

中图分类号: TP393

单位代码: 10231

学 号: 2018300598



硕士学位论文

面向边缘设备的信任评估机制研究

学科专业: 计算机技术

研究方向: 网络与信息安全

作者姓名: 王甜甜

指导教师: 李 晶 副教授

哈尔滨师范大学

二〇二〇年六月

中图分类号：TP393

单位代码：10231
学 号：2018300598

硕士学位论文

面向边缘设备的信任评估机制研究

硕 士 研 究 生：王甜甜
导 师：李 晶 副教授
学 科 专 业：计算机技术
答 辩 日 期：2020 年 5 月
授予学位单位：哈尔滨师范大学

A Thesis Submitted for the Degree of Master

RESEARCH ON TRUST EVALUATION MECHANISM FOR EDGE DEVICES

Candidate	: Wang Tiantian
Supervisor	: A.P. Li Jing
Speciality	: Computer technology
Date of Defence	: May,2020
Degree-Conferring-Institution	: Harbin Normal University

目 录

摘 要.....	I
Abstract.....	II
第 1 章 绪论	1
1.1 研究背景及意义	1
1.2 国内外研究现状	3
1.2.1 边缘计算隐私保护和数据安全研究现状	3
1.2.2 信任评估机制的研究现状	5
1.3 研究目标与主要工作.....	6
1.4 论文组织与结构	6
第 2 章 边缘计算概述	8
2.1 边缘计算系统架构	8
2.1.1 边缘计算基本特征.....	9
2.1.2 边缘计算应用场景.....	10
2.2 边缘计算研究现状	13
2.3 边缘计算面临的问题.....	15
2.4 本章小结.....	17
第 3 章 信任评估内容和框架.....	18
3.1 信任与可信.....	18
3.1.1 信任定义	18
3.1.2 可信定义	19
3.1.3 信任属性	19
3.1.4 信任获取	20
3.2 信任机制定义与分类.....	20
3.3 动态信任机制基本内容与框架	21
3.4 信任机制存在的问题.....	23
3.5 本章小结.....	24
第 4 章 边缘设备动态信任评估机制	25
4.1 边缘设备身份信任认证.....	25
4.1.1 身份认证架构.....	27
4.1.2 身份认证模型设计.....	29
4.2 边缘设备行为信任评估.....	30

4.2.1 基于改进的贝叶斯方法的直接信任评估	30
4.2.2 基于改进的灰关联分析的间接信任评估	32
4.2.3 行为信任度计算及更新	35
4.3 边缘设备综合信任度.....	36
4.4 本章小结.....	37
第 5 章 试验与结果分析.....	38
5.1 试验环境.....	38
5.2 试验结果与分析	38
5.2.1 可靠性分析	38
5.2.2 准确性分析	41
5.2.3 系统开销分析.....	42
5.2.4 信任值分析	43
5.3 本章小结.....	44
总结与展望	45
参考文献	47
攻读硕士学位期间所发表的学术论文	51
哈尔滨师范大学学位论文独创性声明	52
致谢	53

摘 要

随着 5G 网络的普及和物联网技术的飞速发展，加速了万物互联时代的进程，同时也转变了位于网络边缘的终端设备的持有角色，从单一的数据使用者转为既产生数据又使用数据的双重角色，传统的云计算模式已无法支撑众多终端设备产生的海量数据，因此，边缘计算应时而生。边云结合的集中式处理模型，可以高速有效地处理海量数据。边缘计算是开放式的环境且具有实时性、动态性、复杂性、资源受限性等特性，也会引发环境中设备安全和数据隐私泄露的问题。在边缘计算环境中，对于边缘设备的可信度是否可以有效地被评估成为一个重要的研究课题。

本文将边缘设备的身份信任和行为信任度进行融合，提出了一种边缘设备动态信任度评估模型。首先根据边缘计算环境的基本特性提出了适用于边缘计算环境的基于 SM9 标识算法身份认证方案，利用 SM9 标识算法对边缘设备进行单域和跨域的身份认证；其次，利用时间退化因子、引入满意度函数修正贝叶斯方程，结合激励机制进行评估边缘设备间直接信任度，并利用改进的灰关联分析法确定指标权重评估设备的间接信任，进而融合直接信任度和间接信任度得出设备的行为信任，同时利用动态更新因子，动态更新行为信任值；最后根据设备的身份认证结果和行为信任度综合得出边缘设备的综合信任度。

通过仿真分析，本文模型中身份认证方案具备良好的安全性和较低的宽带开销，同时相比其他模型，本文模型在降低恶意设备中误检率的同时一定程度上提高了设备间交互成功率，并且验证了该信任评估模型在时间开销方面优于其他模型，结果表明本文模型能够更准确高效的评估边缘设备的信任度。

关键词 边缘计算；信任评估；身份认证；信任度

Abstract

With the popularization of 5G network and the rapid development of Internet of things technology, the process of Internet of things has been accelerated. At the same time, the role of terminal equipment on the edge of the network has been changed from a single data user to a dual role of both generating and using data. The traditional cloud computing mode has been unable to support the massive data generated by many terminal equipment. Therefore, edge computing It comes from time to time. The centralized processing model combined with edge cloud can effectively process massive data at high speed. Edge computing is an open environment and has the characteristics of real-time, dynamic, complexity, resource constraints and so on. It will also cause the problem of device security and data privacy disclosure in the environment. In the edge computing environment, whether the credibility of edge devices can be effectively evaluated has become an important research topic.

In this paper, the identity trust and behavior trust of edge devices are combined, and a dynamic trust evaluation model of edge devices is proposed. Firstly, according to the basic characteristics of the edge computing environment, an identity authentication scheme based on SM9 identification algorithm is proposed, which is suitable for the edge computing environment. The SM9 identification algorithm is used to authenticate the identity of the edge devices in single domain and cross domain. Secondly, the time degradation factor is used, the satisfaction function is introduced to modify the Bayesian equation, and the incentive mechanism is used to evaluate the direct trust between the edge devices. The improved grey relational analysis method is used to determine the index weight to evaluate the indirect trust of the device, and then the direct trust and indirect trust are integrated to get the behavioral trust of the device, and the dynamic update factor is used to dynamically update the behavioral trust value; finally, the comprehensive trust of the edge device is obtained according to the authentication result and behavioral trust of the device.

Through simulation analysis, the authentication scheme in this model has good security and low broadband cost. Compared with other models, this model can reduce the false detection rate in malicious devices and improve the success rate of interaction

between devices to a certain extent, and verify that this trust evaluation model is superior to other models in terms of time cost. The results show that this model can be more efficient Evaluate the trust of edge devices accurately and efficiently.

Keywords edge computing; trust evaluation; identity authentication; trust degree

第1章 绪论

边缘计算的产生并不是代替云计算，而是弥补云计算环境中存在的实时性、能耗、安全性等问题的缺点，进而提高万物互联网络中数据交互的传递效率^[1]。但边缘计算是一个开放动态的环境，隐私保护和数据安全也是边缘环境面临的重要问题^[2]。随着对边缘计算的深入研究，对边缘计算环境中设备可信评估的研究也被广泛关注，同时设备可信也是解决边缘计算环境安全的首要问题之一。

1.1 研究背景及意义

随着 5G 业务兴起和物联网技术的飞速发展，万物互联的趋势日渐加深，许多业务应用场景不断涌现，例如：智能电网，无人驾驶，移动支付，位置服务等，相应场景中智能传感设备的使用也呈直线式状态增长，随之众多智能传感设备会产生海量的数据^[3]。根据思科云最新的数据流量预估，预计至 2021 年，全球的数据流量会呈现出惊人的 19.5 泽字节^[4]。据华为公司预测，如图 1-1 所示，未来五年内物联网接入智能设备将无限趋向于 1000 亿^[5]。

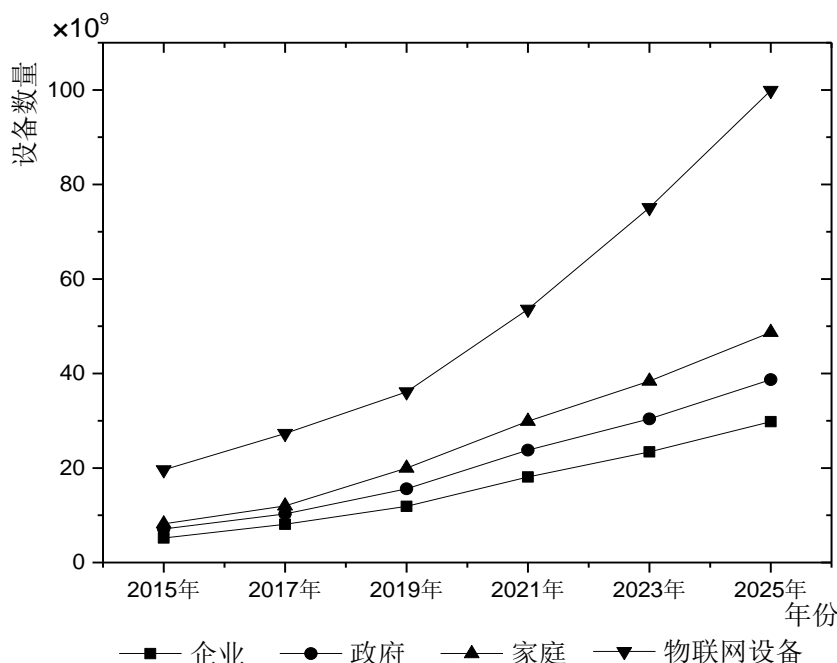


图 1-1 物联网设备预测增长趋势

Fig.1-1 Internet of things devices forecast growth

2016 年 11 月，国际上成立了边缘计算产业联盟组织，该组织由华为技术有限公司、Intel、中国科学院沈阳自动化研究所、中国信息通信研究院等多领域公司联合成立；工业界 Cisco 公司提出了与边缘计算基本理念完全切合的“Fog Computing 雾计算”，它主要关注着环境中可信执行和硬件部署技术等方面的内容；目前边缘计算与工业应用的结合处于萌发时期，随着学术界和工业界也开始对边缘计算方面的前沿技术的密切关注，推动着有关边缘计算的科研和产业结合的创新与发展，为未来我国万物互联的时代发展奠定了坚实基础。在传统的云计算模式的架构中，是智能设备产生的数据通过网络上传至云端进行处理。云计算的计算模式具有动态性、灵活性、按需计算等基本特征。云计算避免了传统计算模式存在的弊端：独占资源；数据中心业务集中性低；企业应用部署繁杂，周期较长，资源利用率低下等，很难满足 IT 灵活运行的要求^[6]。而如今，我们逐渐进入万物互联的新时代，对于万物互联的交互形式不仅限于物与物的互联，而且提升到人与物的互联的高层次。它也使环境中的万物具有语境感知的功能、使对数据的处理进行更强更有效地计算，能将设备与数据信息巧妙地整合至互联网中。与此同时，边缘设备节点具备了处理并计算各种不同种类的数据的功能，再通过云计算服务中心进行协同合作，为系统用户提供高效便捷的服务。但随着广泛的分布式智能设备在万物互联环境中被使用，海量的数据上传至云平台，造成了传输通道的堵塞，以及独占资源的问题，利用云计算模式解决此问题比较困难^[7]，而边缘计算技术可以很好的解决该类问题。

以传统的云计算的集中式数据处理的中心化方式的自身特点，直接导致这种计算架构无法推广。其弊端集中表现在：1) 由于边缘设备的急剧增长，导致边缘数据呈直线式增长，面对海量的数据，云计算无法实时的进行处理和统计；2) 海量的数据通过网络传输至云中心，则会使宽带负载加大，导致网络延迟；3) 边缘设备产生的数据涉及用户个人隐私，使得边缘计算环境中的安全问题也变得更加严峻；4) 资源能力有限的边缘设备无法低耗的传输到云中心，会消耗大量电能和传输过程中的能源。基于传统云计算架构的不足之处，边缘计算应运而生以及 5G 的快速发展，更好的将边缘计算技术和云计算融合，使部分数据转移至具备计算能力的网络边缘侧的设备进行处理^{[8][9]}。

边缘计算被定义为靠近数据产生者或数据源头的网络边缘侧，将存储、计算、网络、应用、智能五个种类资源融合的分布式开放平台，边缘计算被学者认为是一种新的计算模式^{[10][11]}，它可以通过在网络边缘侧进行数据的处理和计算，提高环境的服务性能和控制能力，从而促进万物互联中新模式新业态，也使得边缘计

算的新型计算模式具有感知性、复杂性、实时性等特点，云计算环境对于保证数据安全和隐私保护安全问题的研究成果已经不再适用于海量设备存在的边缘计算环境，致使边缘计算环境中对于数据传输、计算、共享等过程的安全隐私问题则日益突出。边缘计算环境安全包括网络、设备、应用、数据等方面的安全，同时，保证数据的保密性和完整性，用户个人隐私的保护等方面也是安全领域的重要内容。由于边缘网络面临海量的数据，而由边缘设备产生的数据带有用户的个人隐私的因素，这使得环境中的数据可信处理以及隐私安全问题明显突出。如何将身份、可信数据处理融合，在多元化的应用服务环境下提供安全的服务是重要的研究方向。

2015 年底，乌克兰电力网络环境被黑客大范围攻击，导致城内出现大停电的情况。2016 年，美国域名服务器管理机构遭受到了分布式拒绝攻击，该事件的源头是以路由器、智能摄像头为入侵路径的 Mirai 病毒。2017 年，360 发现与 Mirai 类似病毒 IoT_Reaper，它利用物联网设备存在的漏洞进行病毒传播，其破坏力比 Mirai 病毒更大。针对危机环境的安全事件的不断发生，更是让全球学者目光聚焦在针对边缘计算安全的问题上。与云计算一样，将可信计算的技术巧妙的融入边缘计算的环境中，在环境中使用经过身份认证的设备组成的可信边缘平台是安全研究的基础，如何增强边缘计算环境的安全可靠的信任交互，是目前边缘计算环境安全的重要研究之一。

1.2 国内外研究现状

1.2.1 边缘计算隐私保护和数据安全研究现状

边缘计算是近几年来研究的热门领域，它不是为代替云计算而产生，而是与之相互协同。云计算的计算模式与万物互联环境特征之间存在着不共融的矛盾，单纯以云计算的集中式计算方式，难以支撑万物互联中海量的应用程序也无法实时处理物联网中设备产生的海量数据，边缘计算应运而生。边缘计算是一种靠近在网络边缘侧和数据源处处理数据的一种计算新模式，借用融合计算，网络，存储为一体的边缘计算平台，提供实时、动态的服务计算，在数据源附近进行处理的计算方式也为解决数据安全和隐私保护的问题提供了更好的结构化支撑。随着 5G 的发展和对边缘计算模型更深入的研究，产业界和学术界针对边缘计算分支雾计算^[12]、移动边缘计算^[13]和移动云计算^[14]等也进行相应研究。

目前，对于边缘计算的隐私保护和数据安全相关的研究还处于不成熟期，主要的研究是借鉴云计算相关领域在数据安全隐私方面问题的研究，并且学者们也

对移动云计算的隐私和安全性问题进行了深入研究。**Roman**^[15]等人对常见的移动边缘范式环境中存在的安全问题进行深入分析,同时也提出了一种协同式的安全保护系统,针对已有问题研究学者提出了相应的意见,也为边缘计算的安全性问题的研究提供了理论性的参考。

针对数据安全的问题,边缘计算的解决方案是将其他计算模式下的数据安全方案移植到边缘计算模式中,根据边缘计算分布式结构和设备终端资源限制的特性进行调整,最终实现适应于边缘计算环境的数据安全保护系统。**Wang**^[16]等人通过改进访问集成文件层的结构进行加密处理,提高了加密效率从而提高了数据的安全性能。**Khan**^[17]等人提出了一种合基于代理和云的双重加密方案,在保证数据安全的同时又将成本最小化。**Zuo**^[18]等人提出了一种基于雾计算的加密方法——外包解密能力的属性加密方法(OD—ABE),并通过实验验证证明了该加密方案的安全性。

边缘计算是一种分布式交互系统,该系统中存在多个可信域,在该系统中,若是仅为环境中的每个实体进行身份标识是不足以保证用户隐私的,需要在环境中不同可信域中进行相互的信任验证。2015年**Liu**^[19]等人提出了一种用于共享权限的隐私保护认证的协议。**Tsai**^[20]等人提出了一种可以应用在分布式云环境中的隐私保护的匿名身份认证方案。**He**^[21]等人在2016年提出了一种基于身份签名的隐私保护认证方案,并对其进行分析验证方案的安全性。**Yang**^[22]等人提出了一种高效的动态审计协议,该协议利用结合密码技术和双线性对中线性性质的方式代替现有的随机掩码技术,进而提高隐私保护的能力。**Mahmood**^[23]等人针对智能电网系统中的安全问题提出了一种基于轻量级ECC的认证方案。有效抑制了恶意攻击,并验证了其方案的低耗和高效性。访问控制技术也是在数据安全和隐私保护研究中的一种策略和手段。访问控制技术是可以应用在多不同环境领域之间进行节点的访问控制,并且考虑多种外部因素进行访问控制。**Jin**^[24]等人为保证数据的安全性,提出了一种基于轻量级加密访问数据的安全策略,可以保证在数据的机密性。**Zhang**^[25]等人利用将外包能力和属性更新能力结合,提出了一种新的访问控制策略。**Huang**^[26]等人对外包能力和属性更新能力的访问控制策略进行扩展,提出了在此基础上又包含密文更新方法的访问策略。

目前对于隐私保的研究主要集中在雾计算和云计算的环境中。**Bahrami**^[27]等人提出了一种轻量级的加密方法来存储数据,采用混沌系统的伪随机置换方法,将操作从云端拉低至设备上,从而保护数据隐私。**Chen**^[28]等将分布式缓存处理技术引入位置隐私保护方案中,从而保证位置数据的隐私。**Niu**^[29]等为实现移动用户

的位置隐私提出了一种用熵量化隐私度量的缓存感知的虚拟选择算法，有效验证了该方案可行性。

1.2.2 信任评估机制的研究现状

无论是互联网还是物联网中身份信任、行为信任都是可信计算技术中研究的重要内容，目前针对于边缘计算环境中的信任机制的研究在基于云计算环境的基础上，而边缘计算环境中的可信评估是根据设备的行为信任度进行评估设备行为的安全性特征。

学者针对边缘计算环境的信任研究，学者在 PTM 的研究项目中提出了一种动态的设备可信的设备信任评估模型，该模型是采用概率加权的方法来对用户的信任度进行评估；在 PET 项目中，学者在研究的基础上，提出了一种基于风险和反馈可信耦合的评估模型，用来计算 P2P 网络中节点在文件共享过程中的可信度。宁振宇^[30]等人对现有的可信执行环境进行详细描述并针对有效评估环境中设备节点的信任度，进而对环境中数据安全方面进行分析，针对如何在边缘计算环境下建立较为安全可信的执行环境做了详尽的分析。张佳乐^[2]等人对从数据安全和隐私保护两个方面进行了边缘计算环境的详细的描述，并将环境中信任域和设备实体之间的关系引入，研究不同的信任域中的设备实体的存在的身份问题，并且提出各层所存在的安全威胁。Chen^[31]等人提出适用于小型蜂窝网络（SBSs）中的一种基于合并分割规则的分布式联盟信任算法，文中定义描述了 SBSs 之间的信任关系，这种关系是通过社会信任网络产生，由连接它们的最短路径传播信任来计算彼此之间的信任关系。邓晓衡^[32]等人针对边缘计算环境中的隐私信任和数据安全问题，以及根据需求如何提升用户的体验质量（Quality of Experience, QoE），提出了根据综合信任的边缘计算多层自适应的边缘计算的数据结构，并且进行任务调节分配，通过试验验证了该模型的有效性，但作者只是利用节点之间的主观评价，忽视客观因素所以该模型存在一定的局限性。Huang^[33]等人提出一种分布式声誉管理方法，采用安全高效的车辆边缘计算和网络，为了保证网络安全保护重点研究了声誉管理，运用加权主观逻辑对系统中信誉进行数据更新。Yuan J^[34]等人提出了一种基于多源反馈信息融合的物联网边缘设备可靠、轻量级的信任机制，该信任机制主要是用风险模型评估直接信任，基于信息熵的方法计算推荐信任，该信任计算机制提升了计算速度和信任的可靠性，但文中没有体现对恶意节点的处理，使信任评估准确度不高。

无论在任何计算环境下，信任评估机制是不断被学术前沿的学者提出，但这些模型算法中普遍存在着某些不可被忽略的问题，只关注交互结果忽略了影响结

果的其他因素和身份是否可信的因素，且没有考虑时间因素，使模型无法有效且及时的抵制恶意欺骗等恶性行为；对于非重要推荐设备权重过高，不符合常规逻辑。所以，信任评估机制依旧是学者研究安全的非常重要的一项课题。

1.3 研究目标与主要工作

本文通过对边缘计算环境中的设备信任机制的研究，将融合设备的身份认证和行为信任进行构建信任评估机制。根据边缘计算环境的特征，本文提出了一种针对设备的动态自适应的信任评估机制，最后通过分析试验结果得出结论并验证方案的可行性技术路线。

本文的研究内容和工作：

(1) 通过查阅边缘计算相关资料，分析边缘计算目前的发展趋势以及面临的安全问题，并且理解边缘计算服务模式的特性和边缘计算模式在用户应用的需求特征，且考虑利用对设备的身份认证来优化边缘计算系统的可信问题。

(2) 构建基于信任评估机制的边缘计算框架：将身份、行为信任综合评估终端设备的信任并且进行建模，用以评估边缘计算环境中终端设备可信，从而提高交互成功率。

(3) 对边缘计算的终端设备的可信度评估进行研究：由于设备间交互结果由多种因素影响，使用满意度因子修正的贝叶斯方程并引入激励机制进行评估边缘设备间的直接信任，并抑制恶意节点的信任值增长速度；其次，利用改进的灰关联分析方法确定指标权重的方法进行改进量化推荐设备节点在间接信任计算中所占比重的准确度，间接信任和直接信任综合形成行为信任并加入设备的身份认证，最终得出设备的最终信任值。

1.4 论文组织与结构

结合本文的研究内容，根据研究工作的需要，本文分为五个章节，每章具体内容如下：

第一章，通过查阅和学习，对边缘计算信任评估机制进行分析，阐述了研究主题的背景和意义，并分析阐述了边缘计算中隐私保护和数据安全的问题、有关信任评估模型方面的相关的研究现状、工作进展以及研究的内容，最后阐明了本文边缘环境可信环境的研究目标与研究内容和全文的章节组织结构。

第二章，针对第一章的内容，详述边缘计算的系统的整体架构，分析边缘计

算基本特征应用场景，并针对边缘计算的研究现状和问题进行重点分析，引出边缘计算的安全问题和边缘终端设备的可信性研究，也为下面几章的研究学习奠定坚实的理论基础。

第三章，描述有关信任的相关概念以及信任评估机制的框架，以及阐述信任在不同方面的研究，分析信任的属性以及介绍了信任评估模型的定义域分类，为本文的建立信任评估模型提供丰富的理论依据以及指明研究方向。

第四章，根据前几章的研究，提出一种边缘设备动态信任评估模型，给出了验证终端设备的身份认证协议，并且对处于边缘计算环境中的终端设备的行为进行信任度评估，在直接信任评估过程中引入满意度函数，时间退化因子改进的贝叶斯方法的直接信任评估和基于改进的灰关联分析的间接信任评估，最后将终端设备的身份信任和行为信任融合，最终实现高效的信任评估机制。

第五章，本章是试验和结果分析的章节，通过仿真试验并结合对比其他模型进行，从而验证本文提出的模型的可行性以及高效与可靠性。

第 2 章 边缘计算概述

边缘计算是将应用、存储、网络、计算、智能等五种资源集中在网络边缘侧的计算模型，为应用提供服务的同时可以提高开放性网络的控制能力又可以提高网络服务的性能，边缘计算作为新型计算模式可以被应用于物联网、互联网多种不同的场景中，边缘计算概念被提起最早源于 2003 年，IBM 和 AKAMAI 开始在类似边缘计算的 WebSphere 服务器中为用户提供的合作，所以边缘计算的兴起时内外力共同合作的结果，也是必然趋势。

2.1 边缘计算系统架构

本文的研究适用于分布式边缘计算环境下边缘设备的信任评估。图 2-1 为基于云平台的边缘计算设备交互环境，该架构分成三层：云计算中心、边缘计算层和边缘设备层。由于本文只是针对解决边缘计算环境中边缘设备信任评估问题，我们假设云计算数据中心层中数据计算和数据反馈过程是可靠的，并且数据具有有效性。边缘计算环境中的信任评估主要是在边缘计算层和边缘设备层，边缘计算层用于监视边缘设备的服务行为以及接收边缘设备的信息反馈并进行数据融合，并对接入的终端设备进行身份认证；边缘设备层的设备进行交互协作共同完成任务，并计算交互过程中的直接信任度。评估设备会向边缘计算层发送请求获取被评估设备的信任值以及身份认证标识，边缘计算节点会通过广播的方式通知邻近节点并获取反馈值。

边缘计算环境主要是依靠设备节点层和边缘网络节点层完成信任的计算，由于对边缘设备的信任计算需要及时响应，更有效率的执行，所以不需要将数据上传至云计算中心平台层。由于经常不可预测的网络延迟和昂贵的带宽以及设备节点层会产生海量的反馈数据，云计算数据中心的数据处理能力不能满足延迟敏感应用程序的严格要求。在云计算平台的条件约束下，缩短数据处理时间以实现实时响应应用、高效的提高数据处理和降低网络压力，需要在边缘计算环境下进行执行可信计算。

在边缘计算的环境中，基于边缘设备之间的内在关系以及边缘设备与边缘网络节点的内在关系，首先，我们构建了基于边缘计算的可信数据反馈的边缘设备层和边缘网络节点之间的系统架构（如图 2-1）。在图 2-1 中，根据边缘环境中实体在

信任计算中的作用，参与信任计算的实体分为两类：边缘设备和边缘网络节点，因此在此信任计算架构中可以形成两种实体集——边缘设备实体集（ $ED = \{ed_1, ed_2, \dots, ed_i, \dots, ed_n\}$ ，其中 i 为边缘设备的编号， n 为在边缘计算中参与信任计算的边缘设备总数）；边缘网络节点实体集（ $ES = \{es_1, es_2, \dots, es_k\}$ ， k 其为参与的边缘网络节点的总数）。在此边缘计算的信任计算的实体集架构中，首先是有边缘计算层节点对接入设备进行身份认证识别，其次计算边缘设备实体集之间评估节点与被评估节点的直接信任与边缘设备反馈的其他设备节点对被评估节点的间接信任，最终信任评估结果是由边缘计算节点 ES 进行计算。

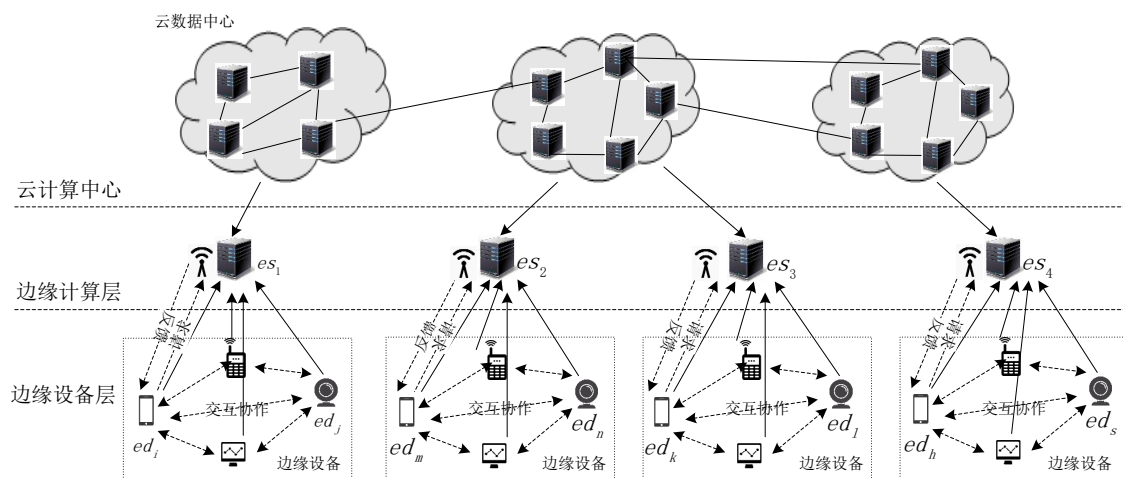


图 2-1 边缘计算设备交互环境

Fig.2-1 The interaction environment of edge computing device

2.1.1 边缘计算基本特征

边缘计算、移动边缘计算和多接入边缘计算就是在无线接入网内提供数据处理的信息技术和云计算的能力，并可以将数据处理靠近于移动端。因此边缘计算是也被学者认为是将云计算能力下沉到具有数据计算能力终端设备的一种新技术，在该技术中边缘计算层被视作小型的云服务器，在边缘侧进行数据处理的同时执行特定的任务。对边缘计算的特性的研究总结，可以将边缘计算的基本特征归为一下5个方面：

1) 低时延：边缘计算中将数据处理移至终端设备的地方，由于产生的数据不会经由网络上传至云计算中心集中进行处理，因此减少了上传数据的时间从而降低运行中的时延，提升了边缘计算环境设备交互的响应时间和用户体验，也减小了传输过程中的数据拥塞。

2) 本地化：边缘即指本地化，指明异于云计算模式，边缘计算可以独立于网络，依附于边缘计算平台的终端设备可以随时获取本地产生的数据进行处理。

3) 位置感知: 边缘网络也属于无线网络中的一部分, 边缘计算可以利用传感器产生的微弱信号判别接入边缘网络中的传感器的位置, 以便于对网络中的设备的位置进行维护。

4) 邻近: 即在靠近数据源信息获取终端设备的数据并进行及时处理, 这便于对用户设备的关键信息进行捕捉, 获取大量的用户数据可以进行大数据分析, 对于网络环境中用户流量的分析, 用户所居位置的跟踪定位等处理。

5) 网络内容信息: 边缘计算所处的无线环境以及在实时网络环境中, 边缘设备产生的数据, 都是被应用程序或某中特定的服务使用以便于提供上下文服务, 这种数据信息对于实时的要求较高, 该特性可以有效实时的对无线网络中信息进行处理和维护。

从效益的角度来看, 无论是业务效益还是技术效益方面, 边缘计算平台的发展都为某些应用场景提供了一种新的价值链。不论是设备商还是运营商或是软件开发商等, 都可以参与到边缘计算环境, 同时可以利用该平台拓展全新的业务模型, 为用户提供高效的服务也从中获取到利益。

2.1.2 边缘计算应用场景

随着边缘计算在万物互联中的推广普及, 边缘计算这种新型计算模式将会随之应用到场景中, 随着技术的推进将逐渐实现边云协同的计算模式, 与云计算协同, 将会得到普遍的应用, 新的技术和算法的产生只有通过应用的实践才能准确评估新技术和算法的适用性。因此, 边缘计算的新型计算模式的对用户的价值大小主要是取决于边缘计算在各领域的适用度, 只有在应用环境中通过实际的应用中才能将边缘计算在生活中面临的机遇和挑战显现出来, 下面针对视频监控、智能家居和车载边缘计算应用场景进行阐述。

(1) 边缘计算视频监控应用场景

视频监控系统^[35]是主要针对视频处理、人员追踪和目标跟踪和查询, 多用于因人或事引起的新的社会管理与犯罪性的问题。随着互联网的发展, 人们对公共安全的问题的发展也更加关注, 在传统的监控系统中众多监控设备资源受限使计算处理数据的能力不足, 致使现行的智能监控系统中对于海量数据处理的能力也存在一定的问题。因此, 为了提升现行的智能监控系统中的监控设备的数据计算处理能力, 进而预防恶性行为的预警和对各种刑事案件问题的处理问题, 所以边缘计算的计算模式的出现有益于视频监控系统的发展。

目前监控系统依附于云服务中心, 但监控系统设备不定时上传海量视频数据, 云计算计算模式对大量数据的计算和处理能力有限, 现对监控系统进行如下研究:

(a) 一种基于边缘计算的视频图像处理技术, 该技术是对视频图像进行预处理获取数据信息的研究, 并将无用的信息进行排除, 减小存储空间, 从而提高上传速率和对图像处理的高效性。(b) 基于边缘计算的视频处理平台环境, 目的是从监控系统中获取视频图像并实时的进行行为特征提取, 并实时的对特征数据进行数据分析, 进而实现行为感知的视频特征数据处理的实时策略。

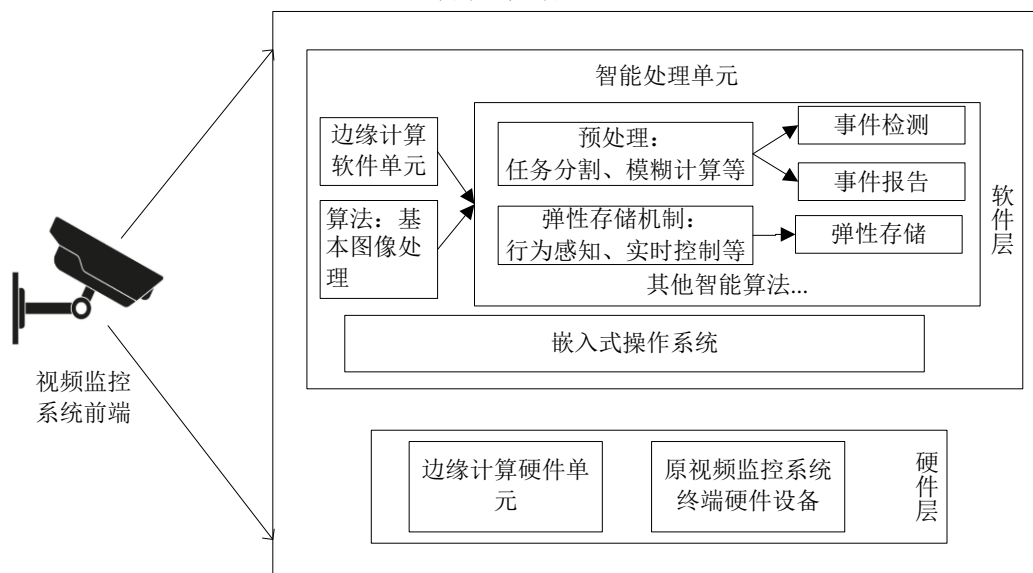


图 2-2 基于边缘计算的视频监控系统

Fig.2-2 Video surveillance system based on edge computing

图 2-2 为基于边缘计算构建的视频监控系统, 它主要是根据边缘计算特有的特征, 致使它可以实时的将数据在数据产生源附近进行计算和处理, 利用目前对视频数据的预处理算法进行图像预处理, 进而对设备产生的视频数据进行实时性的处理以便为用户提供实时响应的服务。Sun^[36]等人对提出的基于边缘计算的智能监控系统进行了可用性的研究, 以及设计了存储性较高的模块, 提高了对现实监控场景的视频存储利用率。

目前, 在公共安全领域方面视频监控系统的安全问题也越来越备受关注, 基于边缘计算监控环境不仅提高数据处理的算力和存储利用率, 还降低了数据的传输时延, 以便于更好的将基于边缘计算的监控架构应用与公安领域。

(2) 边缘计算在智能家居的应用场景

在万物互联的时代, 智能家居是这个时代的一个重要实践的应用场景^[37], 智能 TV、智能机器人、智能监控等都是智能家居中的智能化设备。在智能家居应用场景中, 不仅有联网的终端设备还有多个传感器部署于智能家居环境中, 数据隐私和传输负载都是智能家居环境中考虑的问题, 针对该问题需要在该环境中对其

处理，但基于云计算的智能家居无法满足需求，而边缘计算具有的特征刚好适用于数据源处对数据进行处理。文献[38]提出了一种高效的基于边缘计算的智能家居服务系统，如图 2-3，在该环境中，智能网关参与边缘计算服务的控制任务，它既可以进行服务选择也降低设备能耗，由于智能设备中所使用的通信技术有所差异，所以通过智能网关进行连接智能设备，为智能设备间数据交互提供服务接口。

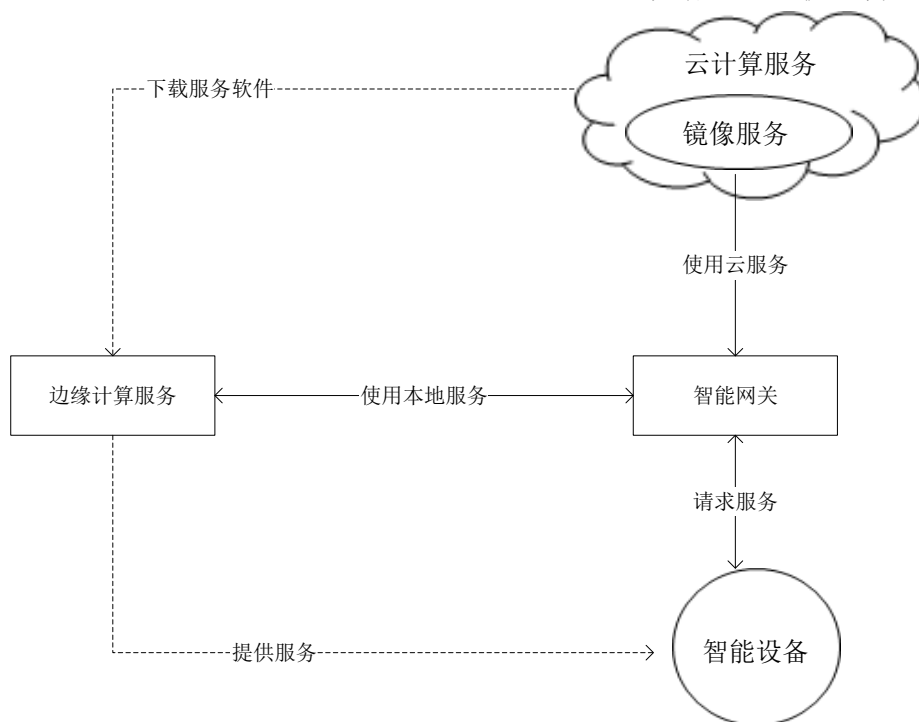


图 2-3 边缘计算在智能家居的应用场景

Fig.2-3 Edge computing in the smart home application scene

（3）智慧城市

信息技术发展过程的产物之一便是受人们关注的智慧城市，目的是对人们所居的城市实现智能化的连接管理和运行，使居民生活更加便捷。2016 年阿里云将“城市大脑”的基本理念带入生活，目的是利用“城市大脑”的理念实现城市多方资源更好的管理城市，快捷方便的服务居民。2017 年 10 月由 Alphabet 建造的 Quayside 的高科技新区，创建者希望通过该项目引领智慧城市的发展。在智慧城市的建设环境中数据来源于多源设备，并会产生异构数据，在对多源移动的数据进行处理同时还要保障城市居民的隐私和安全的问题，因而利用边缘计算平台将数据转移至网络边缘侧进行处理是解决该问题很好的方案。环境检测、噪音水平等城市环境数据都可以根据分布在城市中的传感器收集信息。在无人驾驶环境中，如果将环境中多方传感器数据传输至云计算服务中心则会增加实时数据的难度，

影响无人驾驶的操作。在智能交通领域，移动自组网的应用实例车辆网络，通过车辆间的交互或由各车辆与路侧设施间的不断进行无线通信，获取数据并进行分析从而保证行车驾驶过程中的安全、高效、舒适的体验。根据文献^[39]提出一种基于边缘计算的智能城市操作系统，如图 2-4，提高了该系统中数据共享的深度和广度。

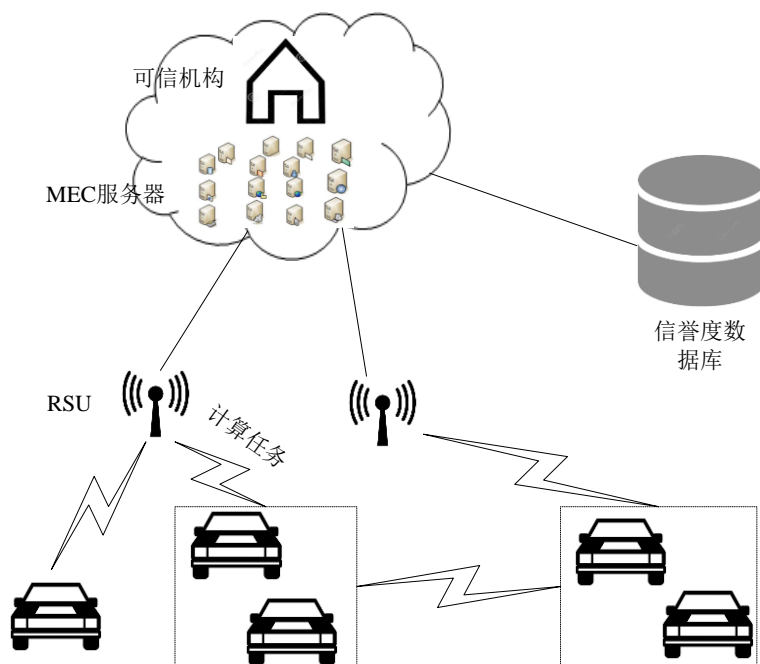


图 2-4 基于边缘计算的智能城市操作系统

Fig.2-4 Intelligent city operating system based on edge computing

文献[40]提出了一种车载边缘计算的卸载方案，在该方案中移动自组网中的车辆可以将任务卸载至其他相邻的移动边缘计算的服务器上进行处理，对于相邻的车辆信誉值进行资源调配，进而高效高量的完成任务，提高用户体验和用户的满意度。智慧城市中对与边缘车载的计算形式有着时延敏感和实时性高的特性，更好的为智慧城市环境中的交通领域提供高质量的服务。

2.2 边缘计算研究现状

至 2019 年以来，根据在谷歌学术上统计数据来看，以“Edge Computing”为关键字进行搜索的文章数量每年呈逐步增长的形式，如图 2-5 所示，以 2015 年为分界线，在 2015 年之前，该阶段为边缘计算的萌芽发展期；2015—2017 年，边缘计算顺应时代发展慢慢被业界熟知，也引起了学者的广泛研究，为边缘计算的快速增长阶段；2018 年，边缘计算进入平稳发展期。

在万物互联的背景下，边缘计算引起了学术界和业务界的极度关注，使边缘计算迎来了爆发性增长期，为了解决数据的算力、压力负载和信息传输等问题，研究者开始对增加数据产生源的数据处理的功能，其中雾计算、移动边缘计算、海云计算为代表计算模型。

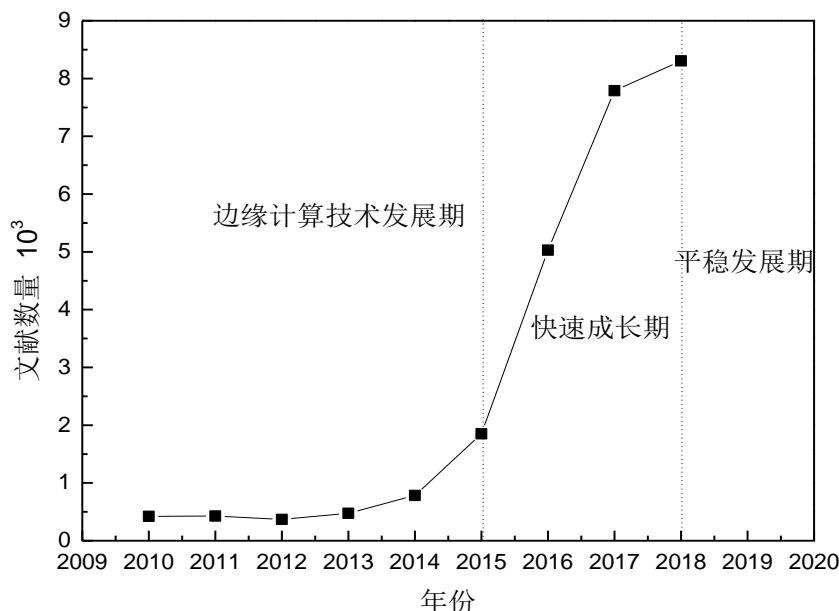


图 2-5 谷歌学术边缘计算搜索增长形式

Fig.2-5 Google academic edge computing search growth form

移动边缘计算^[41]意指在移动用户的无线网络范围附近，为用户提供具有 IT 服务和云计算能力的新网络结构。由于移动边缘计算可以处于用户无线网内，更靠近移动用户，所以对用户的服务质量较高且减少了数据处理的时间，降低时延。且移动边缘计算的服务器的层次和架构更加切合，它可为边缘计算模型某阶段进行服务。2012 年，雾计算的概念被思科公司提出，将其定义为一种把云计算中心的数据处理任务迁移至网络边缘设备的虚拟化计算平台。雾计算与边缘计算在计算模式上具有很大的相似性，两者间的区别是雾计算更关注与基础设施间的资源共享问题，而边缘计算的关注范围比较广泛。2013 年，美国研究学者 Ryan LaMothe 在试验室内部报告中首次提出^[42]“Edge Computer”，此时，边缘计算已经含有云服务功能的上行和万物互联服务的下行。在政府方面上，2016 年 5 月，美国自然科学基金委将认为边缘计算可以有效代替云计算进行数据处理，并将边缘计算列为突出领域；10 月，自然科学基金委针对边缘计算面临的重大挑战专门召开研讨会。在学术界，同年 5 月美国韦恩州立大学施巍松教授对边缘计算进行研究并对其给出相关的定义：边缘计算是在网络边缘侧执行数据计算的一种新型计算模型，并

对其研究内容发表论文，文中指出了边缘计算研究中面临的一系列挑战，该文章在 2018 年被研究者引用 650 余次。10 月，IEEE 和 ACM 针对边缘计算的研究联合组织了顶级会议，成为全球首次围绕边缘计算这一概念进行深度研究的科研学术会议，随后，WWW，MiddleWare，ICDCS 等重要的国际会议也随之对边缘计算开始进行专题研讨。工业研究方面，2015 年，欧洲电信标准化协议发表了有关边缘计算的白皮书^[42]，在 2017 年 3 月多组织为了更好的满足边缘计算的应用需求致力于研究边缘计算标准化制定^[43]。2015 年 11 月 OpenFog 联盟致力于推荐边缘计算和应用场景的结合，且该组织在 2018 年年底并入了工业互联网联盟。

国内针对边缘计算的研究步调与全球相比是基本一致的。2016 年 1 月，国内著名的研究机构针对边缘计算在北京成立了边缘计算产业联盟，致力于推动“政产学研用”各个方面的资源合作，并推动边缘计算技术在国内应用场景中顺利持续发展。2017 年 5 月，各组织在合肥 召开中国首届边缘计算技术研讨会，8 月中国针对边缘计算专委会成立，也同时代表着边缘计算在专业学会的发展得到了认可和推动。

2018 年，边缘计算在发展历程中有 4 个重要事件，2018 年 1 月，总结边缘计算的研究全球出版了第一本书籍《边缘计算》^[40]，它从多个角度分别对边缘计算进行阐述。9 月，在上海召开的世界人工智能大会上，以“边缘计算，智能未来”为主题进行了边缘智能的讨论。2018 年 8 月，以“由云到端的智能架构”为主题的全国计算机体系结构学术年会，意味着在学界内的研究焦点由云计算逐渐往边缘计算方向转变。10 月 Eclipse 基金会和 CNCF 基金会展开合作，将 Kubernetes 技术带入到物联网边缘计算环境中，促进其在边缘计算环境中的适用。2018 年之后，边缘计算成为了学术界和产业界中最热门的话题，为民众提供便捷的生活。

2.3 边缘计算面临的问题

目前针对边缘计算的安全研究大多是从其结构特征方面进行的，大多数的研究人员是从研究边缘计算环境的安全性存在威胁这一方面进行研究。参考 Shi^[44]等人对边缘计算架构的分析和研究后，提出了边缘计算面临的安全问题如下。

（1）用户隐私和安全问题

从 Wi-Fi 网络安全的角度进行分析，目前大多数家庭中都在使用无线网络，但在用户使用 Wi-Fi 网络的环境中 49% 都是不安全的，在 80% 的家庭中未重置路由器设备的密码仍在沿用默认密码。对于公共场所的 Wi-Fi 热点，接近 90% 的热点都是不安全的，若用户进行连接则会对用户的个人隐私信息泄露，健康检测仪、网

络监控等设备也会容易被他人利用，致使隐私数据被窥探甚至外泄。

(2) 边缘设备具备双重角色

移动设备手机的数据存储于云服务提供商，并由边缘计算平台进行数据分析，若将数据移交至用户设备处进行存储，将是一种对用户隐私加强保护的方案。边缘移动设备收集的数据应存储于边缘处，并且用户可以有权将数据提供给云服务使用，也降低了设备从云平台请求数据的时延，为保护用户的个人隐私，应该在边缘设备处过滤用户高度个人隐私数据。

(3) 缺乏数据安全防护工具

大多数边缘移动设备资源有限，目前对于数据安全研究方法并不完全适用于边缘计算的环境，而且在开放式的边缘计算环境中，边缘设备面临高度动态的环境，很容易致使边缘网络遭受恶意设备的外部攻击，为加强对用户设备的隐私数据保护，大多数研究学者对隐私数据的加强保护进行研究，但对于边缘计算的数据的处理仍需开发更多有效地工具。

在传统的无线通信环境中，互联环境中的设备节点之间可能会产生嗅探、干扰或其他类型的攻击，在边缘计算环境中，设备节点间的数据交换对数据的准确性要求较高，对于资源受限的设备节点传统的安全方案并不适用于，而在环境中边缘设备节点容易造成数据泄露或攻击，因此边缘计算的安全问题是许多学者研究重点方向。传统网络安全和边缘计算安全的区别总结^[45]见表 2-1，Roman 等人对边缘计算环境和架构进行详细的分析，并对边缘计算环境中可能面临的安全威胁进行了分类。

表 2-1 传统网络安全和边缘计算安全的区别

Table 2-1 The difference between traditional network security and edge computing security		
安全内容	传统网络	边缘计算
法律法规	目前，相关法律比较完善	缺少通用标准，相关法律不完善
数据存储	将数据存放于内网中，对其有操作性的控制	将数据存储于边缘数据中心
安全模式	基本运用于企业内部，采用访问控制技术和防火墙技术对其进行安全维护	环境中，每个边缘设备节点都可能受到攻击
技术差异	初步虚拟化技术	基本采用的是虚拟化技术

虽然基于边缘计算的应用能够带给用户的生活以便利，但对于边缘计算环境中设备交互安全和数据安全方面的研究还处于发展阶段，需要对其技术上进一步完善，对于如何构建合理的防御策略、信任安全机制等方面研究较少，因此，如

何能有效利用设备资源的同时再保护用户的数据安全性，需要对边缘计算执行环境的安全性进行相关研究。

2.4 本章小结

本章首先针对边缘计算系统架构进行相应的分析，其中包括边缘计算的基本特征和阐述了边缘计算应用的场景。其次，从学术界、业务界和政府三方面对边缘计算的研究现状进行分析，从边缘计算运用的技术储备期、技术快速增长期和稳健发展期三个阶段进行阐述。最后，根据研究调研分析了边缘计算目前面临的安全问题，并对传统网络安全和边缘计算安全的区别进行总结，为针对边缘计算环境中的安全问题研究奠定理论基础。

第3章 信任评估内容和框架

边缘计算环境是具有大量的终端设备且开放、动态的分布式环境的特性，给边缘计算的安全带来了一定的挑战性。边缘计算虽然将计算拉近到数据产生源处，但也面临互联网中的非法访问，恶意反馈，拒绝服务等安全问题，每个智能设备涉及用户的个人隐私的问题，还面临着隐私威胁的问题，妥善解决安全性问题以及如何保障环境中数据的安全是所有应用场景中必然面临的问题，也是再推动边缘计算广泛运用过程中首要解决的问题。因此建立面向边缘计算环境的终端信任评估机制是必要的。

3.1 信任与可信

3.1.1 信任定义

信任是人们生活中进行交互的重要的基础因素，例如，交易、通信和交互的环境。在不同研究领域和人文背景下，人们对信任的理解和描述也存在一定的差异。在互联网的时代，信任也是必不可少的，在边缘计算的环境中每一个终端设备之间也是陌生的，节点间信息访问和交互，它们往往也是用信任来维系的。下面对信任进行从心理、数学和社会方面进行解释。

(1) 心理信任 (Trust in Psychology): Morton Deutsch 对心理信任进行了定义：在某一特定的情况中，对与个体预期的收益和成本进行分析。心理信任场景分析：若个人对于前方路的不确定性，最终选择结果的好坏取决于其他人的选择行为。并且，对于选择继续前行的结果伤害大于利益，该人还是选择前行就意味着做出了信任选择，否则就是不信任。

(2) 数学信任 (Trust in Mathematics): 用数字大小度量来定义信任，将信任值度量成数字概率，在 $[0,1]$ 区间内划分信任程度，将0和1定义为极端，0为极不信任，1为完全信任，使人们更直观更便捷的区分和理解信任值。

(3) 社会信任 (Trust in Society): 从社会学的角度分析与解释信任，在人与人交往过程中，信任是降低复杂度的衡量方式。有学者认为信任是能够减小交往的复杂性，在面对复杂或决策性问题的环境中，我们会对特定的情况做出一些可信的选择。将信任定义为期望，对于信任的界定分为三个不同的层面：a)道德的社会秩序和自然秩序的运作的期望；b)针对自己所处的关系中，按照角色要求进而行

为的期望；c)针对其人能完全承担责任和风险的胆量，以他人利益为重的期望。

综上所述，对于信任还未有统一严格的定义标准。但大多学者认为，信任是主体对客体交互过程中的主观评价，是指主体与客体在一定的时间内进行一定的交互过程中，根据交互记录的结果逐渐形成的。其他主体节点利用该评价来引导与客体节点间的数据交互行为。

3.1.2 可信定义

目前对于可信的研究还没有统一的定义概念，目前研究学者对可信有以下几种定义：

(1) 可信计算组织 TCG：预先评估某已设备节点时，若该实体按照系统中对实体期望的方式实现系统预期的目标值，则该实体被认为是可信的。

(2) ISO/IEC 15408 标准：在一定的环境里，参与计算的组件、操作的过程中是可以预测的，并可以抵抗干扰继续完成工作。

(3) 其他学者的定义：计算机系统为某一应用或客户提供的一定的服务是可以被验证并被用户信赖，则该服务是具有可信赖性。

3.1.3 信任属性

在针对信任评估机制的研究过程中，根据信任独特的属性，学者根据各自的研究重点进行了深入研究，结合信任的特点，将信任的属性总结如下：

(1) 主观性 (Subjectivity)：信任值是主体在进行直接交互过程中对客体主观评价的一种主观结果，不同的主体节点对客体节点的信任评价标准也会不同，即在同一环境同一时间点的行为相同，每个主体节点的信任量化判断也不同。

(2) 动态性 (Dynamic)：信任值随时间和环境的变化而动态变化的，信任的动态性主要是由信任主体与客体的自然属性决定的。信任值的动态变化既可以是由客体的主观因素，例如主体的心理、知识、能力等原因引起的，也可以是根据客体的外因引起的，例如客体的行为、固有因素、协议等等。但变化的主要原因是由于客体的外因影响的，主体可以直接客观的观察出客体的外因，虽然模糊不确定，但依旧可以进行信任的量化和预测。

(3) 数量性 (Arity)：主体与客体之间的信任关系存在四种关系模式，分别为着一对一，一对多，多对多，多对一。

(4) 传递性 (Transitivity)：在环境中，节点间的信任关系虽然并不具备完全的传递性，例如若 A 实体对 B 实体较信任，B 实体对 C 实体也较为信任，但并不能完全得出 A 实体信任 C 实体，但是在一定条件约束下，节点间的信任关系又具有一定的传递性，在信任评估模型中节点的推荐信任就是信任传递性的一种表现。

(5) 相对性 (Relativity): 主体在一定的领域内对客体进行信任评价得出的结果, 代表着该信任与内容之间存在着关系。若 A 主体对 B 主体在计算方面具有一定的信任, 但是对于 B 主体的存储方面并不信任, 因此, 信任关系是相对的。

(6) 衰减性 (Attenuation): 信任是随着时间的递进而慢慢减弱, 信任值被计算出的越久, 越不具说服力。

(7) 可度量性 (Measurability): 数学可以对信任值及进行度量并对其进行区分等级, 信任等级可以根据系统环境的需求进行数字量化, 量化区间可以是连续的也可以是离散的。任何一个信任的关系都对应着一个信任等级。在信任评估模型中若利用数学三元组进行度量信任值, a 为信任, b 为不信任, c 为不确定, 并且 a, b, c 为连续的, $0 < a < 1, 0 < b < 1, 0 < c < 1$, 并且 $a+b+c=1$ 。

(8) 非对称性 (Asymmetry): 信任是不具有对称性的, 是节点单方面计算得出。例如, A 节点对 B 节点具有一定的信任度, 但并不能保证 B 节点对 A 节点的信任度量是一致的。

3.1.4 信任获取

对某一实体执行某一特定行为产生的主观可能性的程度被称为信任, 对于实体间的信任关心, 一般分为直接信任和间接 (推荐) 信任两种。在环境中, 实体的信任评价实则是实体对评价实体交互结果的客观期望。若实体之间不存在或长时间无直接交互的经验和记录, 则可以根据第三方实体关系综合得出第三方实体对评估实体的信任评价价值并进行决策。

在边缘计算环境中, 设备之间信任的获取渠道主要分为间接获取和直接获取两种。若环境中 A 设备实体和 B 设备实体有直接交互经验, 则 A 设备实体对 B 设备实体的可信度可以从两者间的直接交互经验来评估确定, 通过设备实体之间的直接交互经验得到出的主观结果为直接信任值。另外, 设 A 设备实体和 B 设备实体无直接交互经验, 则 A 设备实体可通过与 B 设备实体比较熟悉的 C 设备实体集来获得对 B 设备实体的信任值, 通过该方式综合计算而获取信任值称为间接信任值, 或者说是 C 设备实体向 A 设备实体的推荐信任值。

3.2 信任机制定义与分类

信任机制模型: 在所有的交互环境中, 参与交互的设备节点的能量或资源会受到限制, 而对于入侵检测、密码加解密技术等能量消耗较大的技术不适用于资源受限的终端设备组成的环境中, 信任机制是利用系统中设备节点之间的交互记录评估被评估设备节点的信任度, 为用户的应用程序提供一种低能耗, 高可靠的

方法，也可以不断更新系统中节点的信任度，将系统环境总的恶意或不可靠、不稳定的节点摒弃，并进行筛选出较为可信的节点进行数据交互。

信任模型是一种对系统环境中设备节点之间评价信任程度的防御机制，目前信任模型是通过信任管理机制和信任框架进行划分，信任机制中是需要利用直接进行交互的节点和其他推荐节点的综合评价来评估客体节点的信任度，将评估的客体信任度进行与系统中的最初设置的信任阈值进行比较来评估客体节点的信任。随着 5G 网络的普及，以及分布式系统在实际应用中会越来越广泛，目前万物互联时代中的计算模式往往以分布式方向发展，而集中式系统中对于设备节点的信任评估机制使用条件也愈发的苛刻。信任机制的分类划分如表 3-1。

表 3-1 信任机制分类

Table 3-1 Classification of trust mechanisms

分类方式		模型具体内容
信任评估机制	基于策略	采用授权凭证的方式进行建立系统中设备节点间的信任关系，并通过对应的信任策略来判断是否信任对方
	基于信任度	利用节点间的交互记录的信任评价来评估节点的信任度
信任评估框架	分布式	在计算环境中，所有参与节点都通过直接信任和间接信任进行计算得到综合信任度
	集中式	该方式是通过第三方对系统中的信任进行管理，设备节点间的信任度是可通过第三方提供。

3.3 动态信任机制基本内容与框架

动态信任机制：在计算环境中的信任关系中，将影响设备节点间信任关系的多种因素（如节点的计算能力、储存能力、可靠性等）考虑入过程中，实时的根据节点的主观与客观的因素的变化而动态更新量化，并将信任度进行量化，适当的调整环境中信任评估、管理和安全决策。

在动态信任机制中，若按照信任的属性进行划分，则可以将信任分成行为信任和身份信任两种；按照信任获取的形式划分，信任又可以被归纳为直接信任和间接信任。

（1）身份信任是根据某种验证协议、加密技术、数字签名等技术，判定环境中节点身份是否值得信任，身份信任只有两种结果产生，既信任和不信任；

（2）行为信任又被称为客观信任，它对特定信赖的问题，特定行为的信任，

图 3-2 展示了一个集中式网络中典型的信任评估框架，其中 A 与 B 节点表示交互的参与方，且假设 A 与 B 节点与网络中的其他节点都有数据交互的历史经验，双方正在考虑是否与之交互。节点在每次交互之后，节点都会向信任中心节点提供最新的节点评价值。信任中心节点动态对节点进行更新，以供需求节点获取最新的信誉值。

(2) 分布式网络信任评估

在某些交互环境中，一个没有中心节点的分布式网络中信任评估系统比集中式网络中的信任评估系统更适合更容易部署。分布式网络与集中式网络不同，在分布式网络环境中，没有负责接收和计算的中心节点管理各个节点的信誉值，取而代之的是几个节点共同负责管理，最简单的方式是环境中的各个节点都存储着与其他节点交互的直接数据值，并向其他需求节点反馈。图 3-3 为分布式网络信任评估框架。

在分布式网络环境中，若 A 节点想与 B 节点进行交互，便会向 D 与 F 或其他与 B 节点有过直接交互的节点发送请求获取与 B 节点的行为信誉值，综合计算后再决定是否与 B 节点进行交互。若节点 A 与 B 有直接交互记录，那么 A 节点对 B 节点的评价值作为私有信息，在计算 B 的综合信誉值时，私有信息会在计算过程中享有更高的权重。但由于分布式网络环境中的特定性，通常主体评价节点从其他节点获取到客体被评价节点的评价值，代价过于高，因此在分布式信任评估系统中，信誉值计算的评价子集可以从邻居节点处获取。

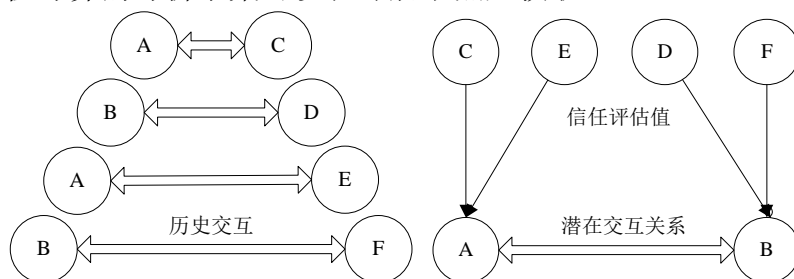


图 3-3 分布式网络信任评估框架

Fig.3-3 Distributed network trust assessment framework

3.4 信任机制存在的问题

对于信任的研究是信息安全领域中一直重要的一项课题，但对于信任机制的可信发展的存在的问题仍旧存在：

1. 理论滞后于技术

在可信计算的领域中，无论是国内外的研究都是理论研究滞后于技术。可信计算的基础是针对某些模型和机制的可信测量，目前在可信计算的系统中缺乏可信的信任评估方法和完善的理论支撑。虽然信任链技术作为信任评估系统中一项重要的技术，但对于信任链的理论目前还不够完善，对于可信计算中的信任传递的理论也是研究的一个重要方向。因此，可信计算领域中理论应在实践中被丰富和发展。

2. 关键技术需持续发展

目前的信任评估模型，对于系统中设备节点的描述能力不足，且量化设备之间的信任关系的标准和形式等问题还未进行统一，同时也缺乏设备节点间信任关系的动态性，从而降低了信任模型评估的准确性和实时性。在实际的应用中，信任评估模型在不同的应用场景中存在着限制和不足，例如，大规模网络中不适用、难以与应用集成、对恶意反馈处理的能力不足等。

3. 可信软件系统缺乏

对于目前存在的操作系统、应用软件、数据库的可信技术还不规范，而在联网环境中实现设备节点间的数据共享和数据交换的交互，技术不规范则会影响系统的安全性和可信性。

4. 可信决策的支持有待加强

目前信任模型缺乏对风险、时效、信任访问控制策略等诸多因素的综合考虑，使得系统得出的信任不准确，影响系统的准确性。同时也很难满足环境和应用的需求，而针对性的研究目前探索处于不成熟期，许多问题有待解决。

由于信任模型中对于信任评估的重要性和面临问题本身的复杂性，针对目前信任评估模型的问题和不足，本文提出了一种改进的动态信任评估模型，不仅适用于分布式的边缘计算环境，而且提高信任模型的可信性。

3.5 本章小结

本章针对系统中设备节点信任评估相关内容进行介绍，首先根据信任的相关内容介绍，如信任定义，信任属性，信任获取等内容，然后介绍信任评估机制的定义以及其分类，再对针对信任评估机制分布式和集中式框架进行详细介绍，最后针对信任机制目前的相关研究总结出信任机制存在的问题。本章内容为构建基于边缘计算的信任评估框架模型奠定了理论基础。

第4章 边缘设备动态信任评估机制

本章基于边缘计算中的身份信任和行为信任两个方面的研究进行阐述，面向边缘计算环境中的终端设备构建了信任评估机制模型。其中边缘计算层中心节点作为可信固定的设施，而终端设备随着用户的行为呈现动态变化的可能性，所以本章主要先对设备进行身份认证再对边缘终端设备进行行为信任度评估，最终获得设备的综合信任值。

4.1 边缘设备身份信任认证

文中身份信任认证是验证边缘设备在环境中身份是否得到认证，而身份认证也是设备接入环境进行信息交互的一个评判标准。随着边缘计算的发展传统的基于云计算“云一端”的身份认证框架也逐渐向基于边缘计算的身份验证架构。在边缘计算环境下的设备交互下，传统的身份验证架构存在一定的局限性^[46]。由于边缘设备可能存在资源受限的特点，而传统的 PKI 体制过度消耗设备的资源，进而无法适用于边缘计算环境中设备的身份认证。由于边缘计算环境中设备移动性较强，如何实现不同边缘设备切换时的高效认证具有很大挑战^[47]。显然，低耗高效的身份认证技术是保证边缘计算安全的前提。因此，设计适用于边缘计算环境的身份认证方案是必要的。

在本文的身份认证过程中，使用国家密码局发布的密码算法——SM9 标识密码算法^[48]，该算法摒弃了 PKI 复杂的验证证书撤销和管理的相关操作，利用双线性对实现并具有安全高效性，它更适用于存在海量且资源受限的边缘计算环境。

SM9 的签名及验签流程算法如下，如图 4-1 所示：

- 第 1 步：计算群 G_T 中元素 $g = e(P_1, P_{pub-s})$ ；
- 第 2 步：产生随机数 $r \in [1, N-1]$ ；
- 第 3 步：计算 G_T 中元素 w ；
- 第 4 步：计算 $h = H_2(M \parallel w, N)$ ；
- 第 5 步：计算 $l = (r - h) \bmod N$ ，若 $l = 0$ 则转至第 2 步；
- 第 6 步：计算 G_T 中元素 $S = [l]d_{s_A}$ ；
- 第 7 步：根据标准规定，得到 M 的数字签名 (h, S) 。

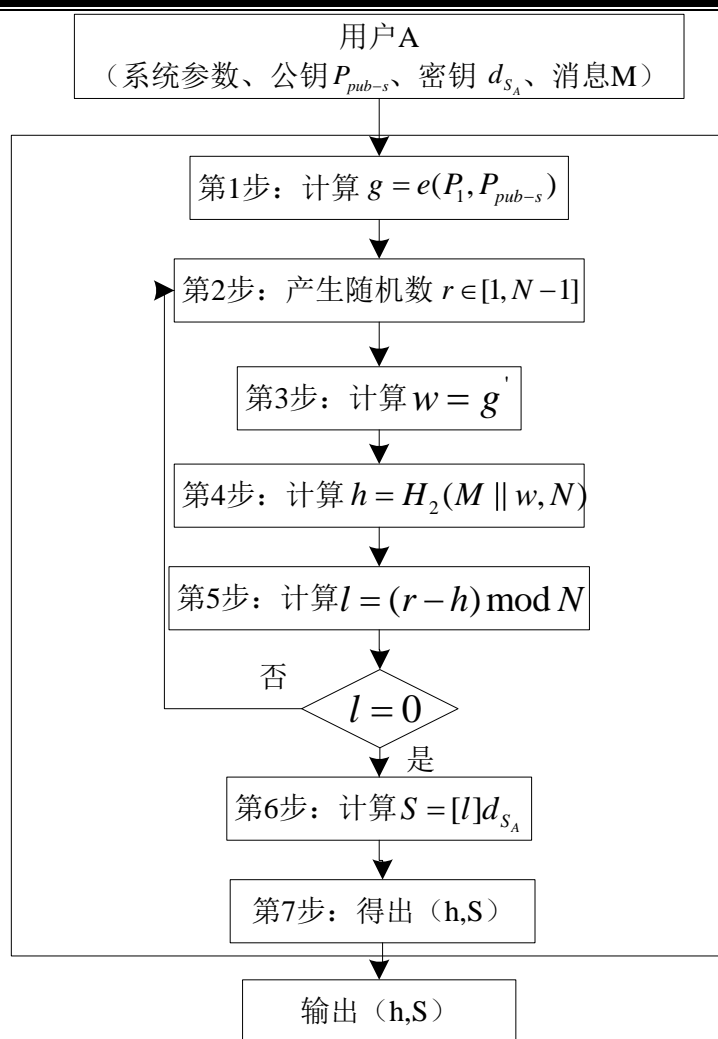


图 4-1 SM9 签名算法流程

Fig.4-1 SM9 signature algorithm flow

国密 SM9 的验签流程图及算法，如图 4-2 所示

第 1 步：验证签名是否成立，不成立直接结束；

第 2 步：计算群 G_T 中元素 $g = e(P_1, P_{pub-s})$ ；

第 3 步：计算群 G_T 中元素 $t = g^h$ ；

第 4 步：计算 $h_1 = H_1(ID_A || hid, N)$ ；

第 5 步：计算群 G_2 中元素 $P = [h_1]P_2 + P_{pub-s}$ ；

第 6 步：计算群 G_T 中元素 $u = e(S', P)$ ；

第 7 步：计算群 G_T 中元素 $w' = u \bullet t$ ，并根据规则置换成比特串类型；

第 8 步：计算 $h_2 = H_2(M' || w', N)$ ，若 $h_2 = h'$ 则验证成功，反之失败。

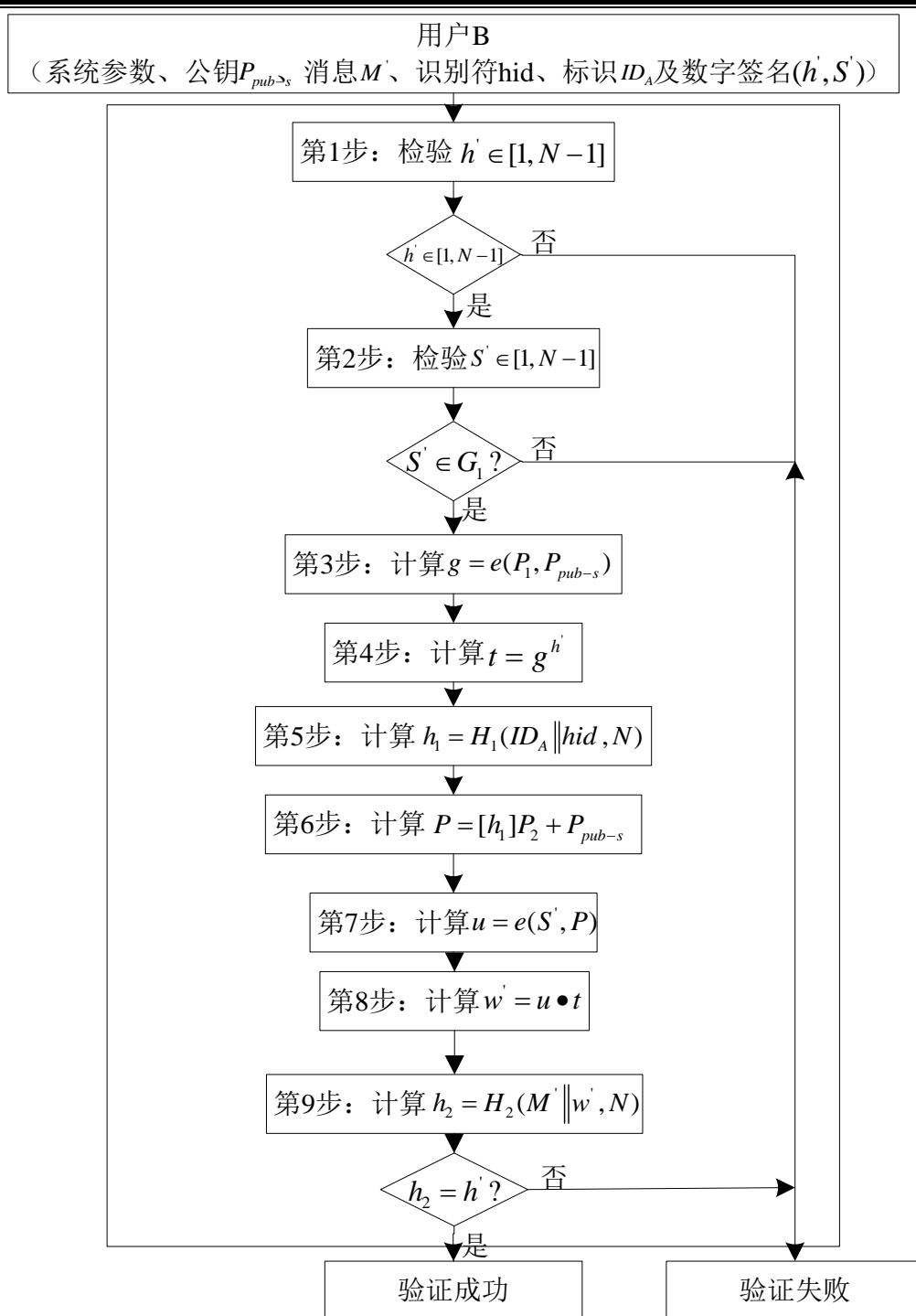


图 4-2 SM9 验签算法流程

Fig.4-2 SM9 signature verification algorithm flow

4.1.1 身份认证架构

在边缘计算环境中，边缘计算层设备加入环境时需要在云端进行身份认证，终端设备只需要向边缘计算层的设备进行认证身份，无需再向云端发送认证请求，

进而实现适用于边缘计算环境的身份认证架构。

如图边缘计算的环境中，存在着三个实体：云中心、边缘层节点、边缘终端设备节点，在云中心系统中，云中心节点对于建立可靠的身份认证技术有较高的身份可信度；在边缘计算的环境中边缘服务器是一类较低的固定基础设施，移动性较低也具有较高的身份可信度；由于边缘计算环境中的终端设备动态性和移动性也较强，进而终端设备的身份认证可信度比较难确定，而且终端设备存有客户的隐私数据，为保护用户的隐私针对终端设备交互的身份认证机制是必须的。所以在该身份认证框架中主要是针对边缘终端设备进行验证。

边缘计算是不同于云计算集中式特性的新型分布式计算模式，边缘终端设备交互分为两种不同的方式，边缘终端设备可能属于同边缘层节点的管控下（即属于同一 PKG 的边缘计算节点）；另外，若终端设备不同的边缘层节点的厂家不同，其 PKG 主密钥不同进而无法实现终端设备的相互身份认证，为终端设备的交互的连续性和稳定性，同时也需要进行跨域的终端设备身份认证机制。图 4-3 和图 4-4 为终端单域和跨域认证图。

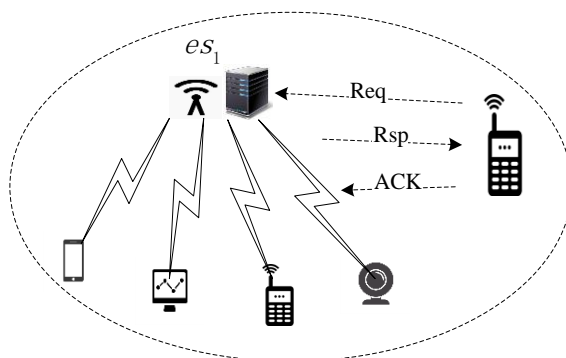


图 4-3 单域终端接入认证

Fig.4-3 Single domain terminal access authentication

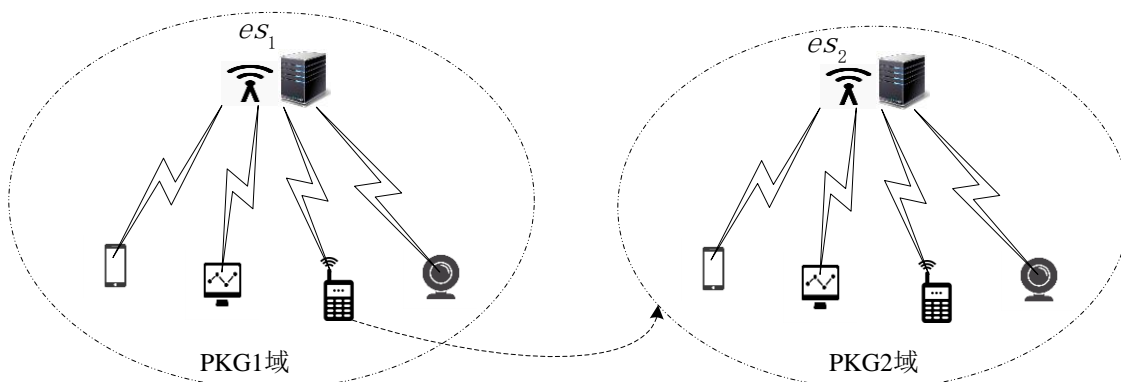


图 4-4 终端跨域认证

Fig.4-4 Terminal cross domain authentication

4.1.2 身份认证模型设计

1. 单域边缘设备终端的身份认证

在边缘计算环境中，无论是需要边缘计算层节点提供服务时，需要向边缘计算层认证自己的身份认证，边缘计算层节点同时会记录该设备的身份认证信息。对于终端设备节点的身份认证过程主要步骤如下：

Step1: 当设备 ed_i 加入网络中时，需要在边缘计算层进行身份认证，则需要向该边缘计算层节点 es_1 发送认证请求，从 PKG 获得对应的密钥，应用于会话的密钥通信。设备发送的请求中包含该设备和边缘层节点的身份标识，利用 $SM9$ 签名算法，运用设备的私钥进行签名计算对应的数字签名 (h, s) 。

$$ed_i \rightarrow es_1 : AccessReq \| N_1 \| ed_i \| es_1 \| h \| S \quad (4-1)$$

其中 $AccessReq$ 为设备接入时的认证请求， N_1 为随机数。

Step2: 边缘计算层在接收到终端设备的身份认证请求后，利用 $SM9$ 签名算法对其进行签名验证，经过验证后边缘计算层节点会将该终端设备的身份标识信息保存到认证列表中，且将加密的认证信息反馈给终端设备节点，首先根据式 (4-2) 计算群 G_1 中的 Q_D 元素的值，根据产生的随机数 r 计算群中的 $Cipher$ 值， $Cipher$ 为密文，其中 $r \in [1, N-1]$ ，再根据式 (4-3) 利用 KDF 计算被封装的密钥 Key ，其 Ky 值为边缘层和终端设备的共享密钥。

$$Q_D = [H_1(ed_i \| hid, N)] P_1 + P_{pub-e} \quad (4-2)$$

$$Key = KDF(Cipher \| (P_{pub-e}, P_2)^r \| D, klen) \quad (4-3)$$

$$es_1 \rightarrow ed_i : AccessRsp \| es_1 \| Cipher \| h \| S \quad (4-4)$$

其中 $klen$ 为密钥长度， $AccessRsp$ 请求响应标识。

Step3: 边缘终端设备在接收到边缘层节点的响应包之后，对接受到的 $Cipher$ 进行解析，从而获取相应的密钥 Key ，首先需要判断 $Cipher$ 是否属于 G_1 中的元素，不属于则输入 0，否则根据式 (4-5) 计算 G_T 中 w' ，再利用 $SM9$ 将数据转换为比特流从而计算出响应的密钥 Key 。

$$w' = e(Cipher, d_{ed1}) \quad (4-5)$$

$$Key = KDF(Cipher \| w' \| ed_i, klen) \quad (4-6)$$

$$ed_i \rightarrow es_1 : AccessAck \| key(ed_i \| es_1) \quad (4-7)$$

其中 $AccessAck$ 确认响应， d_{ed1} 为终端私钥。

综上所述，若得出的密钥为 0，则身份认证失败，反之设备身份认证成功，并且将设备的身份标识保存至边缘计算层节点中。

2. 跨域边缘设备终端的身份认证

边缘计算环境是典型的分布式计算模式，当处于两个不同的边缘层节点管控时，其 PKG 可能不同，因此身份认证的认证密钥也不会相同，为实现终端设备的跨域认证，具体实现过程如下：

Step1: 跨域认证的前提是终端设备在所属域中已经完成了身份认证，当设备移动至另一个领域 es_2 时，则边缘计算节点则发送跨域认证的请求，并根据式(4-8)对身份标识进行加密，计算出 (3-31) 发送给新的领域边缘计算节点：

$$C = E_{key_old}(ed_i \parallel es_1 \parallel es_2) \quad (4-8)$$

$$ed_i \rightarrow es_2 : Reauth \parallel ed_i \parallel es_1 \parallel es_2 \parallel C \parallel N_1 \quad (4-9)$$

其中， $Reauth$ 代表跨域请求， N_1 为随机数。

Step2: 若新的边缘计算节点接收到设备的跨域认证请求时，首先根据传过来的身份标识，验证是否与原领域有信任关系，若存在信任关系则直接执行 Step3，否则，新的领域向原边缘计算层节点发送请求获取认证信息， es_1 接受到请求后，首先利用数字证书对 es_2 进行身份认证，获取 es_2 的公钥 PK_{es_2} ，在 es_2 接收到反馈信息时，也会对 es_1 进行验证，从而获取 es_1 的公钥 PK_{es_1} 。

Step3: 跨域的终端设备的认证信息是由 es_2 和 es_1 共同得出，首先根据 es_2 产生的 r_{es_2} ，计算出 $G * r_{es_2}$ ，将信息发送给 es_1 。

$$es_2 \rightarrow es_1 : KeyAgree \parallel (ed_i \parallel es_2 \parallel G * r_{es_2} \parallel C \parallel N_2)_{PK_{es_1}} \quad (4-10)$$

其中 $KeyAgree$ 代表协商的请求， N_1 为随机数。

Step4: es_1 在接收到请求后，会进行验证设备的身份和接收到的跨域信息，根据 r_{es_1} ， $G * r_{es_2}$ 和 $rg2$ ，计算得出 $G * r_{es_1} * r_{es_2}$ ，得出最终的终端的身份认证信息，并将信息反馈给 IDg2，如式 (4-11) 所示：

$$es_1 \rightarrow es_2 : KeyAck \parallel (ed_i \parallel es_1 \parallel G * r_{es_1} \parallel E_{key_old}(key) \parallel N_3)_{PK_{es_2}} \quad (4-11)$$

综上，则完成了不同边缘计算层节点管控的域间终端设备的身份认证，在该过程中无需进行复杂的计算和通信，简单运用数字认证，密钥协商完成终端设备与边缘计算层的身份认证，有效的降低了验证过程的计算和开销。

4.2 边缘设备行为信任评估

4.2.1 基于改进的贝叶斯方法的直接信任评估

1. 问题分析

目前对于直接信任的研究大多使用基于贝叶斯信任的评估方法，在该信任评

估方法中，主要是通过评估设备节点 ed_i 与被评估设备节点 ed_j 间交互的历史数据进行计算，用 r 和 s 来记录两设备之间的交互成功和失败的次数，由于 beta 分布函数更好的拟合信誉分布，则 ed_i 对 ed_j 的直接信任的统计期望为：

$$C_{ed_i, ed_j} = E(\text{Beta}(r+1, s+1)) = \frac{r+1}{r+s+2} \quad (4-12)$$

虽然上式能够通过历史交互数据预测未来设备节点的信任值，但是信任具有动态性，信随时间的变化而变化，上式并未体现时间衰减性致使很难保证设备节点的信任评估的时效性。其次，上式忽视了被评估设备节点在交互的过程中因为异常导致的交互失败，使得对直接信任评估的结果不能准确刻画出被评估设备节点行为。

2. 直接信任度计算

(1) 满意度计算

满意度函数记录的是评估设备与被评估设备交易的满意度。在边缘计算环境中，由于边缘设备节点在交互过程中会根据当时影响因素的变化而影响交互结果（其中影响因素为：计算能力、数据存储能力、能量供应能力等方面的限制性），且有的评估设备节点关注交易速度，而有的更关注与交互数据的完整性，所以评估边缘设备节点只从历史交互记录计算直接信任度，可能会造成较大的误检率，为解决这一问题，文中引入了满意度 $q_{(t)}$ 的概念对 beta 密度分布函数进行修正，公式定义如式（4-13）：

$$q_{(t)} = \sum_{k=1} e_k * w_k \quad (4-13)$$

其中， $e_k \in [0,1]$ 为评估设备节点对交互参与的影响因素 k 评价， w_k 为评价权值， $w_k \in [0,1]$ ，对式（4-13）加入满意度修正因子的直接信任评估方法：

$$C_{ed_i, ed_j}(t) = \frac{r_{(t)} + 1}{r_{(t)} + (1 - q_{(t)}) \cdot s_{(t)} + 2} \quad (4-14)$$

(2) 时间退化因子

节点间的信任度是动态变化着的，信任作为节点之间在合作上的一个重要标准，根据信任度的预测进行节点选择合作，同时两节点之间的信任值是选取较近时间节点更新的信任值作为评价指标，所以需要时间退化因子来反映信任值随时间动态变化的特性。其定义如式（4-15）：

$$k_z = \frac{1}{t - t_z + 1}, \quad k \in (0,1) \quad (4-15)$$

其中, t 为当前时间。时间退化因子是根据节点间的交互产生的时间来计算该时间节点的俩设备节点间的直接信任度, 在时间相近的交互记录中就会产生相同的因子值。同时, 为便于使用 β 密度函数, 本文引入 p 变量, 若两节点的交互成功则 $p=1$, 否则 $p=0$ 。引入时间退化因子, 原 β 密度函数中的变量随之变化, 其最新的构造方法为:

$$\begin{cases} r_{(t)}^{new} = \sum_{z=1}^n k_z p_z \\ s_{(t)}^{new} = \sum_{z=1}^n k_z (1 - p_z) \end{cases} \quad (4-16)$$

(3) 激励机制

根据历史交互情况引入激励机制计算直接信任值, 阈值为交互失败次数和成功次数的平均值, 若失败次数大于平均值则引入惩罚因子, 反之引入奖励因子, 如下式:

$$EP = \begin{cases} \left(\frac{1}{1+e^{-\rho \cdot r_{(t)}}} - \frac{1}{2} \right) \cdot \frac{1}{1+e^{-r_{(t)}}} & , \rho > 0 \\ -\left(\frac{1}{1+e^{-\theta \cdot s_{(t)}}} - \frac{1}{2} \right) \cdot \frac{1}{1+e^{-s_{(t)}}} & , \theta > 0 \end{cases} \quad (4-17)$$

从 (4-17) 式中可以看出激励机制对于节点的惩罚和奖励程度是不一样的, 式中体现对于节点信任缓慢增加, 但惩罚节点的信任的减弱是很快的。在计算直接信任度过程中引入激励机制后, 所得到的节点间的直接信任由 (4-18) 式决定:

$$DT_{ed_i, ed_j}(t) = C_{ed_i, ed_j}(t) + EP \quad (4-18)$$

4.2.2 基于改进的灰关联分析的间接信任评估

目前多数信任模型对于间接信任度的计算, 都主要倾向于评估设备节点对其他推荐设备的信任度越高越可靠, 但有些恶意设备会通过自己良好的直接信任度实施恶意推荐的行为, 从而降低了被评估设备的推荐的信任度的准确性。同时, 传统的信任模型存在对于推荐设备提供的信任因素进行人工加权或主观加权的局限性, 不能准确反映信任决策过程的自适应性, 从而导致对被评估设备节点信任度的误判。

1. 间接信任度估计模型包含如下要素:

(1) 假设参与间接信任度评估的推荐设备节点为 k 个, 其中 k 个推荐设备节点与评估设备节点公共的设备节点有 n 个, 记作 $R: \{R_1, R_2, R_3, \dots, R_k\}$ 为推荐设备集, $C: \{C_1, C_2, C_3, \dots, C_n\}$ 为集合 R 与评估节点都有过交互历史的公共设备节点的集合。

(2) 推荐设备权重集合记作 $W: \{w_1, w_2, w_3, \dots, w_k\}$, 其中 $\sum_{i=1}^k w_i = 1$, $w_i > 0$ 。

(3) 计算矩阵 $f = [DT_{R_i, C_j}]_{k \times n}$, 其中 DT_{R_i, C_j} 是推荐设备 R_i 对公共设备 C_j 的直接信任值。

$$f = \begin{bmatrix} DT_{R_1, C_1}(t) & DT_{R_1, C_2}(t) & \cdots & DT_{R_1, C_n}(t) \\ DT_{R_2, C_1}(t) & DT_{R_2, C_2}(t) & \cdots & DT_{R_2, C_n}(t) \\ \cdots & \cdots & \cdots & \cdots \\ DT_{R_{k-1}, C_1}(t) & DT_{R_{k-1}, C_2}(t) & \cdots & DT_{R_{k-1}, C_n}(t) \\ DT_{R_k, C_1}(t) & DT_{R_k, C_2}(t) & \cdots & DT_{R_k, C_n}(t) \end{bmatrix}$$

2. 传统基于灰关联度求解指标权重的方法

灰色关联分析作为一种系统分析技术, 是用于分析某系统中多个因素关联程度的一种方法。将其用于计算多个因素评价指标的权重, 但实际是对于推荐设备对于公共设备的直接信任与某设备的最大直接信任值进行量化比较, 根据设备间的差异性的大小分析公共设备对于推荐设备的信任度的关联程度, 即为关联度。其关联度越大, 说明公共设备对于该设备信任趋于一致, 该推荐设备在间接信任评估计算中重要程度就越大, 其权重也就越高。据此对参与间接信任计算的所有推荐设备进行归一化处理, 确定其权重。

(1) 从矩阵 $f = [DT_{R_i, C_j}]_{k \times n}$ 中每一列中选取参考值 X 组成参考序列记作 X_0 。

组成新的决策矩阵, 第一行为参考序列, 其余由推荐设备和公共设备节点之间的直接信任组成的对比序列。

$$f \rightarrow \begin{bmatrix} x_0 & x_1 & \cdots & x_n \\ DT_{R_1, C_1}(t) & DT_{R_1, C_2}(t) & \cdots & DT_{R_1, C_n}(t) \\ DT_{R_2, C_1}(t) & DT_{R_2, C_2}(t) & \cdots & DT_{R_2, C_n}(t) \\ \cdots & \cdots & \cdots & \cdots \\ DT_{R_k, C_1}(t) & DT_{R_k, C_2}(t) & \cdots & DT_{R_k, C_n}(t) \end{bmatrix}$$

(2) 计算关联系数及关联度

根据灰关联分析理论, 对矩阵 f 利用式 (4-19) 求出推荐设备节点与参考序列在公共设备指标上的关联系数和关联度。

$$\xi_{0i} = \frac{\min_i \min_x |x_0(x) - x_i(x)| + \rho \max_i \max_x |x_0(x) - x_i(x)|}{|x_0(x) - x_i(x)| + \rho \max_i \max_x |x_0(x) - x_i(x)|} \quad (4-19)$$

$$r_{0i} = \frac{1}{n} \sum_{x=1}^n \xi_{0i}(x) \quad (4-20)$$

其中, ρ : 分辨系数, 通常取 0.5。关联度 r_{0i} 的大小反映了对应推荐设备在计算间接信任度的重要程度。

(3) 以作为推荐设备的权重值, 即 $w_i = r_{0i}$ 。

3. 基于改进灰关联求解权重的方法

基于传统的灰关联求解权重,容易受 ρ 取值的影响,使权重值具有不确定性,从而影响对间接信任值的评估。为此对传统灰关联求解权重方法进行,借鉴灰色关联度相近的思想,选取评估设备节点较为可信的值作为参考序列,经过公式(4-21)、(4-21)进行计算,再进行权值归一化处理,得出推荐设备节点在间接信任评估计算中的权重值。计算过程中不需要决策者主观设定参数,消除了决策者的主观干扰,使得计算出的间接信任值更加可靠。

(1) 确定参考序列

评估设备节点对 C 公共设备集中的直接信任是较为可信的,所以决策矩阵中的最优参考序列为 $DT_{ed_i,C}(t)$ 。

(2) 求推荐设备对比序列与参考序列之间的绝对距离

$$D_{0i} = \sum_{x=1}^n (x_0(x) - x_i(x))^2 \quad (4-21)$$

(3) 求推荐设备的权重值

$$w_i^* = \frac{1}{1 + D_{0i}} \quad (4-22)$$

(4) 求推荐设备的归一化权重

$$w_i = w_i^* / \sum_{i=1}^k w_i^* \quad (4-23)$$

4. 间接信任度计算

基于改进的灰关联计算推荐设备在间接信任评估中的所占权重,以评估设备较可信的直接信任为参考序列,推荐设备对指标设备的直接信任值作为对比序列,根据与参考序列的距离计算出推荐设备的权重,从而得出间接信任 $IT_{ed_i,ed_j}(t)$,具体操作如算法1所示:

算法1.间接信任度计算

输入: 评估设备与被评估设备;

输出: 间接信任 $IT_{ed_i,ed_j}(t)$;

- 1: $[R] \leftarrow \text{GetD}(R_1, R_2, \dots, R_k)$ // 获取推荐设备集
- 2: $[C] \leftarrow \text{GetD}(C_1, C_2, \dots, C_n)$ // 获取推荐设备的指标设备
- 3: $[X_0] \leftarrow \text{Get_Data}$ // 评估设备对 C 直接信任,构成参考序列
- 4: $[D] \leftarrow \text{Get_Data}$ // R 对 C 的直接信任矩阵,构成对比矩阵
- 5: $[\text{target_Data}] \leftarrow \text{Retrie}(D)$ // 对比序列
- 6: $[X] \leftarrow [\text{target_Data}]$
- 7: for ($x=1$ to k) do

```

8:   for (y=1 to n) do
9:        $D_{0x} = \sum_{y=1}^n (x_0(y) - x_x(y))^2$ 
10:   end for
11:    $w_x^* = 1/1 + D_{0x}$  //根据计算, 得到集合  $\{w_1^*, w_2^*, \dots, w_k^*\}$ ;
12: end for
13:  $w_x = w_x^* / \sum_{x=1}^k w_x^*$  ( $0 < w_x < 1$  且  $\sum_{x=1}^m w_x = 1$ ) //通计算各指标的权重;
14:  $IT_{ed_i, ed_j}(t) = \sum_{R_i \in D, x=1}^k DT_{R_x, ed_j}(t) * w_x$ 

```

4.2.3 行为信任度计算及更新

行为信任是融合评估节点 ed_i 对被评估节点 ed_j 的直接信任和间接信任, 根据两者权重计算, 权重值 $w_1 + w_2 = 1$, 该权重是根据直接信任度和间接信任的信息熵进行计算。

$$TR_{ed_i, ed_j}(t) = w_1 \cdot DT_{ed_i, ed_j}(t) + w_2 \cdot IT_{ed_i, ed_j}(t) \quad (4-24)$$

在边缘计算环境中, 计算出的行为信任值并不是一成不变的, 在设备节点异常的情况下, 两节点交互过程中的可能会出现快速或不可预料的情况产生, 使计算出的被评估的节点不具有可靠性, 所以需要结合前期交互的情况进行动态更新生成行为信任值。

$$BT_{ed_i, ed_j}(t) = \alpha_t \cdot T_{ed_i, ed_j}(t-1) + (1 - \alpha_t) \cdot TR_{ed_i, ed_j}(t) \quad (4-25)$$

其中, $T_{ed_i, ed_j}(t)$ 为当前时刻信任值, $T_{ed_i, ed_j}(t-1)$ 前一时刻的信任值, α_t 指信任动态更新因子, 计算如下:

$$\alpha_t = \begin{cases} \alpha_{t-1} & , s_{(t)} = s_{(t-1)} \\ \alpha_{t-1} \cdot [1 - \frac{s_{(t)}}{s_{(t)} + r_{(t)}}] & , s_{(t)} > s_{(t-1)} \end{cases} \quad (4-26)$$

由公式可知, α_t 是根据到达 t 时刻两设备节点的交互失败率动态变化的, 随失败次数增多而变小, 则 $t-1$ 时刻的信任贡献随之下降。行为信任度计算和动态更新过程如算法 2:

算法 2. 行为信任度计算

输入: $DT_{ed_i, ed_j}(t)$, $IT_{ed_i, ed_j}(t)$, $[S]$ 和 $[\alpha]$;

输出: 行为信任度 $BT_{ed_i, ed_j}(t)$;

1: 计算直接信任度 $DT_{ed_i, ed_j}(t)$

- 2: 根据算法一计算间接信任度 $IT_{ed_i,ed_j}(t)$
- 3: $w_1 \leftarrow 1 - \left(\frac{H(DT_{ed_i,ed_j})}{\log_2 DT_{ed_i,ed_j}} \right) \Bigg/ \left[1 - \frac{H(DT_{ed_i,ed_j})}{\log_2 DT_{ed_i,ed_j}} \right] + \left[1 - \frac{H(IT_{ed_i,ed_j})}{\log_2 IT_{ed_i,ed_j}} \right]$ // 直接信任度权重
 $w_2 \leftarrow 1 - \left(\frac{H(IT_{ed_i,ed_j})}{\log_2 IT_{ed_i,ed_j}} \right) \Bigg/ \left[1 - \frac{H(DT_{ed_i,ed_j})}{\log_2 DT_{ed_i,ed_j}} \right] + \left[1 - \frac{H(IT_{ed_i,ed_j})}{\log_2 IT_{ed_i,ed_j}} \right]$ // 间接信任度权重
- 4: 根据公式 (11) 计算行为信任值 $BR_{ed_i,ed_j}(t)$
- 5: if($s_{(t)} = s_{(t-1)}$)
- 6: $\alpha_t \leftarrow \alpha_{t-1}$
- 7: else
- 8: $\alpha_t \leftarrow \alpha_{t-1} \cdot \left[1 - \frac{s_{(t)}}{s_{(t)} + r_{(t)}} \right]$
- 9: 根据公式 (4-25) 动态更新行为信任值 $BT_{ed_i,ed_j}(t)$

根据直接信任度计算过程可知, 计算直接信任度的时间复杂度为 $O(n)$, 由算法 1 间接信任度计算, 该过程时间复杂度由算法的执行次数决定, 由于最大循环数达到 $n*k$ 次, 所以间接信任度计算过程复杂度为 $O(n*k)$, 行为信任度计算和动态更新是结合直接与间接信任度计算, 而 $O(n*k) > O(n)$ 所以综合信任度计算算法的时间复杂度由算法 1 最大循环次数决定为 $O(n*k)$ 。

4.3 边缘设备综合信任度

身份信任指的是被评估边缘设备节点 ed_j 在边缘计算环境中关于身份认证、授权等身份可靠性保障机制对自身所确定的身份的合法性, AT_{es_k,ed_j} 取值具有二值性:

$$AT_{es_k,ed_j} = \begin{cases} 0 & , \text{ 未经过认证} \\ 1 & , \text{ 经过认证} \end{cases} \quad (4-27)$$

综合信任度是根据边缘层对于终端设备的身份认证的结果和对终端设备进行的行为信任度的计算共同得出, 由于身份认证只有两种结果产生认证成功和失败, 将身份认证结果进行量化则具有二值性, 认证成功为 1 反之为 0。在计算设备的信任度中, 设备身份认证只是作为计算信任度的一个辅助因素, 设备身份认证未通过仍然可以进行设备交互, 其信任度必然比其他设备信任度低。

在计算终端设备的综合信任度时, 终端设备的身份信任度和行为信任度根据两者权重计算如式 (4-28), 权重值 $w_a + w_b = 1$, 在计算过程中权重值由 ed_i 决定, 若评估设备较注重身份标识则 $1 > w_a > w_b > 0$, 若注重设备行为则 $1 > w_b > w_a > 0$ 。

$$T_{ed_i,ed_j}(t) = w_a \cdot AT_{es_k,ed_j} + w_b \cdot BT_{ed_i,ed_j}(t) \quad (4-28)$$

4.4 本章小结

本章主要是构建边缘终端设备的动态信任评估机制模型。首先利用国密 SM9 验证机制对终端设备进行身份认证，其中包括单域和跨域的两种情况对设备进行认证，减小认证过程的时间开销；然后利用满意度函数和时间退化因子改进贝叶斯方程计算行为信任中的直接信任度，并对改进灰关联方法进行计算各设备的间接信任的权重，提高间接信任的准确度；最后结合身份认证结果和行为信任共同得出边缘设备的信任值。

第 5 章 试验与结果分析

本章介绍了试验环境并通过仿真试验,从不同方面验证提出的边缘设备动态信任度评估模型 (Dynamic trust evaluation model, DTEM) 的有效性和准确性。

5.1 试验环境

运行环境为 Ubuntu 12.04-64 位系统,计算机采用 3.10GHz Intel(R) Core(TM)i5-3230M CPU 和 8GB 内存。为了使试验更接近边缘计算环境,在 NetLogo-6.0.4-64 版模拟器中,参考 Random Waypoint 移动节点随机分布生成模型,在部署面积为 500*500 的范围内,生成 1000 个移动节点作为边缘网络中的边缘设备节点,并对边缘设备节点进行编号以及设定两种设备身份:边缘设备节点和边缘网络节点,边缘设备节点的通信半径为 20,边缘网络节点则位于检测区域的中心。并对设备设定两种类型:正常设备或恶意设备(两种设备的比例随试验要求而定),正常设备是在交互过程中提供真实服务,恶意设备是指在交互过程中存在着恶意反馈或不真实服务。设定边缘设备节点之间交互 10~50 次,并将设备间的交互记录通过接口模块传递到 Matlab 中进行计算,实现整个系统网络数据交互。仿真试验中各参数设置,如表 5-1 所示。

表 5-1 仿真参数

Table 5-1 Simulation parameters

参数	描述	值
n	边缘设备总数	1000
部署面积	部署范围 m^2	500*500
T	信任初始值	0.5
r	通信半径	20
ρ	奖励因子	0.2
θ	惩罚因子	0.7
α_0	动态更新因子初值	0.5


5.2 试验结果与分析

5.2.1 可靠性分析

Scyther^[49]是目前较为流行的一款自动化分析工具,对于验证协议的攻击输

出和安全模型等方面较其他工具有优势。该分析工具是在 Ubuntu 操作系统中利用 Python 语言进行开发，以人机交互的界面的形式将协议验证结果展示出来，更直观的对协议进行分析和完善。

如图 5-1 是利用 Scyther 工具对 SM9 认证协议进行验证的结果：在验证的过程中加入了随机数 N ，确保消息的时效性，在传输消息的过程中加入身份标识，有效防护重放攻击，也有效抵抗了假冒攻击的风险性；在基于 SM9 的标识密码算法中，恶意攻击者获取设备的合法信息，后才可以计算出密钥，所以该协议具有较高的安全性。


Scyther results : verify

Claim				Status		Comments
PKIAndSM9	Edge	PKIAndSM9,e1	Secret ne	Ok	Verified	No attacks.
		PKIAndSM9,e2	Alive	Ok	Verified	No attacks.
		PKIAndSM9,e3	Niagree	Ok	Verified	No attacks.
		PKIAndSM9,e4	Nisynch	Ok	Verified	No attacks.
		PKIAndSM9,e5	Weakagree	Ok	Verified	No attacks.
	Device	PKIAndSM9,d1	Secret nd	Ok	Verified	No attacks.
		PKIAndSM9,d2	Alive	Ok	Verified	No attacks.
		PKIAndSM9,d3	Niagree	Ok	Verified	No attacks.
		PKIAndSM9,d4	Nisynch	Ok	Verified	No attacks.
		PKIAndSM9,d5	Weakagree	Ok	Verified	No attacks.

Done.

图 5-1 身份认证协议分析结果

Fig. 5-1 Authentication protocol analysis results

对于分析终端设备的行为信任模型可靠的两个重要指标是检测率和误检率，根据该模型的信任评估方案检测出恶意设备节点个数占总恶意设备节点个数的比率为该模型的检测率；根据信任评估方案误检的设备节点个数（正常设备节点被误检为恶意设备节点，恶意设备节点被误检为正常设备节点）占被检测的总设备节点数量的比率为误检率。在该仿真试验中，为了得出较为准确的检测率和误检率，分别做了五组试验，分别在试验环境中部署了 5%，10%，15%，20%，25%，30% 的恶意设备节点，仿真试验为验证 DTEM 能有效检测恶意节点，加入了不含满意度函数 q 的方案模型以及文献[52]中的基于贝叶斯理论的信任评估（reputation-based framework for high integrity sensor network, RFSN）模型进行对比，图 5-2 和图 5-3 为在不同比例的恶意设备节点下三种方案模型的误检率和检测率。

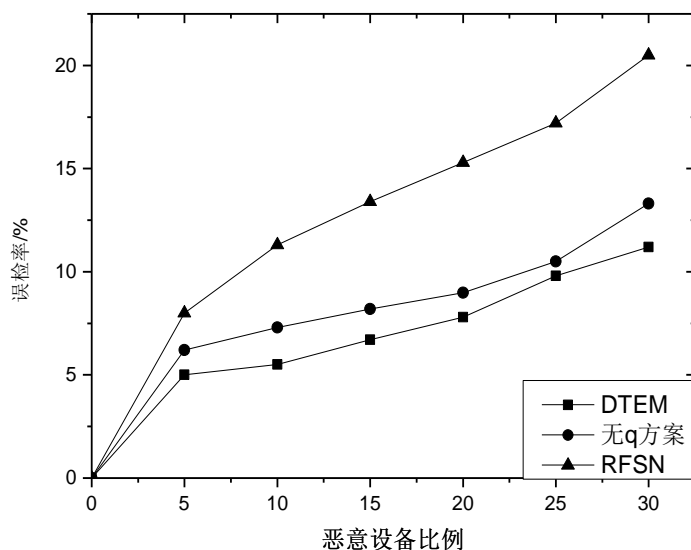


图 5-2 误检率对比

Fig. 5-2 Comparison of false detection rate

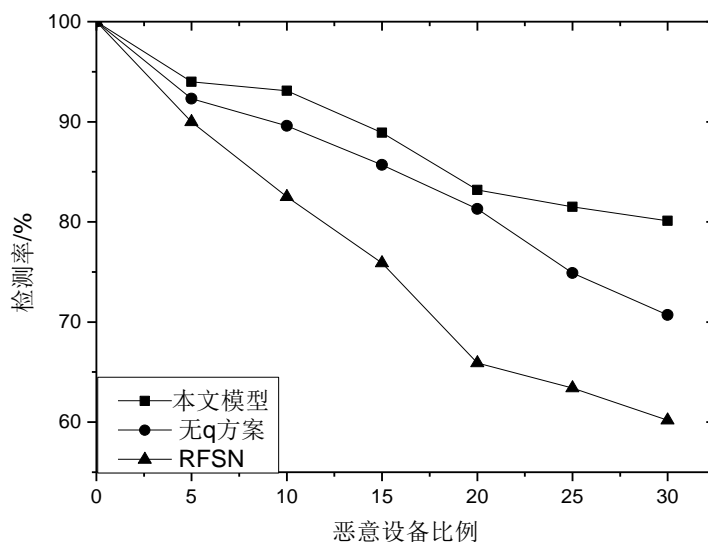


图 5-3 检测率对比

Fig.5-3 Comparison of detection rate

从图 5-2 可知，误检率随着恶意设备节点的比例增加而增加，但是在该试验中 DTEM、无满意度函数模型和 RFSN 三种模型平均误检率分别为 7.67%，9.08% 和 14.28%，对比下 DTEM 的误检率最低，主要是因为本文引入了满意度函数，由主体设备节点对被评估设备节点行为满意度评价，避免了非入侵因素导致两设备节点之间交互失败而错误判断的影响，因此减少了由交互记录判断设备节点的误检率，从图中看出性能明显优于其它两种模型。从图 5-3 可知，DTEM 的检测率明显高于其它两种方案，且在五组不同比率的恶意设备节点中检测率高于 80%，由于文献[51]的信任评估模型中只是传播节点良好的声誉，对于信任的评估并不

准确,同时也忽略了恶意节点因为恶意夸大反馈导致的信任值过高导致检测率降低; DTEM 由于加入满意度函数在一定程度上提高了恶意设备节点的检测率。

5.2.2 准确性分析

为了说明本文提出的改进的灰关联分析法对于求解推荐设备权重方法的准确性,本文通过与计算权重典型的熵方法和传统灰关联方法对比证明本文提出的方法准确度高。在本仿真试验中,选择 10 个推荐设备计算间接信任,记为 $R:\{R_1, R_2, R_3, \dots, R_{10}\}$, 假设 10 个推荐设备与评估设备之间存在 5 个公共边缘设备 $C:\{C_1, C_2, C_3, C_4, C_5\}$ 作为评判推荐设备权重的属性集,根据统计 C 集合中与评估设备主体与推荐设备的直接信任值,构成矩阵 f :(其中第一列为最优集,设置设备为 1, 5, 8, 10 的数据更贴近最优集)

$$f \rightarrow \begin{bmatrix} 0.490 & 0.845 & 0.646 & 0.709 & 0.455 \\ 0.590 & 0.748 & 0.441 & 0.575 & 0.891 \\ 0.319 & 0.055 & 0.865 & 0.845 & 0.982 \\ \dots & \dots & \dots & \dots & \dots \\ 0.190 & 0.879 & 0.498 & 0.661 & 0.863 \\ 0.495 & 0.989 & 0.901 & 0.730 & 0.484 \end{bmatrix}$$

利用矩阵 f 中的提供的数据,结合本文方法、传统灰关联方法以及典型熵法计算推荐设备的权重^[50],试验结果如 5-2 表所示。

RFSN 是基于贝叶斯理论的信任评估模型,该模型使用贝叶斯公式进行信誉表示、更新、集成和信任演化,提供了一种统一的方法来检测恶意行为的节点进而提升交互成功率,但是该模型具有不共享节点的交互体验,计算量大是以牺牲系统效率为代价的模型¹。

表 5-2 权重计算结果比较

Table 5-2 Comparison of weight calculation results

方法类型	推荐设备权重						
	w_1	w_2	w_3	\dots	w_8	w_9	w_{10}
本文方法	0.106	0.092	0.096	\dots	0.112	0.081	0.147
典型熵法	0.101	0.105	0.094	\dots	0.083	0.092	0.117
传统灰关联方法	0.519	0.687	0.771	\dots	0.745	0.689	0.871

在改进的灰关联方法中,加入了主体的主观评价作为最优集,越接近最优集的推荐设备,权值越高。由于权值归一性,参与的推荐设备较多时权值相差 0.01 区分度也是较大的,基于改进灰关联分析法的权值求解方法比典型熵权值求解方法和传统灰关联权值求解方法更合理,越接近最优设备集的设备权重值较大。采

用该方法,对比基于熵的评估模型、传统灰关联方法下得模型和 RFSN 模型的交互失败率,从图 5-4 可知,在恶意设备比例较低的情况下除 RFSN 模型的三种信任模型无明显差距,随着恶意设备比例的增加,基于改进的灰关联分析方法的模型交互失败率明显低于其他三种模型,主要是因为基于改进的灰关联分析方法的推荐设备的权重的准确性降低了设备之间的交互失败率。

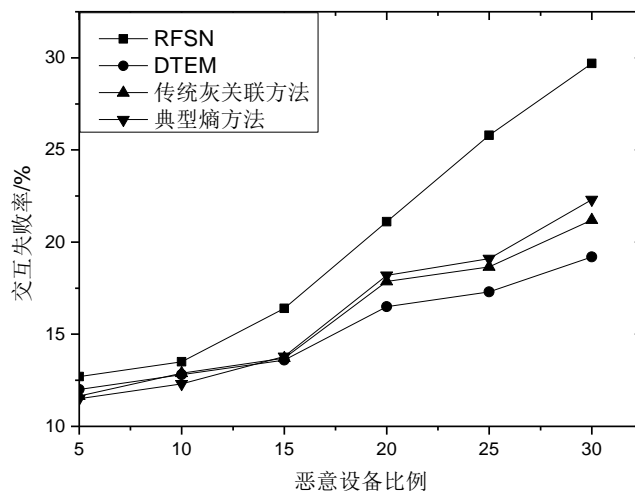


图 5-4 交互失败率

Fig.5-4 Interaction failure rate

5.2.3 系统开销分析

在对终端设备进行身份认证过程中,实时记录身份认证过程中的流量监控,对 100 个不同的终端设备进行两次身份认证并发测试,测试流量监控如图 5-5 所示,在前 30s 内完成对 100 个终端设备的第一次身份认证,在第一次身份认证过程中流量最高处于 800kb/s; 50s 后随机更新设备的信息进行第二次身份认证,测试过程中所使用的流量稍高于第一次但未超过 850kb/s,由此可知,设备的身份认证过程并未大量消耗系统流量,节省系统宽带开销。

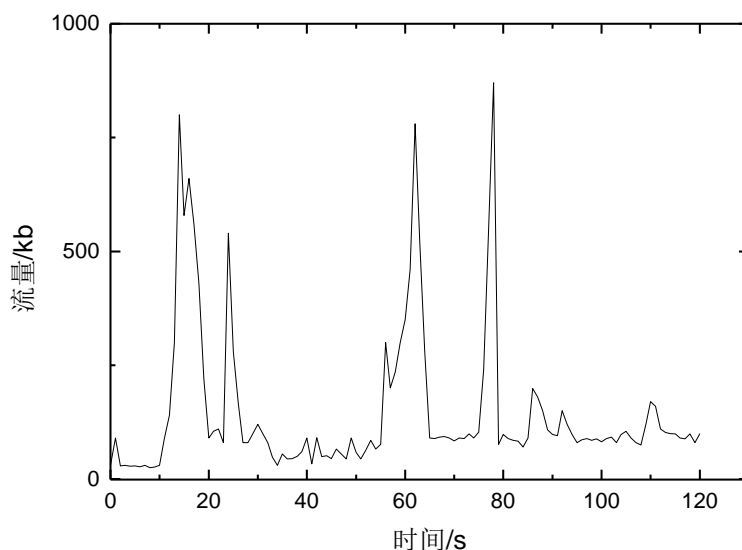


图 5-5 身份认证流量监控

Fig.5-5 Authentication traffic monitoring

本文提出的边缘设备动态信任度评估模型 DTEM，系统开销是在对设备节点进行信任评估过程中的重要评价指标。因此，通过对本文模型，RFSN 模型和基于雾计算的分层信任机制^[53] 基于雾计算的分层信任机制 FHTM 的三个不同方案的时间开销进行对比，而在信任评估的过程中，时间开销主要来自推荐信任评估的过程中。在试验过程中，为了使时间具有区分性，选择 6 组不同的推荐设备数量 {50, 100, 150, 200, 250, 300}，由于每次运行程序计算的系统运行时间具有偶然性，为准确记录时间开销，记录每组不同设备数量中的信任数据在不同的方法下都测试 10 次，并记录运行时间的平均值。

由图 5-6 可以看出，当参与设备数量少时，由于 DTEM 和 FHTM 模型的评估机制的系统消耗主要集中在 3 个方面：直接信任、推荐信任和信任更新，使本文提出的模型和 FHTM 模型的信任评估系统时间开销略高于 RFSN 模型，但随着参与设备的数量增多时，由于 RFSN 模型的信任评估是在整个网络不断迭代，致使数据查找次数增多融合数据量增大，导致基于该模型的时间开销增长迅速，而 DTEM 综合信任评估由网络层节点计算，减少了边缘设备的计算时间，提高了系统的效率，减少了信任聚合的全局收敛时间，使之时间开销增长缓慢。由于边缘计算中存在着大量的边缘设备，与被评估设备节点的交互的边缘设备数量也在不断增加，所以在设备数量较多的环境中 DTEM 时间开销优于其他两个模型。

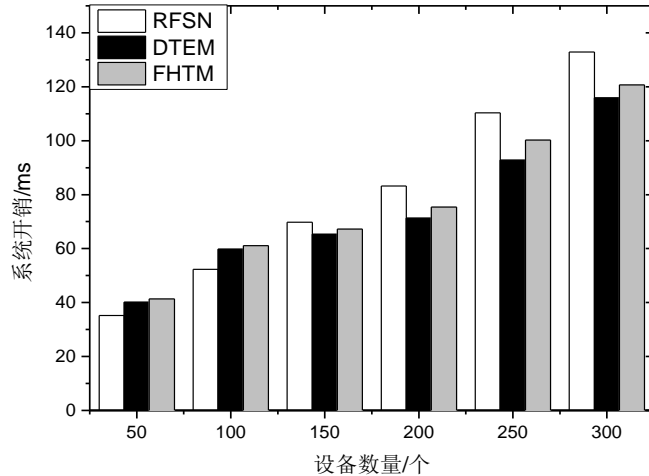


图 5-6 系统开销对比

Fig.5-6 Comparison of System cost

5.2.4 信任值分析

针对本文提出的边缘设备动态信任度评估模型 DTEM，从两个方面对被评估设备信任值进行仿真试验，由于本文信任模型在行为信任阶段加入了激励机制和动态更新因子，使在边缘设备交互时，信任值上升缓慢，若交互失败次数增加则会使得的被评估设备的信任值迅速下降。在该仿真试验中，同一设备在一定时间段内分别对 3 种不同的交互设备（记为设备 1，设备 2，设备 3），进行行为信任评估，

试验初始值为 0.18, 0.37, 0.8。设备 1 为信任度较好的设备, 并且在该时间段内交互记录都是成功的; 设备 2 为在该时间段内的某一时刻交互记录失败率较高; 设备 3 的初始状态信任较高, 但长期处于交互失败的状态。从图 5-7 中可以看出虽然设备 1 初始值较低, 但由于长期交互记录成功率较高, 信任值在该时间段内一直平稳上升。设备 3 由于在交互过程中交互结果失败率过高, 导致信任值下降迅速, 最终趋于 0。设备 2 初始信任值 0.37, 由于设备 2 在 0~160 时刻过程中交互记录良好, 信任值也平稳上升, 但在 160 时刻被检测出该设备有恶意行为, 致使该设备的信任值快速下降。从该试验中可以看出在加入激励机制的信任评估模型中, 信任值在不同行为的设备节点下上升与下降的速度的不同, 从控制节点的信任值进行抑制恶意节点不诚实反馈的行为。

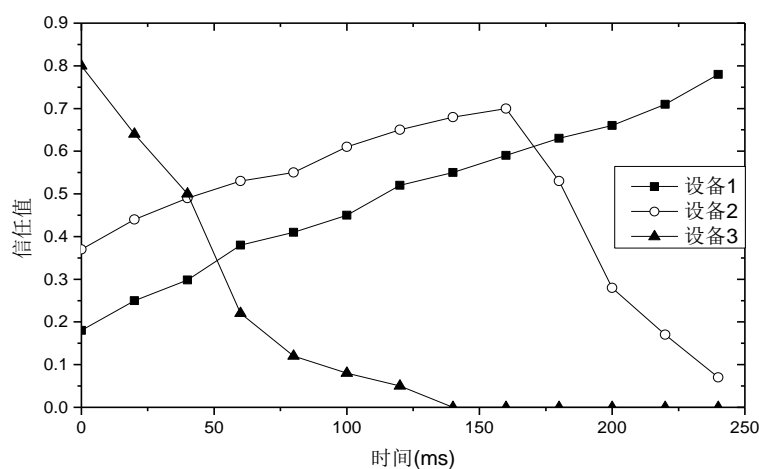


图 5-7 信任值变化

Fig.5-7 The changes of trust value

5.3 本章小结

本章通过仿真试验来验证提出的边缘设备动态信任度评估模型的有效性和准确性。使用 NetLogo 事件模拟器进行了大量的试验, 该模拟器提供了一个多代理可编程建模环境, 并通过模块接口与 Matlab 进行数据交互。在仿真试验过程中, 分别对信任模型以及协议的安全性、推荐设备的权重准确度、身份验证带宽和时间开销以及不同行为的信任值四个方面进行仿真试验, 从而验证本文提出的信任评估模型对于信任度评估的可靠性、准确性和高效性有一定的优势。

总结与展望

边缘计算在横向发展领域中以通用的计算能力为主，在纵向的发展领域主要集成垂直行业的应用，逐渐成为智能社会的关键，边缘计算作为新型的计算模式，有着无限的前景和广泛的应用。与此同时，边缘计算环境中安全问题也会随之而来，如何确定边缘计算环境的可信并选择可信的设备与之交互是边缘计算发展中研究的重要内容。

本文在对边缘计算和物联网环境深入了解的基础上，详细阐述并分析了目前边缘计算信任安全等方面的研究现状，分析并归纳学者的研究成果，为后续相关的研究工作奠定了理论基础。本文提出了一种边缘设备动态信任评估模型，针对边缘计算环境中的终端设备的身份认证的问题，引出了一种适用于边缘环境灵活高效的终端设备身份认证方案，再结合由基于改进贝叶斯得到的直接信任度和利用改进的灰关联方法得出的间接信任度融合计算出的行为信任度。最后在理论基础之上进行仿真试验，并从多方面验证本文模型在边缘计算环境中可行性和安全性。本文主要的研究内容如下：

(1) 针对在边缘计算环境中对于边缘设备身份认证过程中存在的问题，提出了一种基于 SM9 的标识算法对终端设备进行身份认证的方案，在此基础之上同时进行了单域和跨域两种不同方式的身份认证，并从安全上和系统开销上有效验证了该方法的适用性。

(2) 针对在众多的信任度评估模型中信任评估的准确性较低的问题，不能更好的检测出恶意设备节点，也不能合理的计算推荐设备的权重值。通过研究，本文主要引入了时间退化因子和满意度修正因子，使得信任评估过程随着时间和满意度的变化动态自适应地进行调整，有效增强了信任评估的合理性；同时，改进了灰关联分析法进行量化推荐设备之间权重值，有效地抑制设备之间不诚实的反馈的行为，提高交互成功率。

目前学者对边缘计算环境的研究集中在边缘计算应用方面，而对其环境的安全性缺乏深入探究，虽然本文主要提出了一种边缘设备动态信任度评估模型解决环境中交互可信，但在本文中并没有对信任值进行加密，对于保存的设备信任数据容易被篡改。下一步工作对模型中信任数据采取相应的安全存储措施，进一步设计边缘计算局部信任更新方法，利用边缘计算联盟的全局信任更新方法来共享信

任信息，从而实现更高效的边缘计算。边缘计算环境的安全的研究目前还处于初步节点，随着技术的发展以及应用范围的扩大，面临的数据安全的问题也会越来越严峻，边缘计算环境的安全与可信的研究也是一项长期的研究课题，为促进边缘计算的发展，需要研究学者为之共同努力提供更为安全的方案。

参考文献

- 1 施巍松, 孙辉, 曹杰, 张权, 刘伟. 边缘计算:万物互联时代新型计算模型[J]. 计算机研究与发展, 2017, 54(5): 907-924.
- 2 张佳乐, 赵彦超, 陈兵, 胡峰, 朱琨. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
- 3 赵梓铭, 刘芳, 蔡志平, 肖依. 边缘计算: 平台、应用与挑战[J]. 计算机研究与发展, 2018, 55(2): 327-337.
- 4 谢人超, 廉晓飞, 贾庆民, 黄韬, 刘韵洁. 移动边缘计算卸载技术综述[J]. 通信学报, 2018, 39(11): 138-155.
- 5 Evans D. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World[J]. Cisco IBSG, 2012:1-9.
- 6 马鑫玉. 基于边缘计算的可信协同机制的研究[D]. 北京邮电大学, 2019.
- 7 季鹏飞, 徐曾春, 胡平. 边缘计算下的多无人机野外协同作业机制研究[J]. 小型微型计算机系统, 2019, 40(5): 959-965.
- 8 Echeverria S, Klinedinst D, Williams K, et al. Establishing Trusted Identities in Disconnected Edge Environments[C]// 2016 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 27-28 Oct. 2016, Washington, DC, USA, 2016:51-63.
- 9 Cicirelli F, Guerrieri A, Spezzano G, et al. Edge Computing and Social Internet of Things for Large-scale Smart Environments Development[J]. IEEE Internet of Things Journal, 2017:1-15.
- 10 Satyanarayanan M, Simoens P, Xiao Y, et al. Edge Analytics in the Internet of Things[J]. IEEE Pervasive Computing, 2015, 14(2): 24-31.
- 11 Lopez P G, Montresor A, Epema D, et al. Edge-centric Computing: Vision and Challenges[J]. Computer Communication Review, 2015, 45(5): 37-42.
- 12 G. M. Shafiqur Rahman. Latency Minimization for Internet of Things (IoT) in Device to Device (D2D) Communication with Intervention of Fog Computing[D]. 北京邮电大学, 2016.
- 13 Abbas N, Zhang Y, Taherkordi A, et al. Mobile Edge Computing: A Survey[J]. IEEE Internet of Things Journal, 2018, 5(1): 450-465.
- 14 Mao Y, You C, Zhang J, et al. A Survey on Mobile Edge Computing: The Communication Perspective[J]. IEEE Communications Surveys & Tutorials, 2017, 19(4): 2322-2358.
- 15 Rodrigo Roman, Javier Lopez, Masahiro Mambo. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, 78(Pt.2): 680-698.
- 16 Data Encryption. Researchers from Shenzhen University Detail New Studies and Findings in the Area of Data Encryption (An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing)[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1265-1277.
- 17 Khan M A, Debnath H, Paiker N R, et al. Moitree: A Middleware for Cloud-Assisted Mobile Distributed Apps[C]// 2016 4th IEEE International Conference on Mobile Cloud Computing,

- Services, and Engineering (MobileCloud). IEEE, 29 March-1 April 2016, Oxford, UK, 2016: 21-30
- 18 Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, Min Ji. CCA-secure ABE with outsourced decryption for fog computing[J]. Future generation computer systems, 2018, 78(PT.2): 730-738.
- 19 Hong Liu, Huansheng Ning, Qingxu Xiong, et al. Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(1): 241-251.
- 20 Tsai J L, Lo N W. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. IEEE Systems Journal, 2015, 9(3): 805-815.
- 21 He D, Kumar N, Khan M K, et al. Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services[J]. IEEE Systems Journal, 2018, 12(2): 1621-1631.
- 22 Yang Y, Zhu H, Lu H, et al. Cloud Based Data Sharing with Fine-grained Proxy Re-encryption[J]. Pervasive and Mobile Computing, 2016, 28: 122-134.
- 23 Mahmood K, Chaudhry S A, Naqvi H, et al. An Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communication[J]. Future Generation Computer Systems, 2018, 81: 557-565.
- 24 Jin Y, Tian C, He H, et al. A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing[C]// 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. IEEE, 26-28 Aug. 2015, Dalian, China, 2015: 172-179.
- 25 Zhang P, Chen Z, Liu J K, et al. An Efficient Access Control Scheme with Outsourcing Capability and Attribute Update for Fog Computing[J]. Future Generation Computer Systems, 2018, 78(PT.2): 753-762.
- 26 Huang Q, Yang Y, Wang L. Secure Data Access Control with Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things[J]. IEEE Access, 2017, 5: 12941-12950.
- 27 Bahrami M, Singhal M. A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing[C]// 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. IEEE, 30 March-3 April 2015, San Francisco, CA, USA, 2015: 189-196.
- 28 Chen M, Li W, Li Z, et al. Preserving Location Privacy based on Distributed Cache Pushing[C]// 2014 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 6-9 April 2014, Istanbul, Turkey, 2014: 3456-3461.
- 29 Niu B, Li Q, Zhu X, et al. Enhancing Privacy Through Caching in Location-based Services[C]// 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 26 April-1 May 2015, Kowloon, Hong Kong, 2015: 1017-1025.
- 30 宁振宇, 张锋巍, 施巍松. 基于边缘计算的可信执行环境研究[J]. 计算机研究与发展, 2019, 56(7): 1441-1453.
- 31 Chen L, Xu J. Socially Trusted Collaborative Edge Computing in Ultra Dense Networks[C]// Proceedings of the Second ACM/IEEE Symposium on Edge Computing. ACM, October 2017, California, US, 2017: 1-11.
- 32 邓晓衡, 关培源, 万志文, 刘恩陆, 罗杰, 赵智慧, 刘亚军, 张洪刚. 基于综合信任的边缘

-
- 计算资源协同研究[J]. 计算机研究与发展, 2018, 55(3): 449-477.
- 33 Huang X, Yu R, Kang J, et al. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks[J]. IEEE Access, 2017, 5: 25408-25420.
 - 34 Yuan J, Li X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion[J]. IEEE Access, 2018, 6: 23626-23638.
 - 35 施巍松, 孙辉, 陈彦明. 基于边缘计算的新型视频监控系统展望[J]. 自动化博览, 2018, 35(12):72-75.
 - 36 Sun H, Liang X, Shi W. VU: Video Usefulness and Its Application in Large-Scale Video Surveillance Systems: An Early Experience[C]// In Proceedings of Workshop on Smart Internet of Things. ACM, October 2017, CA USA, 2017: 1-6.
 - 37 王昊天. 物联网智能家居发展分析[J]. 信息系统工程, 2016(6): 38-38.
 - 38 宋朋涛, 李超, 徐莉婷, 梁晓晓. 基于个人计算机的智能家居边缘计算系统[J]. 计算机工程, 2017, 43(11): 1-7.
 - 39 施巍松, 刘芳, 孙辉, 等. 边缘计算[M]. 北京:科学出版社, 2018.
 - 40 吴卫. 边缘计算环境下物联网身份认证与隐私保护技术研究[D]. 西安电子科技大学, 2019.
 - 41 田辉, 范绍帅, 吕昕晨, 赵鹏涛, 贺硕. 面向 5G 需求的移动边缘计算[J]. 北京邮电大学学报, 2017, 40(2): 1-10.
 - 42 LaMothe R. Edge computing[R]. Pacific Northwest National Laboratory, 2013.
 - 43 Sabella D, Roth K. Multi-Access Edge Computing (MEC) Service Provision Based On Local Cost Measurements[P]. US, 16/150,121, 2019-8-8.
 - 44 Weisong Shi, Jie Cao, Quan Zhang, et al. Edge Computing: Vision and Challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.
 - 45 Mach P, Becvar Z. Mobile Edge Computing: A Survey on Architecture and Computation Offloading[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1628-1656.
 - 46 Ni J, Zhang K, Lin X, et al. Securing Fog Computing for Internet of Things Applications: Challenges and Solutions[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 601-628.
 - 47 HE D B, ZEADALLY S, WU L B, et al. Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity-Based Public Key Cryptography[J]. Computer Networks, 2017, 128(9): 154-163.
 - 48 袁峰. SM9 标识密码算法综述[J]. 信息安全研究, 2016, 2(11): 1008-1027.
 - 49 Cremers C J F. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols[C]// Proceedings of the 20th international conference on Computer Aided Verification. ACM, 7-14 July 2008, Princeton, NJ, USA, 2008: 414-418.
 - 50 崔杰, 党耀国, 刘思峰. 基于灰色关联度求解指标权重的改进方法[J]. 中国管理科学, 2008(5): 143-147.
 - 51 谢丽霞, 魏瑞炘. 一种面向物联网节点的综合信任度评估模型[J]. 西安电子科技大学学报, 2019, 46(4): 58-65.
 - 52 Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based Framework for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37.

-
- 53 WANG T, LI Y, CHEN Y, et al. Fog-based Evaluation Approach for Trustworthy Communication in Sensor-cloud System[J]. IEEE Communications Letters, 2017, 21(11): 2532-2535.

攻读硕士学位期间所发表的学术论文

- 1 Zhao G.S, Qu X.F, Liao Y.T, Wang T.T, Zhang J.T. Cloud Service Security Adaptive Target Detection Algorithm Based on Bio-Inspired Performance Evaluation Process Algebra (Bio-PEPA)[J].WuhanUniversityJournalofNaturalSciences,2019,24(3):185-193
- 2 王甜甜,李晶,纪雷,余周安. 一种面向边缘计算的身份认证方案[J]. 科学与技术, 2019(17): 43.

致谢

岁月不居，时节如流。行文至此也意味着两年的研究生生涯已进入尾声，感触良多不知从何下笔。两年的科研学习的经历，虽然短暂但是教会我如何独立思考，同时提高了我学习新知识的能力，在科研学习的过程中认识很多人，发生很多事，在论文完成之际，我要向曾经帮助我的朋友和同学表以致谢。

老师是我们知识的源泉，思想的脐带，灵魂的雕刻者，所以我最应该感谢的是赵国生教授和李晶副教授，在整个科研过程中，两位老师给予了我太多帮助，两位老师对于科研的严谨的态度，渊博的见识，长远的眼界和对学生平易近人的性格无不令我佩服。从刚入试验室到确定研究方向再到最后毕业论文的撰写，赵老师耐心的指导我，对于论文的不足给我提供了宝贵的意见，同时引导我去寻找解决问题的方法。无论是学习还是生活中遇到挫折或是不顺心的事，两位老师也是很耐心的为我解惑。

其次，还要感谢研究生学习期间教授我知识的老师对我学业上的关心与帮助；尤其感谢张慧、谢宝文、晁绵星、廖玉婷、张婧婷、刘冬梅等同门师兄弟，每次在学术报告会议上为我答疑解惑，互帮互助共同进步，一起播撒汗水，其间凝聚着多少的欢乐和祝福，都值得我们认真回味；感谢学院的领导和导员刘琪老师，无论是在学习还是生活中，他们都给予最大的关心和帮助以及感谢学校为因疫情在家的学子们提供学习的平台与机会。

最后要感谢我的父母和家人对我极大的鼓励，他们为我提供了优质的生活条件，也是我精神上的支柱，是你们见证了我的成熟和一次次的蜕变，成为我坚强的后盾。

此外，衷心的感谢各位评审专家和老师对于本论文给出的中肯的意见和评阅。