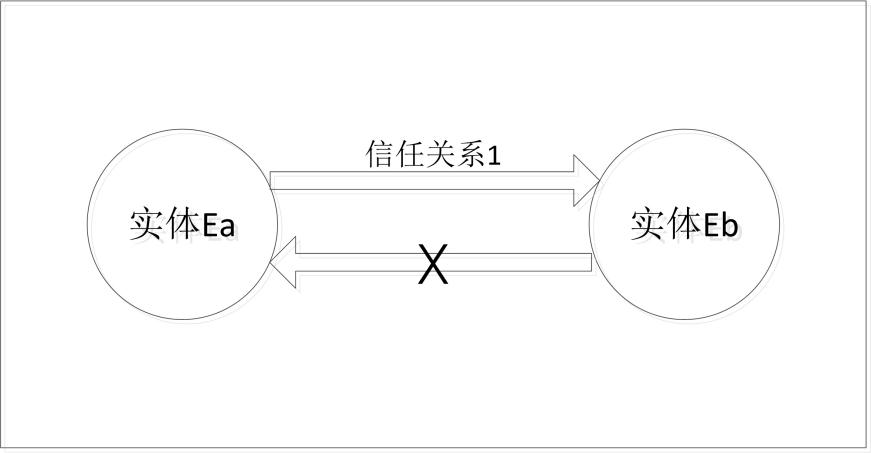


图2.3 信任非对称性关系图

(5)信任的上下文服务背景相关性[40]：由于在物联网环境下，存在多种不同的服务类型，因此在计算跨域实体间的信任度时就应该考虑到目前实体所处的上下文服务背景，上下文服务背景的改变必然会改变跨域实体间的信任度。

(6)信任的可度量性：信任可以被量化处理并计算出具体的数值，用以衡量和判断域间关系。

根据信任的特征进行分析，发现信任有很强的主观性，不同的实体给出的信任评价是不同的。在物联网环境下，由于实体所属的管理域不同，导致实体间的信任评估机制也可能是不同，因此跨域实体间的信任并没有主观存在的联系，而且信任关系也不对称。这与人类的社会关系非常相似，物联网中跨域实体间的信任关系评估涉及到行为、属性、上下文环境等因素，难以定量表示和预测，因此信任管理和评价面临着非常大的挑战[41]。

2.1.3 信任关系的评价

信任关系的评价是指应用数学方法对信任度的大小进行描述，现在所提出的信任模型中信任值的表示方法主要有：离散值方法、概率值方法、模糊理论、灰色值方法、证据理论、信任云方法以及各类数学分布方法等。

根据物联网环境特性和具体服务情况分析得出，跨域实体间存在两种信任度：直接信任度（DT\_Direct Trust）和推荐信任度（RT\_Recommend Trust），若跨域实体间不存在直接信任关系，则可以通过推荐信任关系进行交互活动，在本次交互活动结束后，即建立跨域实体间的直接信任关系；若域间既不存在直接信任关系，也不存在推荐信任关系，在进行资源交互时，直接建立域间直接信任关系。根据上述分析，本文将物联网环境下信任关系的相关概念归纳定义为：

定义2.4 域内信任度：域内信任度表示物联网环境下各管理域内实体的信任度。

定义2.5 管理域间信任度：管理域间信任度表示物联网环境下两个管理域间的信任关系。

定义2.6 跨域实体间信任度：跨域实体间信任度表示物联网环境下两个不同管理域内的实体间的信任关系。

定义2.7 直接信任度：直接信任度表示两个跨域实体间存在直接的信息资源交互关系。

定义2.8 推荐信任度：推荐信任度表示为两个跨域实体间存在一条或多条路径，该路径称为推荐信任路径，即两个跨域实体间可以通过推荐信任路径的关联关系建立信任关系。

跨域实体间信任关系的评价需要根据直接信任度和推荐信任度的共同作用，同时需要结合实体的域内信任度以及实体的各类特征属性共同进行评估。信任关系的评价需要根据确定的跨域实体对象及相关参数来测定跨域实体间的信任度，并将跨域实体间信任度这种抽象的主观判断转换为客观量化的计量值，评价本质上是对评价对象进行价值判断的过程[42]，因此信任关系评价的最终目的是为了消除信任关系无法统一度量的差异。如图2.4所示，信任关系的评价流程中通过对物联网环境下的实体建立信任模型，最终得到跨域实体间的信任度。

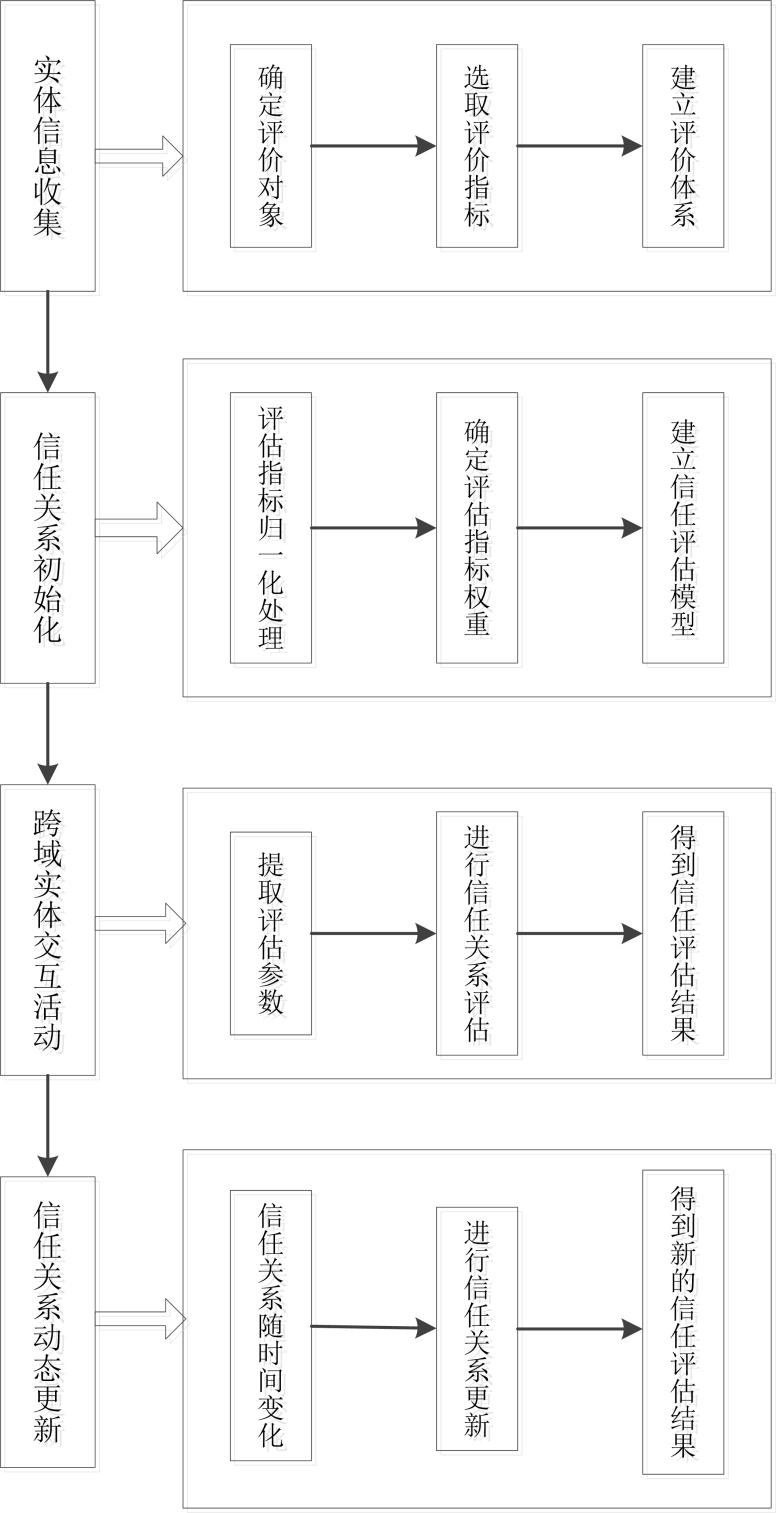


图2.4 信任关系评价流程图

为了使最终的信任度结果真实可靠，在信任关系的评价过程中需要参考如下准则[43]：

(1)信任关系的客观性：信任关系的评估大部分属于实体间的主观评价是，为了保证信任关系的客观性，需要建立合适的客观评价体系，使信任关系具有客观性。

(2)信任关系的规模性：为了保证信任关系的评价结果真实可靠，能够准确的反应实体间的实际信任情况，需要对于建立的信任模型进行大量的实验，保证实体间的交互活动数量。

(3)信任关系的时间衰减性：由于实体间的信任值会随着时间的推移而动态变化，因此在进行信任关系评价的过程中需要考虑到时间衰减因素，距离当前交互时间越近的信任值越能反映实体间的信任关系。还可以根据已有的历史信任关系对于未来的信任关系进行合理的预测，这样可以更好的评价实体间的信任关系。

(4)信任关系的多样性：物联网环境下各实体间存在着复杂的关联关系，可以是一对一、一对多或者多对多的信任关系。

(5)实体交互活动的风险性：实体间的信任关系评估不仅需要考虑实体本身对于信任关系的影响，还需要考虑到实体间进行交互活动过程中外界环境对于信任关系的影响，因此需要对于实体交互活动过程中可能出现的风险因素进行分析，并将其可能产生的影响加入到信任关系的评价中。

(6)实体属性的规范性：能够反映实体信任属性的参数复杂多样，而且具有不同的表现形式和度量单位，因此必须对于实体属性参数进行标准化的量化处理。

2.2 典型的信任模型概述

Marsh在1994年，第一次将对信任的研究引入计算机领域当中[14]，根据不同网络环境的信任需求，专家学者们目前提出了很多不同网络背景下的信任评估模型。信任评估模型的研究，是指根据收集到的实体属性信息、实体行为信息以及与之交互的实体间的交互信息，通过建立的数学模型对这些信息进行分析、处理和计算，从而得到一个可以客观准确的评价实体间信任关系的信任值[44]。从不同的角度、不同的环境分析信任模型，可以将信任模型分成很多种类。根据信任模型的工作内容，可以将信任模型分为静态信任模型和动态信任模型。描述个体身份信息可信程度的信任称为身份信任，针对身份信任进行评估、控制与管理的信任模型称为静态信任模型；描述个体行为可信程度的信任称为行为信任，针对行为信任进行评估、监控与预测的信任模型称为动态信任模型。静态信任模型和动态信任模型是相互依赖、相互补充的，前者确保网络中节点的身份可信，后者评估和规范节点的后续交互行为[45]。本文所研究的跨域实体间的信任模型属于动态信任模型，因此本章主要针对典型的动态信任模型进行概述。目前典型的动态信任模型主要有基于贝叶斯理论的信任评估模型、基于模糊理论的信任评估模型、基于证据理论的信任评估模型以及基于访问控制技术的信任评估模型，接下来将对于这几类典型的动态信任模型进行分析。

2.2.1 基于贝叶斯理论的信任评估模型

基于贝叶斯的信任评估方法是指利用贝叶斯网络来描述实体的不同信任因素，并指定先验概率分布，然后利用贝叶斯规则推测后验概率，从而可以将它们整合以度量实体可信度[46]。贝叶斯理论是一种广泛使用的信任评估工具，贝叶斯理论基本原理图如图2.5所示。基于贝叶斯理论，Ganeriwal等人[21]提出一个信任框架RFSN，框架利用信誉分布与Beta拟合来评估节点的可信度，得到节点的信誉分布服从Beta分布的结论。Che等人[22]提出一种轻量级的WSN信任管理方案，利用贝叶斯理论进行直接信任的更新与计算，同时利用熵进行权重分配，降低了主观分配权重的局限性。Song 等人［47］提出的基于贝叶斯决策理论模型的方法，假设实体不具备模糊性，实体行为只有成功和失败两种状态，在文献［48］中的实验表明这种确定性在快速变化的网络中，恶意事件报告率并不理想，且当信任阈值较小时，恶意事件误报率较高。邵楠楠等人[24]提出的一种基于贝叶斯的改进WSNs信任评估模型，利用异常衰减因子来修正贝叶斯公式，实现了模型的轻量化，利用直接信任置信度的概念来判断是否需要计算间接信任，同时根据熵来分配权重克服了主观分配权重的局限性。贝叶斯方法考虑了信任的随机不确定现象，其自动学习机制非常适合信任的动态建模需求，但须事先假定历史评价信息服从某类典型分布[46]。

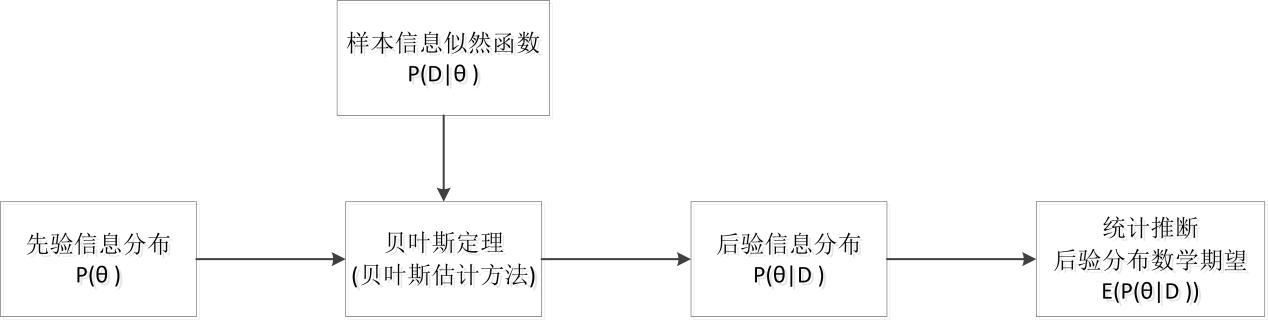


图2.5 贝叶斯理论基本原理图

2.2.2 基于模糊理论的信任评估模型

1965年美国加州大学的L.A.Zadeh教授发表了著名的论文[49]，文中首次提出表达事物模糊性的重要概念：隶属函数，从而突破了19世纪末康托尔的经典集合理论,奠定模糊理论的基础。信任关系的评估存在很大的主观模糊性，基于模糊逻辑的信任模型可以利用隶属函数来描述信任的级别，并通过模糊逻辑推理规则产生模糊值，从而处理信息的模糊性。典型的模糊推理过程如图2.6所示，模糊规则的形式一般为，其中A与B都是语言变量，而a和b则是由隶属函数映射得到的语言值，在数据库中都有相应的隶属函数加以定义。推理机制（Decision-making unit）按照这些规则和所给的事实执行推理过程，求得合理的输出或结论。

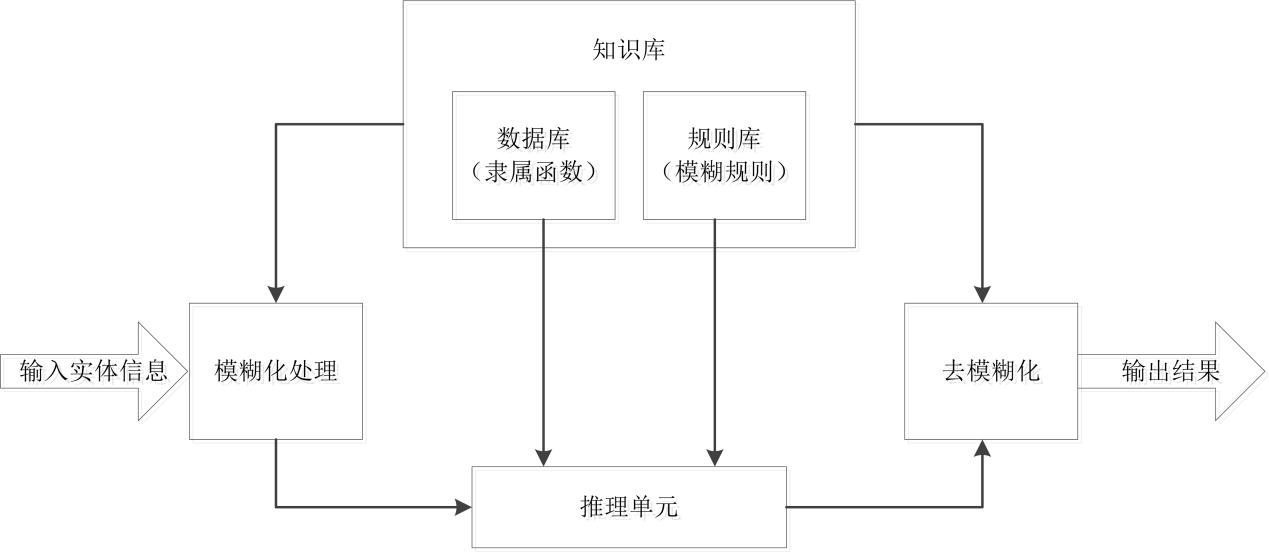


图2.6 模糊推理过程图

根据以上模糊理论的推理过程，Song等人[50]基于模糊理论，在隶属函数中引入了交互成功率和恶意节点入侵自身防御能力这两个参数，用来制定模糊推理规则，并综合新的实体行为和历史因素来动态更新信任值，可以较好地抵御恶意实体同时保证信任值计算的准确性。Tajeddine等人[51]提出了一种实体信誉与模糊子系统相结合的信任模型，在评估信任值时综合考虑了实体的历史信誉、实体相似度、实体活跃度以及实体流行度，根据模糊子系统分析交互活动的重要性，并决定是否进行交互，该算法复杂度小，便于自动化处理，但是上述参数的权重因子根据自身经验事行给定，使得计算结果具有较强的主观性。Xia等人[52]介绍了一种基于个体历史经验和逻辑规则预测方法的信任模型，并将节点的预测信任值引入到标准源路由机制中，建立了一种灵活可信的路由协议，以抵制不可信节点获得可靠路径传递路由和缓解恶意节点的攻击行为。

2.2.3 基于证据理论的信任评估模型

证据理论是一套能够细腻地将命题不确定性问题转化为集合不确定性问题的数学理论。证据理论的适用范围非常广泛，如决策分析、信息融合和模式识别等领域[53]。在基于D-S证据理论的信任模型中，主要依据基本类概率分配（BPA）函数进行信任评估，BPA函数大多基于古典概率理论建立[54-55]，容易忽略了不同信任证据对信任值的影响；针对恶意节点攻击的问题，研究者们在基于证据理论的信任模型[56]中加入了时间衰减因子，但是却导致了可信服务无法持续提供的问题。现有的大多数基于证据理论的信任模型都采用三元组定量的表示信任关系。在文献[57-58]的定量模型中，通常用三元信任关系组中的基本信任函数或D-S证据理论的信任函数来表示信任值，但是却忽略了不可信分量和不确定分量对信任值的影响。证据理论在构造信任函数时，限定了事件的概率，并且不需要对某些难以获取的准确概率给出特定解释。作为不确定性推理的一种方法，证据理论具有完善的数学理论基础，它提供了一种有效的决策工具来融合不确定信息。D-S证据理论是贝叶斯推理方法的一种推广，贝叶斯推理方法主要是基于概率论中的贝叶斯条件概率来进行的，有必要知道先验概率，而D-S证据理论不需要知道先验概率，能够很好地表示“不确定”，所以广泛用于处理不确定的数据。D-S证据理论的信任模型结构图如图2.7所示。

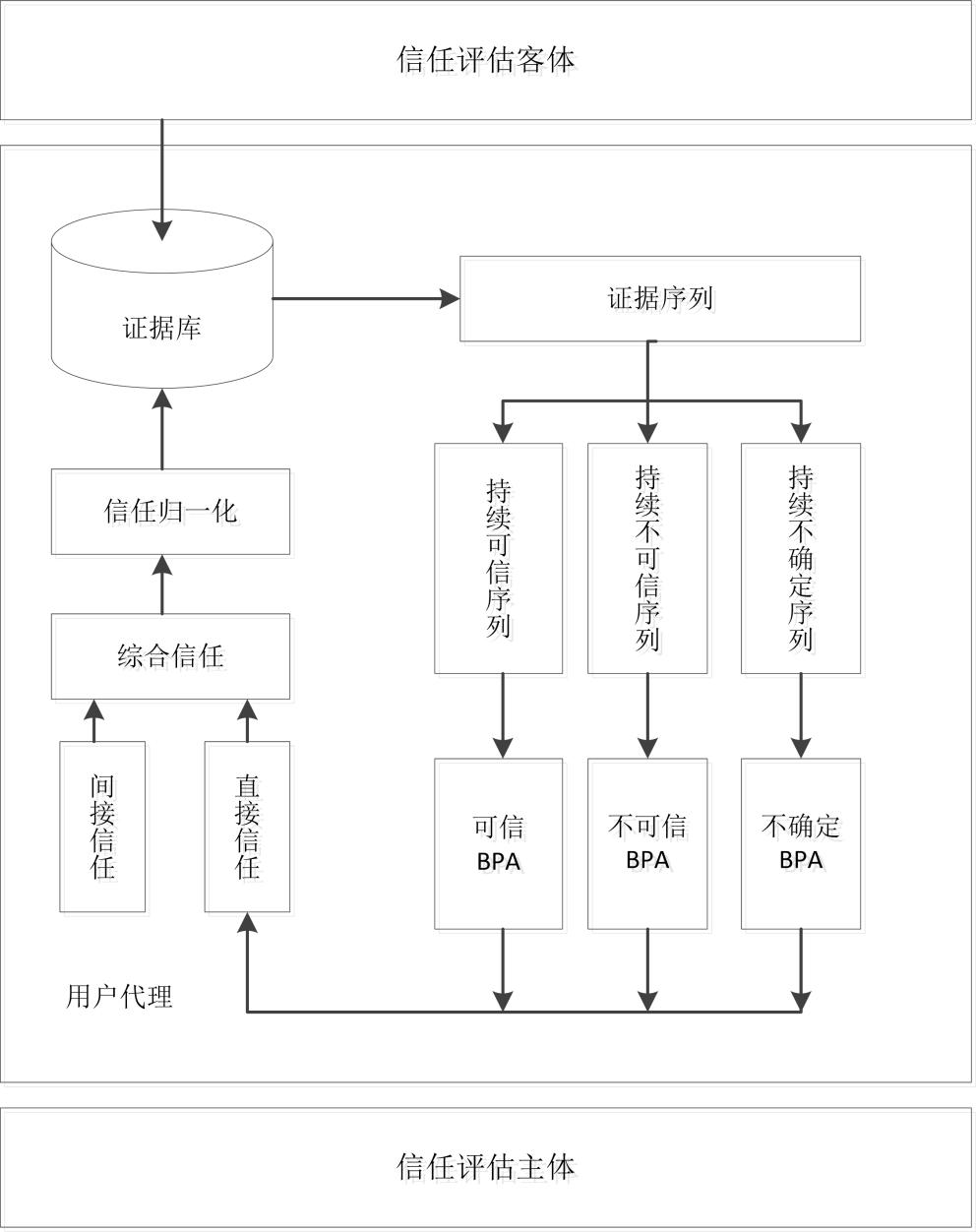


图2.7 D-S证据理论信任模型结构图

2.2.4 基于访问控制的信任评估模型

访问控制是对实体交互访问的行为进行监控和约束的一种操作[59]：允许符合访问要求的实体在特定的条件下进行合法的交互访问，有效安全地使用资源[王文博10]。基于访问控制技术建立的信任评估模型，可以应用访问控制技术于对安全信任系统进行描述和控制，同时对于安全访问的信任值进行评估。基于访问控制的信任评估模型定义了对交互请求实体依据模型所规定的访问控制权限对其他实体进行交互活动的访问控制操作。目前主流的访问控制技术有三种，分别是：基于角色的访问控制技术(RBAC)、基于属性的访问控制技术(ABAC)和基于任务的访问控制技术(TBAC)。

基于角色的访问控制技术[60](RBAC)是在实体和交互访问权限之间利用角色属性建立两者之间联系的一种访问控制模型。针对不断增加的实体数量和日益复杂和频繁变化的实体组织结构，RBAC模型的建立可以有效地解决交互访问权限管理更加复杂的问题。RBAC模型在很大程度上简化了对实体访问的权限管理，能够有效缓解巨大规模的授权管理问题，被认为是一种比较通用的访问控制技术。基于角色访问控制的信任评估模型中，将实体信任评估的问题转化为实体交互访问权限控制的问题，利用基于角色的访问控制技术，对实体的信任值进行评估，有效解决了实体信任评估问题。

基于属性的访问控制技术[61](ABAC)是在实体信任评估和实体交互访问授权决策中引入了大量与实体相关属性的一种访问控制技术，模型中所有实体都是通过其自身特征属性来进行描述的，可以充分体现实体的相关特性，在进行实体信任评估时具有更高的可信度。通过实体属性来控制实体信任交互的方式使得该方法具有更高的灵活性可以满足细粒度的访问控制需求。此外ABAC模型在信任评估的过程中并不会重点关注交互访问实体，而是严格检测交互请求实体的各项属性集，使其更好的适应开放式环境。同时，基于属性的访问控制技术还会根据交互请求特征生成匹配策略集合，并从集合中选取最合适响应实体进行交互推荐，有效的完成了信任评估模型中的结果推荐功能。

基于任务的访问控制技术[62](TBAC)是区别于传统访问控制模型的一种新型访问控制模型。该技术突出的特点在于从交互任务的角度出发，把交互任务作为最核心的因素进行信任模型的构建。模型在交互请求实体和交互响应实体间加入任务层[63]，实现对于访问权限的分离，交互请求实体的访问权限并不固定，会随着任务的状态和环境进行动态变化，同时交互请求实体的访问权限也具有时间衰减性，当一次交互请求任务结束后，交互请求实体的访问权限就会失效，这样有效防止了交互请求实体对交互响应实体访问权限的长时间占有，使信任模型的安全性拥有保障。因此，基于任务的访问控制技术是一种非常灵活的动态访问权限控制技术，很适合应用于信任评估模型中。

根据上述典型信任模型的对比分析，目前已有的典型信任模型依据不同的理论和技术有效的解决了实体信任评估的问题，但是针对特定的物联网环境建立跨域实体信任模型，还需要选取适合物联网环境特性的理论技术进行进一步分析和完善。

2.3 物联网环境下的信任模型概述

物联网的多域环境具有复杂性，跨域实体间交互活动的信任关系评估也呈现出动态发展的趋势。在现有的物联网环境下跨域实体交互研究工作中，普遍情况下均假设物联网环境中各实体之间是相互信任的，而且可以进行资源传递和共享等交互活动，但是在实际的物联网应用环境中，各跨域实体之间并没有建立任何的信任关系，大部分实体间的交互活动都是在同一个管理域内，或者具有相同信任评价标准的管理域内进行的，对于跨管理域的实体间交互活动可能不会完成，因此需要建立物联网环境下跨域实体间的信任评估模型。物联网环境中各实体间的信任关系会随着时间的推移及实体间的交互情况发生改变，而且实体间的信任关系具有非对称的特性，必须结合特定时间段的历史交互情况、上下文服务环境以及实体的特征属性才能进行跨域实体间的信任评估。伴随物联网技术的发展，物联网感知层中的感知设备种类也越来越丰富，突破了原有的无线传感器中通信半径受限的约束，具备了远距离、跨区域信息互联与资源共享的功能[64]。但是不同管理域间实体的信任模型之间存在很大的差异，在跨域实体进行交互活动时受到了很大的限制。

针对物联网环境中的信任模型目前有大量的相关研究，因此信任模型的功能也越来越完善，在本节中选取了四个典型的信任模型分别进行模型优缺点的分析。从分析中可以发现，每个信任模型都存在着一些缺陷，本文在建立跨域实体信任模型时应该考虑到这些限制，尽量避免这些缺陷。

2.3.1 基于狄利克雷(Dirichlet)分布的信任模型

狄利克雷(Dirichlet)分布是一组连续多变量的[概率分布](https://baike.baidu.com/item/%E6%A6%82%E7%8E%87%E5%88%86%E5%B8%83/828907" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)，是多变量普遍化的Beta分布，Dirichlet分布常作为[贝叶斯统计](https://baike.baidu.com/item/%E8%B4%9D%E5%8F%B6%E6%96%AF%E7%BB%9F%E8%AE%A1/3431194" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)的[先验概率](https://baike.baidu.com/item/%E5%85%88%E9%AA%8C%E6%A6%82%E7%8E%87/6106649" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)。当Dirichlet分布维度趋向无限时，便成为[狄利克雷](https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7/971345" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)过程(Dirichlet process)[65]。

文献[倪伟32]提出了一种基于Dirichlet分布的信任模型，该模型假设一个实体对其他实体的评价有k个不同的离散等级，模型中对应的Dirichlet分布共有k个可能状态。在某一时段n内，对实体a的累计评价值可以用集合来表示，在某一时刻t时，对实体a的评价值可以用集合来表示，t时刻实体x对实体a的评价值用集合来表示。当实体x对实体a的评价级别为i时，改变集合中第i个元素值为1，其他的元素值则为0。收集t时刻所有实体对实体a进行信任评价的评价值集合，则有，其中表示t时刻对实体a进行评价的实体集合。该信任模型中的基于Dirichlet分布的信任算法考虑到实体间信任关系的时间衰减性，在计算实体间信任度时引入了时间衰减因子，因此在t+1时刻，对实体a进行信任评价的累计评价集合由t+1时刻的信任评价向量和前一时刻t对实体a进行信任评价的累计评价集合结合时间衰减因子共同计算，利用其计算表达式为：



由于Dirichlet分布是共轭分布，所以后验概率分布也服从Dirichlet分布，因此利用Dirichlet分布的后验分布期望估计值求出实体间的信任度。

该模型主要优点有：(1)利用Dirichlet分布的概率期望值表示实体间的信任度，可以有效地解决实体间信任关系的不确定性；(2)模型中算法采用迭代方式进行计算，算法思路清晰实现起来比较简单。但是该模型也存在着一些缺点：(1)模型缺乏对于恶意实体攻击的风险分析，没有在信任评估中加入惩罚机制；(2)模型中的信任度算法只考虑到了实体间的直接信任关系，没有考虑到实体间的推荐信任关系以及实体间的上下文服务环境，不能全面完整的描述实体间的信任度。

文献[66]针对多Agent系统(MAS)也提出了一种基于狄利克雷分布的信任模型，该模型对于实体间信任度计算分为三个部分，首先计算实体间的直接信任度，然后进行推荐信任度的计算，最后针对恶意节点进行过滤。在MAS中，实体间的直接信任关系是对实体节点历史交互经验的总结，Dirichlet分布常作为[贝叶斯统计](https://baike.baidu.com/item/%E8%B4%9D%E5%8F%B6%E6%96%AF%E7%BB%9F%E8%AE%A1/3431194" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)的[先验概率](https://baike.baidu.com/item/%E5%85%88%E9%AA%8C%E6%A6%82%E7%8E%87/6106649" \t "https://baike.baidu.com/item/%E7%8B%84%E5%88%A9%E5%85%8B%E9%9B%B7%E5%88%86%E5%B8%83/_blank)，且Dirichlet分布是共轭分布，所以后验概率分布也服从Dirichlet分布，因此该模型利用Dirichlet分布的后验分布期望估计值求出实体间的直接信任度，计算表达式为：





其中N表示实体间发生的交互次数，事件的先验分布是Dirichlet分布，后验概率分布也服从Dirichlet分布，则有的后验分布期望估计值就是实体间的直接信任度。

在进行推荐信任度计算时，该模型使用最优无偏估计方法对推荐信任度进行估计，同时采用概率链式法则来合成推荐信任度，计算表达式为：



其中和分别表示实体间发生的交互次数。

多Agent系统中基于狄利克雷分布的信任模型中，结合实体间的直接信任度和推荐信任度以及针对恶意节点过滤的层次过滤算法共同计算实体间的信任度，该模型主要优点有：(1)能够克服了已有信任模型的部分局限性，有效处理简单恶意节点的攻击；(2)利用Dirichlet分布的概率期望值表示实体间的信任度，可以有效地解决实体间信任关系的不确定性，同时结合推荐信任度，可以有效提高了信任评估的准确性。但是该模型也存在着一些缺点：(1)该模型主要针对局域网络环境进行测试，不能适应不同应用背景下信任评价标准不同的管理域间实体的交互需求；(2)模型中的信任度算法没有考虑到实体间的上下文服务环境以及实体自身的特征属性，没有完全体现实体间的信任关系，不能全面的描述实体间的信任度。

2.3.2 PTM信任模型

Almenarez F[67]等人提出了一个普适环境下的动态信任模型PTM(Pervasive Trust Management Model Based on D-S Theory)，PTM模型采用证据理论进行信任建模，信任度评估采用概率加权平均的方法，实体间信任关系的评估表达式为：





其中分别表示实体的积极行为（positive action）和消极行为（negative action），实体间的信任度随时间及上下文服务环境的改变动态变化。在PTM模型中，进行实体间信任度评估的流程包括实体间信任度初始化和实体间信任度更新两个部分。根据PTM模型的架构，在特定的上下文环境中，实体间的信任关系可以通过直接或间接的方式建立。信任关系形成后，得到实体间的初始信任值，这个价值就是基础的信念空间。但是，实体间的信任关系会根据实体的行为而改变，通过提供关于实体在交互过程中的表现反馈给证据空间，这个过程叫做信任演化。信任关系的形成和信任演变都改变了实体之间建立的信任关系，这些信任关系由整个模型系统支撑。实体间的信任度和交互活动的可信任度是非常重要的。PTM模型的架构图如图2.8所示。PTM模型中进一步指出通过实体间的信任度计算通常会得到多个可以进行实体交互的推荐结果，PTM模型中计算所有推荐结果()的平均值，然后结合推荐信度进行加权计算()得到最终的交互推荐结果，计算表达式为：



PTM模型主要的功能是实现了对普适网络环境下实体间的信任关系进行管理。PTM模型有许多优点：(1)PTM模型是分散的，不需要在建立层次关系；(2)在信任度更新部分增加了恶意节点攻击的惩罚机制；(3)模型很好的结合了实体间的上下文服务环境因素进行信任度评估，实体间的信任度随时间及上下文服务环境的改变动态变化；(4)PTM整体的计算公式具有良好的数学理论支撑，而且不需要进行复杂的迭代计算，有效的的减少了实体间信任评估的计算量；(5)在PTM中，信任根据实体的行为动态变化，模型中最小化了人工干预，大多数安全管理功能可以自动执行，因此PTM模型很容易在受限设备上执行。

但是PTM模型也存在着一些不足：(1)PTM模型认为普适网络环境下各管理域的信任评价标准是固定，因此模型不能适应不同应用背景下信任评价标准不同的管理域间实体的交互需求；(2)PTM采用概率值的形式来描述信任值，只单纯的考虑实体间信任关系的客观性评价，却没有考虑实体间信任关系的模糊性、主观性和不确定性。

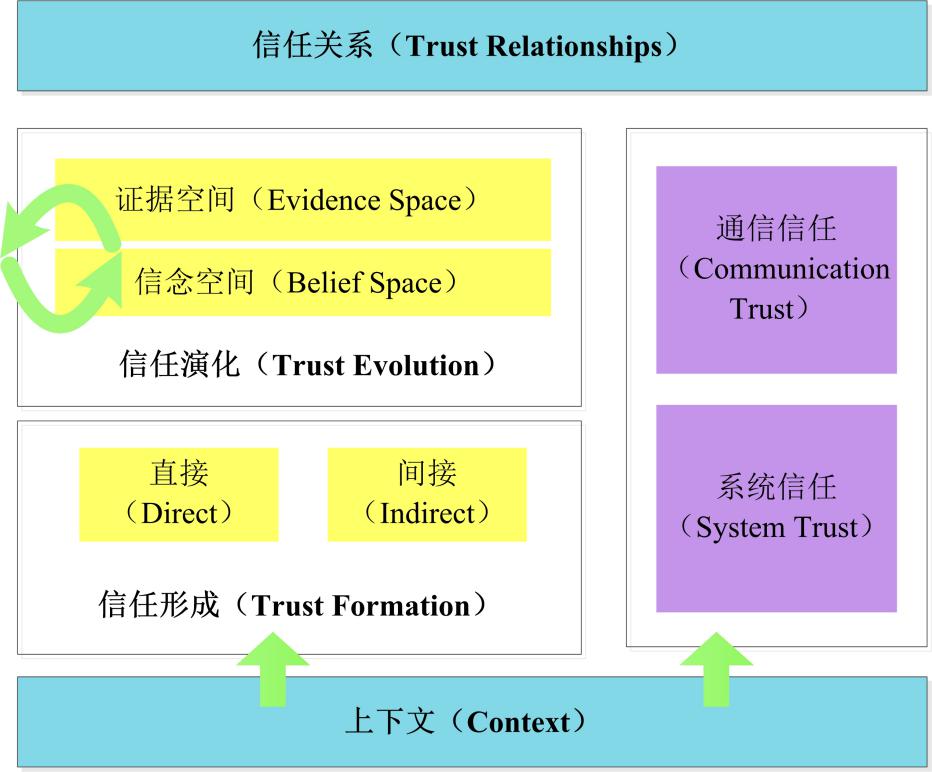


图2.8 PTM模型架构图

2.3.3 CBTM信任模型

文献[68]提出一种基于云模型的信任模型(CBTM\_Cloud-Based Trust Model)，该模型适用于普适网络环境下实体间的信任计算，在实体间不存在直接信任关系的情况下，可以通过实体间的推荐信任关系进行信任度计算。CBTM模型针对实体间的信任关系建立信任云，正常云的定义可以表示为三个数字特征[69]，分别为期望值(Ex)、熵(En)和超熵(He)。利用这些数字特性，可以将不确定概念的模糊性和随机性统一起来。在普适计算环境中，实体通常无法直接从信任邻居实体中获得陌生实体的信任推荐，因此需要信任云传播。模型假设有n个实体，实体集合为，其中实体对于实体的信任云是，那么实体对于实体可以定义为，计算表达式如下：









其中表示为云逻辑乘法运算符号。

CBTM模型中提出在许多情况下，可以计算一个实体的多个信任云，即该实体存在多条信任推荐路径，因此，有必要将这些信任云合并为一个唯一的信任云。假设有m条信任推荐路径，用集合表示，合并后的信任云为：









其中表示为云逻辑加法运算符号。

CBTM模型与以往的信任模型不同，其主要的优点有：(1)CBTM模型考虑了信任的不确定性，以统一的信任云形式描述了信任程度和信任不确定性；(2)在CBTM模型中，应用信任云描述了计算推荐信任值和聚合信任值的算法，算法具有良好的实验性能，实验结果误差小。但是CBTM模型也存在着一些不足：(1)CBTM模型没有将其他因素纳入模型中，例如风险、声誉等，没有考虑在普适计算环境下的欺骗或恶意行为；(2)模型没有具体说明的实体信任值初始化过程；(3)模型没有考虑普适环境下上下文服务环境的动态变化特征，也没有考虑到实体间信任关系随时间变化而呈现出时间衰减性质；(4)模型算法较为复杂，时间复杂度较大，不利于模型的实际应用和扩展。

2.3.4 UTM信任模型

文献[70]提出一种通用的跨域信任管理模型(UTM\_Universal Trust Management Model)用于解决物联网环境中的跨域实体信任评估问题，UTM模型实现了在分布式系统中跨域实体的信任关系建立[71]，因此，UTM模型既可以作为一个独立的信任模型在分布式网络环境中使用，也可以为不同管理域的跨域实体提供跨域信任管理。UTM模型的优点在于提出了代理服务器作为中间桥梁的进行跨域连接和跨域实体间信任度转换的理论，对于不同的管理域采取集中式的管理方式，每个管理域都由代理服务器来负责域内实体的信任度管理以及跨域实体间信任度类型的转换，同时代理服务器负责连接任务，实现了管理域间的连接。但是UTM模型也存在着很多缺点：(1)模型没有明确给出模型的数学理论建模，也没有明确给出跨域实体间信任度评估的计算表达式；(2)模型采用集中式的管理方式，对于代理服务器的存储能力以及计算能力有非常大的要求，但是在实际的物联网环境中，实体的计算能力以及存储能力都是有限的，不能完全满足UTM模型的需求；(3)模型没有明确指出跨域实体间信任度类型的转换方法，不能实际解决物联网环境下跨域实体间的信任关系转化问题；(4)模型没有考虑物联网环境下实体的动态变化特征，也没有考虑到实体间信任关系随时间变化而呈现出时间衰减性质，因此UTM模型的适应性较差。

2.4 本章小结

本章根据物联网的发展情况进行分析，根据物联网环境的特点对于信任进行定义，并描述了信任的特征以及信任关系的评价等，同时分析了典型信任模型的特征，并针对物联网环境下典型的信任模型进行优缺点分析。

本章对物联网环境、信任、信任关系以及典型信任模型的研究，为下文物联网环境下跨域实体信任模型的设计与实现奠定了理论基础。