基于协作信誉和设备反馈的物联网边缘服务器信任评估算法

张琳[1,2]，魏新艳[1]，刘茜萍[1]，黄海平[1,2]，王汝传[1,2]
（1. 南京邮电大学计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003）

摘 要：针对边缘服务器的安全问题，提出了一种集成了服务器协作信誉以及设备用户反馈的信任评估算法来提高边缘计算上下文的安全性。交互过程中，使用了一种基于客观信息熵理论的融合算法来聚合服务器间的协作信誉，同时采用了部分同态加密算法来防止交互过程中用户数据的泄露。交互结束后，选择高可信的设备节点计算反馈信任，克服了传统机制的恶意反馈。在计算全局信任时，考虑了服务器的期望评分和自适应的权重计算算法，克服了传统信任方案的局限性。实验结果表明，所提信任度计算方案具有较低的时间复杂度和空间复杂度，并且可以有效抵抗恶意节点的攻击行为。

关键词：物联网；边缘服务器；信誉；反馈；信任聚合
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022024

Trust evaluation algorithm of IoT edge server based on cooperation reputation and device feedback

ZHANG Lin[1,2], WEI Xinyan[1], LIU Xiping[1], HUANG Haiping[1,2], WANG Ruchuan[1,2]
1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China

Abstract: Aiming at the security problem of edge server, a trust evaluation algorithm was proposed, which integrated server cooperation reputation and device user feedback to improve the security of edge computing context. In the process of interaction, a fusion algorithm based on objective information entropy theory was used to aggregate the cooperation reputation between servers, and a partial homomorphic encryption algorithm was used to prevent the leakage of user data in the process of interaction. After the interaction, the highly trusted device node was selected to calculate the feedback trust, which overcame the malicious feedback of the traditional mechanism. When calculating the global trust, the expected score of the server and the adaptive weight calculation method were considered, which overcame the limitations of the traditional trust scheme. The experimental results show that the proposed trust calculation scheme has low time complexity and spatial complexity, and can effectively resist the attack of malicious nodes.

Keywords: Internet of things, edge server, reputation, feedback, trust aggregation

0 引言

随着 5G 移动通信和云计算技术的快速发展，移动应用的数据量呈爆炸性增长，在物联网领域引起了极大的关注。传统的人与人社交扩展到了人与物、物与物的更广阔的网络中，物联网可以无缝透明地整合大量异构智能设备或终端系统，同时，数据子集的开放访问为开发数字服务提供了便利。物联网环境中计算复杂性高和数据存储量大的任务通常由资源丰富的云服务器来处理，为了减少传输

收稿日期：2021−05−06；**修回日期**：2021−10−20
基金项目：国家自然科学基金资助项目（No.61572260, No.61872196, No.61872194）；江苏省科技支撑计划基金资助项目（No.BE2017166）
Foundation Items: The National Natural Science Foundation of China (No.61572260, No.61872196, No.61872194), Scientific and Technological Support Project of Jiangsu Province (No.BE2017166)

数据量以及系统开销，可以通过在分布式网络的边缘执行数据处理来优化云计算系统，这种方式称为边缘计算。同时，它还涵盖了广泛的技术，包括物联网（IoT, Internet of things）边缘计算[1]、云计算、雾计算[2]、分布式数据存储、增强现实等。

物联网和边缘服务的集成是当前新的研究热点。与许多新技术一样，边缘计算环境中也存在诸多挑战，主要分为两类：安全性（设备网络）和信任关系（恶意节点反馈和攻击）。因此，物联网面临的安全性挑战转移到了边缘网络中。为了解决边缘网络上下文环境的安全问题，可以选择可信赖的边缘服务器（ES, edge server）进行交易。但是，鲜有关注边缘服务器可信度的研究，并且评估边缘计算的上下文安全的文献更是少之又少。因此，本文着重于通过使用信誉和反馈的信任评估算法计算服务器的可信赖性，从而提高基于边缘计算的 IoT 上下文的安全性。

由于越来越多的具有相似功能特性的提供者竞争边缘服务器，探讨边缘服务器的可信赖性已成为最具挑战性的课题之一。与传统的网络安全认证机制不同，信任计算机制在服务提供中有动态行为感知能力，并且可采取预防措施来认证服务提供者的恶意服务行为[3]。作为一种传统网络安全的补充技术，信任机制通过判断服务质量[4]解决了提供相应访问控制的问题，提高了服务可靠性。为了确保协作服务行为的质量并帮助边缘设备之间建立信任，物联网边缘计算服务商使用了基于协作的信任机制[5]。这些研究专注于利用与边缘服务器的相互质量评分来评估 ES 的可信赖性，即服务的综合信誉度量。

用户反馈会影响边缘设备用户（EDU, edge device user）的选择，而传统文献在反馈信任评估中没有考虑设备层安全性。尽管反馈评级可以捕获服务器的某些信任功能，但它们远非 ES 可信度的完备衡量标准。尽管已有一些工作尝试保护设备层的隐私数据、评估服务器的可信赖性[6]，但由于缺乏细粒度的安全性度量，安全性没有明显改善。

另外，在边缘计算中所有设备节点直接或通过中继连接到可靠性未知的其他服务器节点，设备之间构成了 D2D（device-to-device）网络，服务器之间构成了 S2S（service-to-service）网络，这可能导致设备敏感数据被未知或不受信任的节点获取，使设备网络的数据隐私保护面临风险[7]。

当前研究中主要有 4 种网络通信的数据保护算法[8]，分别是访问控制、数据混淆、数据匿名化和同态加密。访问控制[9]是利用访问者身份及系统预先定义的策略限制访问资源的权限，保护用户数据隐私，通常用于系统管理员控制用户对服务器、文件等网络资源的访问。数据混淆[10]是基于摘要信息保护数据隐私或提供虚假信息以降低数据准确性。数据匿名化[11]是已发布的私有数据包含一定数量的假名，使接收此类数据的移动设备节点无法识别私有数据所有者。传统的非对称加密算法只能对解密后的明文进行计算[12]，无法执行对密文的数据安全聚合操作，从而难以对数据实行高效的隐私保护，引入同态加密[13]对用户反馈评分进行保护，可以在边缘服务器上执行密文安全聚合操作而不需要解密。

本文结合边缘服务器的协作信誉和设备用户的安全反馈，提出了一种基于信誉和反馈的信任评估（TERF, trust evaluation based on reputation and feedback）算法。本文的主要贡献如下。

1) 提出物联网边缘计算中基于信誉和反馈融合的安全可靠的信任评估算法。在物联网中，信任是衡量网络安全的重要标准，并且信任难以被量化和预测。本文将服务器信誉和用户反馈信息进行融合来评估边缘服务器的可信赖性，这种组合降低了网络风险，也大大提高了信任评估的准确性。

2) 为了评估边缘服务的可信度，提出了一种基于客观信息熵的信任评估算法，该算法通过使用对边缘服务质量的协作评分来评估边缘服务的信誉。为了评估边缘服务相对于反馈的可信度，提出了一种基于设备反馈的信任评估算法，该算法首先对用户数据进行部分同态加密处理，然后利用高信任节点的反馈评分来评估边缘服务的安全性。

3) 为了将信誉和反馈结果有效地集成到边缘服务的信任评估中，依据可信用户对边缘服务的期望评分提出了一种集成的自适应信任评估算法，从而获得边缘服务的可量化的信任值。

1　相关工作

文献[14]全面阐述了边缘计算中数据安全与隐私保护的研究背景，提出以安全为中心的体系架构。围绕数据安全、访问控制、身份认证和隐私保护等关键技术，探讨了近年来针对边缘计算安全的最新研究成果。Huang 等[15]提出了一种用于安全高效的车辆边缘计算和网络的分布式信誉管理，采用车辆边缘计算服务器来执行车辆的本地信誉管理

任务。文献[16]针对云服务提供商不能被完全信任的情况，提出了基于属性加密的流程加密策略，分为密钥策略和密文策略。加密者通过将接收者的访问策略融入加密消息里来指定密文的接收者；当解密者满足密文中描述的访问策略时，才可恢复明文消息。文献[17]针对提交的恶意评价，采用控制图理论对评价中的数据进行过滤，通过信息熵对不同维度的评价数据进行融合，从而进一步得到综合信誉。

云服务的可信度通常会根据用户的经验和意见来评估。文献[18]对传感云和信任评价机制进行调研，归纳了传感云的信任评价机制并探讨了雾计算信任机制未来的研究方向。Nagarajan 等[19]提出使用大数据处理框架来评估云服务的可信赖性，通过集成 MapReduce 框架的云代理来预处理反馈评估。文献[20]提出一种新颖的信任评估算法将反馈评估组件和贝叶斯博弈模型相结合，以识别恶意用户及其反馈评级。前者用于检查和识别伪造身份，后者用于检测恶意用户及其反馈。文献[21]针对传感器系统中存在的数据不可信问题，设计了基于边缘计算的传感云可信数据收集框架，利用移动边缘节点进行可信的数据收集，解决了底层传感器计算能力太弱和节点面临的内部恶意攻击问题。

由于服务器捕获的图像数据与用户的个人隐私信息密切相关，交易过程中应该注重用户的隐私数据保护。Li 等[22]为了减少终端设备的资源消耗，提出了一种用于图像处理的边缘辅助的隐私保护外包计算框架，通过边缘节点与终端设备协作以保护数据并支持半信任云服务器上的隐私保护计算。

从上述相关工作可以看出，现有关于服务器信任评估的研究主要分为两类，即基于信誉的评估算法和基于反馈评级的算法。但是，这些工作没有考虑边缘设备与服务器交互时数据的安全性。基于此，本文提出了一种结合设备层安全反馈和服务器层信誉的综合信任评估算法。该算法不仅基于各服务器的协作来评估服务器的安全级别，而且在保护设备层隐私数据的基础上用反馈等级评估服务器的信任，从而保证了边缘网络上下文的安全性。

2 前提与概述

2.1 问题的提出

根据边缘计算中网络设备的功能，信任涉及 2 种来源，即服务器和设备（物联网用户），本文定义一个元组 $G=\langle S,E,M,D\rangle$，其中 S 为边缘服务器的集合，E 为服务器之间的边的集合，M 为服务器发出的消息的集合，D 为物联网边缘设备的集合。节点 $s_i \in S, i=1,2,\cdots,m$ 表示边缘服务器，边 $e_{ij} \in E$ 表示服务器 s_i 与服务器 s_j 之间的交互，M_i 表示服务器 s_i 发布的一组信息，$d_k \in D, k=1,2,\cdots,m$ 表示物联网设备。信任度评估和模型是信任管理的核心技术，在介绍可信度计算机制的细节之前，本节首先介绍一些关于可信度的基本定义，可信度的取值范围为[0,1]。

定义 1 直接信任。关于服务器 s_i 到另一个服务器 s_j 的直接信任称为 S2S 直接信任。直接信任是服务器完成请求任务能力的量化值，是基于 2 个服务器之间交互式记录的历史记录，涉及相似度、历史行为和关注度等因素。

定义 2 间接信任。关于边缘设备 d_j 到一个服务器 s_i 的反馈信任称为 D2S（device-to-service）间接信任。当服务器数据处理任务完成后，边缘设备将客观计算服务器 s_i 的反馈评分；当另一个服务器 s_j 请求它时，边缘设备将反馈值发送给请求者。

2.2 体系结构

本节介绍基于云的边缘计算三层网络架构如图 1 所示。该架构由四部分组成：云数据中心、边缘网络、中继和设备网络。云数据中心负责数据的计算和存储；边缘网络负责传输和指定通信机制；中继是边缘网络中的计算设备；设备网络最接近用户，主要功能是采集数据。数据的处理分为 2 个模块：数据获取和数据聚合。设备网络最接近用户，可以直接获取信息，一般借助中继或第三方进行计算加工。边缘网络负责信息聚合处理，主要对数据进行分析处理。

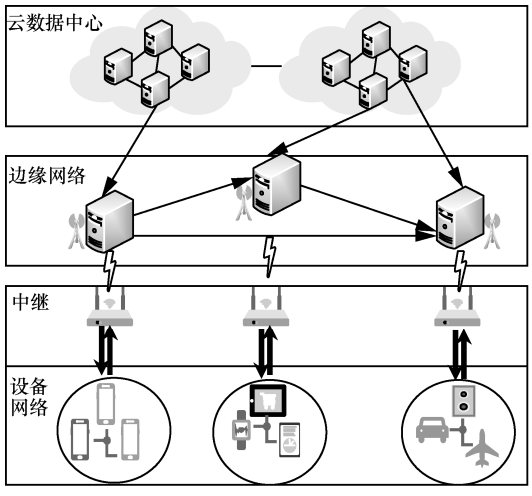

图 1 基于云的边缘计算三层架构

3　基于信誉和反馈的信任评估算法

本节介绍信誉评估模型和反馈评估算法。该算法由 2 个主要模块组成：信任数据获取模块和聚合信任计算模块。基于信誉和反馈的信任评估算法如图 2 所示。首先，通过云服务中心获取服务器的身份信息，如授权认证、相似度、共同行为以及关注度来评估服务器的直接信任因子，并将相关数据存储至数据库。然后，计算边缘服务器反馈（即同伴反馈）和边缘设备用户反馈（即用户反馈）来获取间接信任。每个边缘服务器在进入交互网络前需要从云中心获得一个证书作为入场凭证，应用程序接口以实时监控的形式协作网络中收集协作网络中服务器间协作的历史评分（同伴反馈）获得服务器基于信誉的信任。用户交易后会对服务进行评价，通过筛选器选出高可信用户的反馈，并对用户数据进行加密。最后，利用可信用户的平均期望计算自适应权重因子，获得每个服务器的全局信任评分。根据信任得分的高低划分不同的服务等级，实现差别化管理。

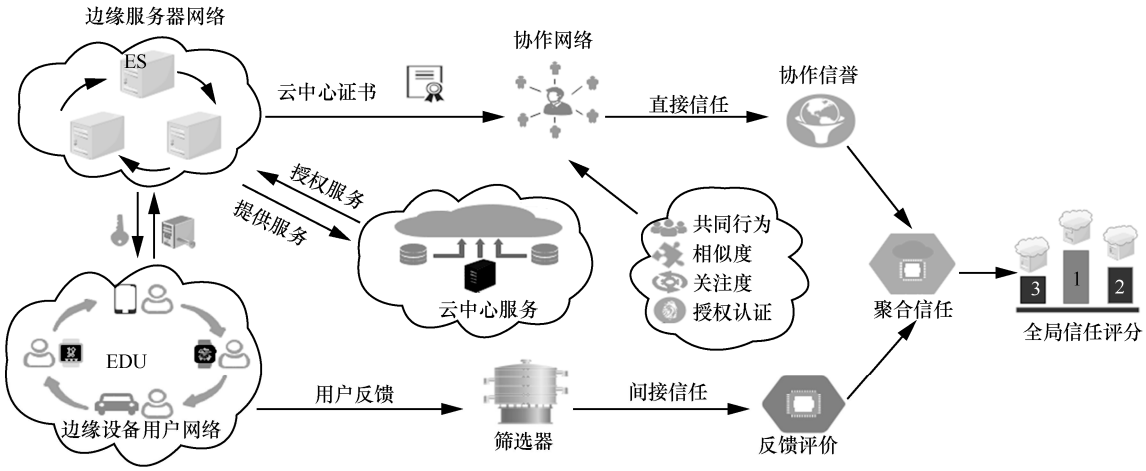

图 2　基于信誉和反馈的信任评估算法

3.1　信誉评估模型

3.1.1　直接信任值计算

物联网边缘计算网络中，边缘服务器的直接信任通常与身份的授权认证、相似度、共同行为和受欢迎度有关，直接信任计算模型如图 3 所示。

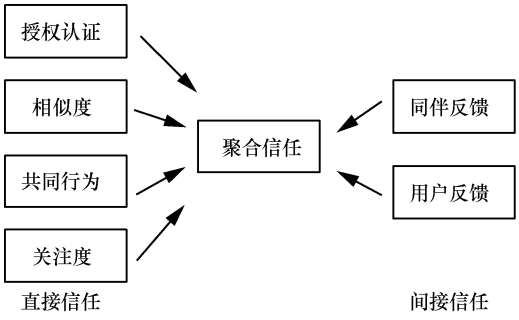

图 3　直接信任计算模型

1) 基于身份的信任档案信息已被证明与服务器的可信度相关。通常，信任取值为 0～1，0 表示不可信，1 表示可信。经过云中心身份验证的服务器可信度为 1，匿名服务器因为身份不明，可信度设为 0.2。因此，服务器 s_i 的授权认证 $\mathrm{AC}(s_i)$ 为

$$\mathrm{AC}(s_i)=\begin{cases}1, \text{已被认证授权的服务器}\\ 0.2, \text{匿名服务器}\end{cases} \tag{1}$$

2) 在边缘计算网络中，服务器节点与节点之间通常具有一定的相似性。若 2 个节点在行为上具有较高的相似性，则表明它们更容易信任对方。所以，可以利用服务器之间的相似度来度量服务器间的信任，相似度越大则越可信。服务器 s_i 与 s_j 的相似度 $\mathrm{SM}(s_i,s_j)$ 为

$$\mathrm{SM}(s_i,s_j)=\frac{\sum_{i=1}^{n}s_i s_j}{\sqrt{\sum_{i=1}^{n}s_i^{\,2}}\sqrt{\sum_{j=1}^{n}s_j^{\,2}}} \tag{2}$$

3) 共同行为。如果边缘网络中的任何 2 个服务器都提供类似的服务或采用相同的建议，则表明交易对象可信任。如果 s_i 具有与 s_j 相同的行为，bh_{s_i} 为 s_i 的行为集合，bh_{s_j} 为 s_j 的行为集合，共同行为的信任 $\mathrm{BH}(s_i,s_j)$ 为

$$\mathrm{BH}\left(s_i,s_j\right)=\frac{\log\left(\mathrm{bh}_{s_i}\cap\mathrm{bh}_{s_j}\right)}{\log\left(\mathrm{bh}_{s_i}\right)} \tag{3}$$

4) 关注度。通常，服务器的关注者数量反映了其服务质量和信任度，如果关注者数量越多，则该服务器的服务质量越高，可信值也越高。$\mathrm{NFollow}(s_i)$ 表示服务器 s_i 的关注者数量，$\mathrm{NFollow}(s_j)$ 表示服务器 s_j 的关注者数量。服务器 s_i 的社会受欢迎程度 $\mathrm{PL}(s_i)$ 为

$$\mathrm{PL}\left(s_i\right)=\frac{\log\left(\mathrm{NFollow}\left(s_i\right)+1\right)}{\log\left(\max\left(\mathrm{NFollow}\left(s_j\right)+1\right)\right)},s_j\in S \tag{4}$$

因此，综合上述四方面的平均值，可计算边缘服务器的直接信任值 $\mathrm{DT}(s_i)$ 为

$$\mathrm{DT}\left(s_i\right)=\frac{\mathrm{AC}\left(s_i\right)+\mathrm{SM}\left(s_i,s_j\right)+\mathrm{BH}\left(s_i,s_j\right)+\mathrm{PL}\left(s_i\right)}{4} \tag{5}$$

3.1.2 基于客观信息熵的信任聚合

假设在边缘服务器集群中存在 n 个服务器 $s_i=\{s_1,s_2,\cdots,s_n\}$，服务器在集群中广播请求数据包。作为响应，群集中的所有设备都将其信任值转发到 s_i。然后，s_i 对应的数据库获得一个由边缘服务协作信任组成的数组 $T_{s_i\to s_j}$，即

$$T_{s_i\to s_j}=\begin{Bmatrix}D_{(s_1,s_1)}(\Delta t) & \cdots & D_{(s_1,s_n)}(\Delta t)\\ \cdots & D_{(s_i,s_j)}(\Delta t) & \cdots\\ D_{(s_n,s_1)}(\Delta t) & \cdots & D_{(s_n,s_n)}(\Delta t)\end{Bmatrix} \tag{6}$$

其中，$D_{(s_i,s_j)}(\Delta t)$ 是关于 s_j 的 S2S 信任。当 $i=j$ 时，该值就是服务器对其自身的评分。为了减少信任欺骗，该值将在信任汇总期间被丢弃。

首先，需要对输入数据进行规范化处理形成归一化决策矩阵 $\boldsymbol{Q}_{n\times n}$，其元素 $Q_{(s_i,s_j)}(\Delta t)\in[0,1]$。然后，利用客观信息熵计算权重，聚合服务器协作评分的信任。

$$p_{ij}=\begin{cases}\dfrac{Q_{(s_i,s_j)}(\Delta t)}{\sum_{i=1}^{n}Q_{(s_i,s_j)}(\Delta t)}, & i=1,2,\cdots,n\\ 0, & \text{无效}\end{cases} \tag{7}$$

$$e_i=-\frac{1}{\ln(n)}\sum_{i=1}^{n}p_{ij}\ln(p_{ij}) \tag{8}$$

$$w_i=\frac{1-e_i}{n-\sum_{i=1}^{n}e_i} \tag{9}$$

其中，p_{ij} 为服务器之间评分所占的概率，e_i 为评分占比的不确定性，w_i 为每个服务器的质量评估所占据的重要性。

因此，边缘服务器基于协作的信誉计算式为

$$\mathrm{RT}\left(s_i\right)=\sum_{i=1}^{n}w_i\mathrm{DT}\left(s_i\right) \tag{10}$$

使用客观信息熵理论来计算服务器的信誉，可以克服传统信任方案的局限性，因此，所提信任评估算法既能鼓励服务器之间相互协作，又能抵御恶意服务器引起的不良行为攻击。

3.2 反馈评估模型

获取边缘设备的反馈数据时，很可能会泄露边缘设备用户的敏感数据。为了在保护用户隐私的同时又能实现数据的可用性，可以在数据获取前对用户敏感数据进行隐私保护，使服务器只能获取指定的相关信息，不能获取其他敏感信息，如位置、爱好、兴趣、社交关系等，从而在实现数据可用性的同时有效保护用户数据的隐私。

然后，从加密后的用户数据中选择高信任节点计算用户的反馈信任。反馈等级使用元组 $\mathrm{FD}=\{D(\mathrm{id}),S(\mathrm{id}),\mathrm{attr}(s_i),F(s_i),\Delta t\}$ 表示，其中，$D(\mathrm{id})$ 和 $S(\mathrm{id})$ 分别表示设备用户和边缘服务器的身份，$\mathrm{attr}(s_i)$ 表示服务器的资源或属性，$F(s_i)$ 表示用户对服务器的反馈评分，Δt 表示用户与服务器交互的时间戳。每个多元组代表对来自云平台的边缘服务的特定属性或整体质量的反馈评分。因此，反馈评分的可信度和确定性在此模型中对评估边缘服务的可信赖性起着重要作用。为了减轻短时间内恶意用户的不真实反馈评级对信誉评估的负面影响，引入高信任反馈节点和确定性权重因子。

3.2.1 同态加密技术

在物联网边缘网络中，移动设备节点通常需要请求整个网络中的信息资源，并且这些资源通常包含一些私有信息。如果直接将相关数据发送给请求设备，容易造成隐私泄露和不安全的 D2D 网络，因此，私有数据需要加密后再发送给请求数据的设备。为了保护设备用户数据隐私，将 Paillier 同态加密模型引入该网络中。同态加密技术[12]满足以下特性。

1) 主要术语

① Paillier 加密。直接计算多重加密的数据以获得集成的密文，该密文与通过相同方式处理未加密的原始数据所获得的密文相同。

在 Paillier 密码系统中，公钥（加密）$\mathrm{PK}=(n,g)$，其中 $n=pq$，p 和 q 是 2 个随机选择的大质数，g 是从正整数中选择的随机整数。私钥（解密）为 $\mathrm{SK}=(\phi,\mu)$，其中 $\phi=L_{cm}(p-1,q-1)$，其中 L_{cm} 表示最小公倍数，$\mu=L\left(g^{\phi}\bmod n^2\right)^{-1}\cdot \bmod n$，$L(x)=\dfrac{x-1}{n}$。假设消息 m 的加密为[m]，加密后可以得到密文 $c=\left[m\right]=(g^m r^n)\bmod n^2$，其中，$r$ 是从正整数中选择的随机掩码，且 $r\in(0,n)$。密文 c 的解密为 $m=L(c^{\phi}\bmod n^2)\mu \bmod n$。

② 同态加法。假设原有消息为 a 和 b，加密后的消息分别为[a] 和[b]，则可以得到 $[(a+b)\bmod n]=[a][b]\bmod n^2$ 和 $[(ab)\bmod n]=[a]^b \bmod n^2$。

③ 不可辨别性。如果明文 a 被同时加密两次，则得到的 2 个密文是完全不同的。

④ 自盲性。任意一个密文可以被转化为另一个密文，不会影响明文。

2) 主要想法

设备网络中的节点向边缘服务网络发出服务请求，边缘服务器给出响应完成功能服务。然后，服务器网络可以通过设备中继向 D2D 网络广播反馈质量请求，每个用户收到请求后对需要提供的私有数据进行加密并将公钥发送出去，中继聚合反馈评分信息发送给服务器，服务器利用公钥获取所需评分信息。为了减少加密开销，本文使用部分同态加密技术，边缘计算中的服务器只可以获取所需反馈信息，可有效保护边缘设备的隐私数据信息，从而促进用户做出真实反馈，构建良好的边缘网络环境。

收集 D2D 网络中每个节点的密文后，中继节点为了防止设备节点的敏感数据被请求服务器节点泄露，对设备的隐私构成威胁，因此需要对接收到的数据执行部分同态加密，如算法 1 所示。最后，将处理后的密文发送到服务器节点，因此请求节点服务器只能获取请求的数据，不能从单节点设备获取其他数据，从而保护了每个节点设备的私有数据。在计算边缘设备的反馈评分时，默认设备代理中继是可信的，这种设定符合现实生活中的情况。

算法 1　安全信任聚合

输入　待加密数据集 M、a、b、n、s_i 等相关系数

输出　安全聚合后的信任值

1) for $i=0\rightarrow M.\mathrm{length}$ do

2) $\mathrm{PK}=(n,g)$ //加密

3) $[(a+b)\bmod n]=[a][b]\bmod n^2$

4) $[(a*b)\bmod n]=[a]^b \bmod n^2$。

5) $C^*=M\left[i\right]$ //密文

6) $\mathrm{FT}\left(s_i\right)=\sum_{j=1}^{m}F_{ij}\left(\Delta t\right)\partial_{s_i}^{j}\left(\Delta t\right)$

7) $\partial_{s_i}^{j}\left(\Delta t\right)=1-\dfrac{\mathrm{NF}(i,j)-\mathrm{avg}(|F_i|)}{\left|F_i\right|}$

8) $\mathrm{LT}\left(s_i\right)=\alpha\mathrm{RT}\left(s_i\right)+\left(1-\alpha\right)\mathrm{FT}\left(s_i\right)$

9) end for

10)return $\mathrm{LT}\left(s_i\right)$

3.2.2　可信反馈

考虑到拥有数万个物联网服务器每秒处理数百个设备的大规模边缘网络环境，如何缩短信任系统引起的时延是一个具有挑战性的课题。因此，具有高计算效率的反馈聚集机制是最基本的要求。在这项工作中，本文设计了一个轻量级的高效反馈机制。

大多数物联网平台都为用户提供功能报告，用户一旦发现某个边缘服务器有恶意，就可以将其上报给平台。通常，用户的反馈不会得到足够的重视，甚至会被忽略，这对于评估来源的可信度至关重要。因此仅考虑来自边缘设备总体信任度 $T\left(d_i\right)$ 不小于预定义阈值（将其经验设置为 0.6）的报告者的反馈。边缘服务器的反馈通常是针对特定属性或者整体的服务质量、响应时间等。

物联网用户 d_j 基于反馈的信任为

$$F_{ij}\left(\Delta t\right)=\frac{f_{s_i}^{+}\left(\Delta t\right)+1}{f_{s_i}^{+}\left(\Delta t\right)+f_{s_i}^{-}\left(\Delta t\right)+2} \tag{11}$$

用户对服务器的反馈信任为

$$\mathrm{FT}\left(s_i\right)=\sum_{j=1}^{m}F_{ij}\left(\Delta t\right)\partial_{s_i}^{j}\left(\Delta t\right) \tag{12}$$

其中，物联网用户的总体信任度 $T\left(s_i\right)\geqslant 0.6$，$f_{s_i}^{+}\left(\Delta t\right)$ 是对信息源 s_i 的正反馈数，$f_{s_i}^{-}\left(\Delta t\right)$ 是对信息源 s_i 的负反馈数，Δt 是给定的时间窗口，$\partial_{s_i}^{j}\left(\Delta t\right)$ 是用户反馈的确定性因子。

3.2.3 确定性因子

值得考虑的是，一些恶意的边缘设备通过创建大量的假名来颠覆反馈评估模型，并使用它们提供大量不忠实的反馈评级，目的是短时间内在网络中进行自我促销或诽谤性攻击。反馈评估模型中提供的确定性权重因子可以通过在短时间内保持恒定数量的客户有效反馈等级来减轻这些攻击对信誉评估结果的影响，计算式为

$$\partial_{s_i}^{j}(\Delta t)=1-\frac{\mathrm{NF}(i,j)-\mathrm{avg}(|F_i|)}{|F_i|} \tag{13}$$

在给定的时间窗口 Δt， $\mathrm{NF}(i,j)$ 表示设备用户 d_j 在服务器 $s_i, s_i\in S$ 上提供的反馈评级的数量，$|F_i|$ 表示边缘服务器 s_i 接收到的反馈等级的总数，$\mathrm{avg}(|F_i|)$ 表示服务去器 s_i 接收到的反馈等级数的平均值，即

$$\mathrm{avg}(|F_i|)=\frac{\sum_{j=1}^{m}(\mathrm{NF}(i,j)-\varepsilon)}{|U|} \tag{14}$$

其中，ε 表示 d_j 在指定时间范围内对边缘服务器提供的反馈等级数量的有效阈值，多余的将被丢弃；$|U|$ 表示为服务器 s_i 提供反馈评级的用户数量。

3.3 自适应权重

在计算直接信任值和间接信任值之后，本文通过式(15)计算获得边缘计算网络中服务器 s_i 的局部信任（LT, local trust）。

$$\mathrm{LT}(s_i)=\alpha\mathrm{RT}(s_i)+(1-\alpha)\mathrm{FT}(s_i) \tag{15}$$

其中，α 是权重系数且 $\alpha\in(0,1)$，用于权衡信誉信任值相对于反馈信任值的重要性。通常，边缘服务器 s_i 的信任度应该近似于使用过 s_i 的用户（即直接信任节点）的平均满意度。因此，将 α 的选择转化为一个最小值优化问题，利用均方误差代表实际值和理想值的误差，即

$$\min(R(\alpha))=\left[\psi-\mathrm{LT}(s_i)\right]^2 \tag{16}$$

其中，ψ 是受信任节点的平均满意度，即 s_i 的期望值。在解决上述优化问题之前，首先需要确定 ψ。

根据上述定义可知，ψ 与直接受信任节点提供的评分有关。令 R 为 k 个可信节点对服务 s_i 提供的全局信任评分集合，即 $R=\{r_1,r_2,\cdots,r_k\}$。通常，评级包含正和负 2 种类型。因此，R 可以分为 2 个子集：正评级集 R^{p} 和负评级集 R^{n}。本文分别用 λ 和 μ 表示正负评级的基数，即 $\lambda=|R^{\mathrm{p}}|$，$\mu=|R^{\mathrm{n}}|$，并在仿真中给出分类原则。

Beta 函数具有强大的数学理论并且在信任管理中很受欢迎，本文使用它来计算服务器 s_i 的期望值。在 IoT 中，k 个可信节点经历了由边缘服务器 s_i 提供的服务后，会产生反馈评分 R，其中每一个评分 $r_i\in R^{\mathrm{p}}$ 或 R^{n}。因此，使用 1、0 分别表示正面评分和负面评分。

Beta 分布是先前的 Bernoulli 分布的共轭。通过这种方式，可以将边缘服务器的全局评分视为伯努利实验的结果，设正评级参数 τ 的概率遵循 Beta 分布。对于 k 个直接受信任的节点，可以将其视为每个节点的二项式分布，并在 Beta 分布之后具有正评级参数 τ 的概率。

因此，期望值 ψ 计算式为

$$\psi=\rho(\tau)=\int_{-\infty}^{+\infty}\tau f(\tau\mid\lambda,\mu)\mathrm{d}\tau=\int_{0}^{1}\tau f(\tau\mid\lambda,\mu)\mathrm{d}\tau=\frac{\lambda}{\lambda+\mu} \tag{17}$$

其中，满足 λ,μ 的概率密度函数 $f(\tau\mid\lambda,\mu)$ 为

$$f(\tau|\lambda,\mu)=\frac{\Gamma(\lambda+\mu)}{\Gamma(\lambda)+\Gamma(\mu)}\tau^{\lambda-1}(1-\lambda)^{\mu-1} \tag{18}$$

获得 ψ 后，接下来考虑优化问题。由于 $R(\alpha)$ 是参数 α 构成的函数，函数最小值是在导数为零的点处获得的，令 $\frac{\partial R(\alpha)}{\partial\alpha}=0$，可得

$$\tilde{a}=\frac{\psi(s_i)-\mathrm{FT}(s_i)}{\mathrm{RT}(s_i)-\mathrm{FT}(s_i)} \tag{19}$$

α 的最佳值应在[0,1]内，即

$$\alpha=\begin{cases}0, & \tilde{a}<0\\ \tilde{a}, & 0\leqslant\tilde{a}\leqslant1\\ 1, & \tilde{a}>1\end{cases} \tag{20}$$

完成上述操作后，将 α 代入优化式，可以获得由边缘服务器 s_i 的全局信任值。

3.4 全局信任的聚集

前 3 个阶段已获得代表单位时间窗口中每个边缘服务器的局部信任。此阶段，可以通过将每个边缘服务器的 LT 与基于时间的权重进行聚合来获得表示评估时段内每个边缘服务器的全局信任（GT, global trust）。因此，可以用定义 3 来详细描述。

定义 3　对于给定的连续时间窗口 $T=1,2,\cdots,t$，$\rho=\{\rho_1,\rho_2,\cdots,\rho_t\},\rho_t\in(0,1)$ 表示在不同单位时间窗口中 $\mathrm{LT}(s_i)$ 基于时间的权重，$\sum_{k=1}^{t}\rho_k=1$；$\mathrm{GT}_{s_i}^{T}$ 表示在 T 时间段内边缘服务器 s_i 的全局信任，计算式为

$$\mathrm{GT}_{s_i}^{T}=\sum_{k=1}^{t}\mathrm{LT}(s_i)\rho_k \tag{21}$$

为了便于排名和比较，可以将每个边缘服务器 $\mathrm{GT}_{s_i}^{T}$ 以统一的方式归一化为[0,1]。

根据人类的社会行为习惯，较旧的知识影响较小，而新知识对信任决策的贡献更大。因此，可以将 $\rho(t)$ 定义为基于时间的衰减函数，即

$$\rho(t)=\mu+(1-\mu)\exp(-\sigma(T-t)) \tag{22}$$

其中，$\mu\in[0,1]$ 用于调整基于时间的衰减函数的效果；$\sigma\in[0,1]$ 是可调的正常数，可以根据实际情况进行相应的调整。

4　理论分析

所提信任评估算法是一种轻量级方案。与大多数现有的基于广播策略从整个群集中收集反馈由此增加系统通信开销的反馈模型不同，本文算法不使用基于广播的策略，而是根据中继的聚合反馈来设置整个设备网络的反馈值。所以，每个设备都不需要与其他设备共享信任信息，反馈信任的计算工作完全由中继或代理人完成，从而减少了系统的开销。

定理 1　时间复杂度。使用本文所提信任评估算法，整体信任计算的总时间复杂度为

$$T=O(n^2) \tag{23}$$

证明　假设 IoT 边缘计算由 m 个群集组成，并且群集的平均大小为 n。在给定的时间窗口 t 中，边缘服务器总体信任计算的总时间复杂度由算法的执行次数决定，总体信任由 2 个部分组成：S2S（信誉）和 D-to-S（反馈）。服务器之间的信誉计算主要通过相互之间的协作完成，采用客观信息熵理论自适应汇总协作设备的总体信任度，执行的最大循环数达到 n^2；设备对服务器的反馈计算主要通过高信任节点的反馈聚合而成，对设备层的信息采用了同态加密算法，牺牲部分计算开销来保护隐私，执行的最大循环数达到 n^2。所以总的时间开销应为 $T_{\text{overhead}}=2n^2$，系统的时间复杂度为 $O(n^2)$。证毕。

定理 1 表明，所提信任评估算法的时间复杂度远优于某些现有方案，例如，基于模糊的信任机制的时间复杂度为 $O(n^3\log 2n)$。与传统的信任机制（例如模糊理论[19]、贝叶斯[20]、支持向量机[23]等）相比，所提信任计算机制更轻量，所需时间更少。

定理 2　空间复杂性。使用所提的信任评估算法，涉及信任信息传递的最大通信开销为

$$S=me(n+2) \tag{24}$$

证明　假设 IoT 边缘计算 e 个边缘服务器，由 m 个设备群集组成，并且群集的平均大小为 n。在给定的时间窗口 t 中，信任计算的最大数量为 δ。S2S 只要计算服务器之间的协作的通信开销 e 即可。在一定时间段内，当边缘网络和设备网络利用同态加密算法完成交互后，每个设备将自己的反馈信息发送给中继。D-to-S 如果基于反馈信息进行信任计算，则每个服务器将向其代理发送最多一个反馈请求，并从代理接收最多一个反馈响应，代理收到请求后会将请求广播到设备网络中，每个设备收到请求后将反馈信息发送给中继。因此，反馈信息的总数为 $e(n+2)$。考虑 m 个群集的情况，在给定的时间窗口中完成信任计算的最大通信开销为 $me(n+2)\delta$。证毕。

定理 2 证明了所提信任评估算法的通信开销是线性增长的，随着设备数量的增加，集群数和系统通信开销随之增长。与传统的反馈聚合机制（例如广播机制）相比，所提反馈聚合算法重量轻且所需空间少。由于不需要考虑设备之间的反馈，这种机制可以减少网络通信开销，从而提高系统资源效率。由于本文设定了设备反馈的可信阈值，选择可靠安全的反馈信任值聚合，从而可以有效缓解恶意反馈等攻击行为的影响，降低开放或敌对计算环境中的网络风险。

5　实验分析

本节首先描述如何在模拟的 IoT 边缘网络环境中建立实验，包括如何在模拟环境中部署拟议的信任方案以及实验配置；然后，通过实验验证 TERF 算法的性能和可靠性并分析实验结果。

5.1 实验设置

为了验证和分析所提出的信任计算机制的有效性，使用 NetLogo 事件模拟器进行了广泛的实验，该事件模拟器提供了多主体可编程建模环境，并在 AI 社区的 Java 中实现。它可以轻松地对并行代理和独立代理进行建模，以模拟物联网边缘计算环境中的交互实体。仿真配置如下：Intel Core i5 2.7 GHz CPU，8 GB RAM 和 Windows 10 操作系统，实验结果通过 MATLAB R2017b 进行仿真。

为了使实验更接近真实的 IoT 计算环境，在模拟器中部署了 3 种设备：基于身份的边缘服务器、基于兴趣的边缘设备和设备代理。服务器评分程序可以是诚实服务器（HS, host server）或恶意服务器（MS, malicious server）2 种类型之一。HS 始终为任何服务器提供正确的反馈，而 MS 始终为其他服务器提供错误的实际数据反馈。设备评分程序为 2 种：诚实设备和恶意设备（MD, malicious device）。诚实设备为服务器提供正确的反馈，而恶意设备为服务器提供错误的反馈。在模拟器中，设备代理作为设备层反馈提供者的行为始终是可信任的，因为经纪人是由某些 TTP（trusted third party）管理的（例如，知名的云服务提供者）。

实验中使用的仿真参数如表 1 所示。模拟器中总共部署 6 个服务器、10 000 个设备，网络中共部署 20 个代理。模拟运行的总时间步长为 200 s，信任计算的时间窗口为 20 s。恶意设备的占比分别设置为 10%、20%和 40%。协作服务器的占比分别设置为 10%、20%和 40%，这意味着 IoT 边缘服务器系统分别处于空闲、忙碌和高度忙碌状态，由此来分析边缘服务器在机制中的信誉评分。

表 1 仿真参数

符号	描述	取值
m	边缘设备个数	10 000
n	服务器个数	6
avg(| F_i |)	特定时间内反馈均值	1
∂	反馈确定因子	0.4
pas	协作服务器占比	10%、20%、40%
md	恶意设备占比	10%、20%、40%
α	信誉的重要性	0.32

本文实验利用从 GitHub 网站获得真实世界的 Web 服务数据集，即 WSDreamdataset2。它记录了 64 个不同时间段（步长为 15 min）中来自 4 500 个 Web 服务的 142 个用户的真实反馈数据。每个服务在原始数据集中都有 2 个质量属性，即响应时间（RT, rESonse time）和吞吐量（TP, throughput）。为了客观和方便起见，在 10 个不同的时间段内随机选择了 6 个服务，并将前 100 名用户的反馈评分标识为有效数据，进行筛选获得可信设备的数据，获得了 2 个较小的数据集，分别包含 6×100×10 个条目。为了促进集成信任评估，将这 6 个服务分配给在 TERF 算法中选择的 6 个云服务提供商作为云服务。使用 2 个较小的设备数据集（即响应时间和吞吐量）来评估 6 个云服务提供商在机制中的反馈评分。

如上所述，服务器的可信赖性是通过结合信誉和反馈聚合来确定的。信誉和反馈的相对重要性权重由聚合涉及的属性计算获得。

5.2 性能验证

本文提出了一种基于信誉和反馈的信任评估算法来评估边缘服务的总体可信度，其中包含了基于协作的信誉（CRT, reputation trusted based on cooperation）评估算法和基于安全性的反馈（SFT, feedback trusted based on security）评估算法。本节将一些现有的信誉和反馈信任评估算法与本文所提信任评估算法（即 CRT 和 SFT）分别进行比较。

首先，选取相关信任因子构成数据集合，通过信息熵等计算式可以计算出 CRT 的信任值，计算过程中时间复杂度可由理论分析获得。将本文算法与其他算法比较可知，CRT 具有较少的时间开销。

然后，设置反馈实验参数，不断调整恶意节点的数量（0～25%），获得不同环境下 SFT 的信任值。将本文算法与其他算法比较可知，SFT 具有较高的安全性。

5.2.1 基于协作的信誉评估算法

为了进行性能比较，将 CRT 与其他几种声誉评估算法进行了比较。比较算法描述如下。

1) 基于平均得分的信誉（ReA, reputation based on average score）算法[24]。该算法通过调用来自用户服务的平均评级来计算每个服务的信誉，然后推荐信誉较高的服务。

2) 基于信誉修订的方法（ReM, reputation revision method）[25]。该算法在计算平均评分时，使用先验知识作为相似性的基础，这有助于识别和过滤不公平的评分。

3) 基于参与者行为的信誉分配模型（URM,

utility-based reputation model）[26]。根据客户端和服务器的预期行为和感知行为，在数学上定义基于实用程序的信誉模型。

为了将 CRT 与其他基于时间复杂度的算法进行比较，将边缘服务器的数量设置为 150，边缘设备的数量为 6～150（步长为 30）。服务器的直接信任由四大因素组成：授权认证、相似度、共同行为和关注度。此外，假设这些比较算法中的每个步骤都是一个运算，而执行运算的总数表示时间复杂度。ES 数量与时间复杂度的关系如图 4 所示。

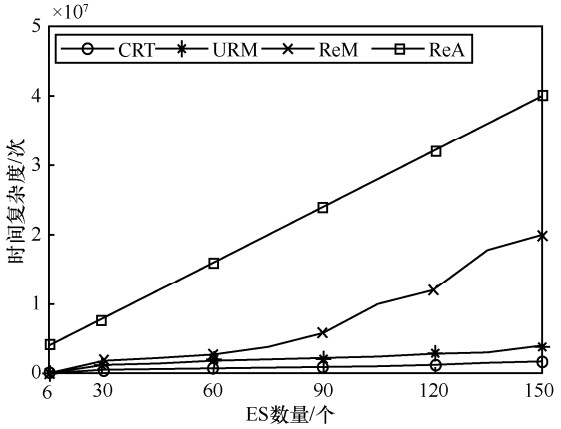

图 4　ES 数量与时间复杂度的关系

图 4 表明，当影响服务器直接信任因素的数量恒定时，随着 ES 数量的增加，时间复杂度增加。从图 4 可以看出，随着 ES 数量的增加，ReA 和 ReM 的时间复杂度均显著增加，相较而言，CRT 的时间复杂度最小，缓解了系统的开销，所以所提算法优于其他算法。由于 CRT 中采用客观信息熵理论自适应的聚合信任因子，可以鼓励服务器之间的诚信评分，促进它们的协作，因此该算法计算开销小而且能够自适应调整权重。这表明所提算法是有效的并且优于其他算法。

5.2.2　基于安全的反馈评估算法

为了进行性能比较，将 SFT 与其他几种反馈评估算法进行了比较。比较算法描述如下。

1) 基于相似度（SFM, similarity framework）的信任算法[27]。该算法可以减轻共谋攻击，并且可以有效地消除恶意推荐对信任计算的影响，提高网络可靠性。

2) 基于多源反馈（MSF, multisource feedback）信息信任算法[28]。该算法通过聚合来自用户的评级和代理的反馈来计算每个设备的信誉，然后选择信任较高的交互设备。

3) 基于体验和信誉的反馈评估（简称为 ERM）算法[29]。该算法通过评估来自用户贡献数据的质量来操纵控制交互，然后通过 2 个信任指标（经验和声誉）的设置选择最信任的用户参加传感任务，从而提高反馈质量。

为了对 SFT 进行比较实验，在单位时间窗口的吞吐量上选择 100 个边缘设备反馈评分数据，这些反馈信任通过比较算法来判断性能优劣程度。

恶意节点占比从 5%变化为 25%，观察其对反馈结果的影响。图 5 显示了不同机制应对不同恶意节点占比时的信任变化率。

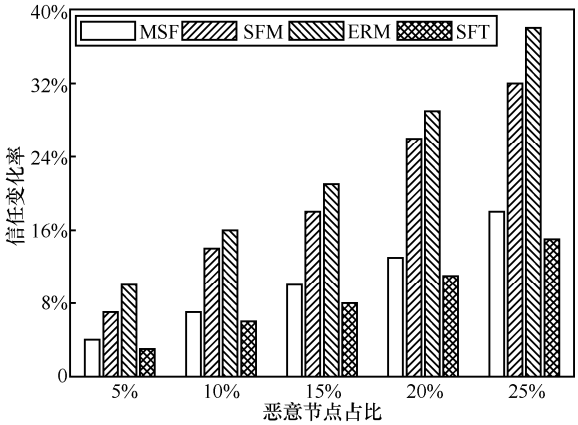

图 5　恶意节点的信任变化率

随着恶意节点的占比增加，所有比较算法的最终反馈评分都会下降，所以上述几种机制对恶意节点的反馈都可以起到抵抗作用。但是，每种算法的反馈信任值的变化是不同的，恶意节点占比与反馈信任值的关系如图 6 所示。

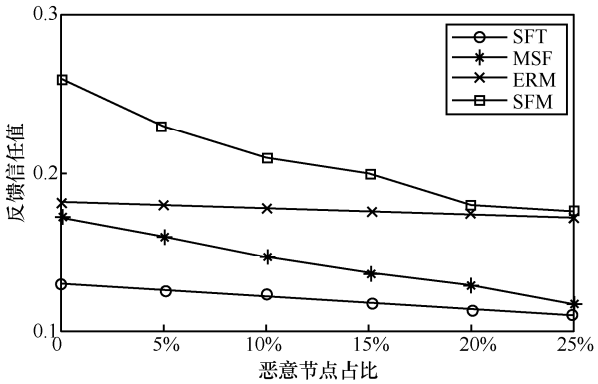

图 6　恶意节点占比与反馈信任值的关系

SFM 变化率最高，即其信誉最容易受到恶意反馈评级的影响，其次是 MSF、ERM 和 SFT，这表

明 SFT 优于其他算法。尤其是当恶意节点占比增加时，由于提出的机制不仅在设备与边缘服务器进行交互时使用了同态加密算法，保证了设备层用户的隐私安全，而且对设备的反馈评分设置了阈值，只对高信任节点的反馈评分进行聚合计算，因此 SFT 相比于其他算法能够很好地抵抗恶意反馈。

以上实验结果表明，TERF 结合了基于协作的信誉评估算法和基于安全性的反馈评估算法，有助于改善边缘服务器的信任评估。

5.3 可靠性

计算任务失败率（TFR, task failure rate）以反映信任计算系统的可靠性，将用户请求能否成功获得服务器的服务作为判断任务成功与否的依据，$\mathrm{TFR}=\frac{\mathrm{Nf}}{\mathrm{total}}\times 100\%$，其中，Nf 为失败的次数；total 为总次数，本次实验设置为 5 000 次。TFR 值越低表明信任机制的可靠性较高。在这组实验中，假设 IoT 边缘计算中的大多数设备代理都是值得信赖的协作者，并且此边缘计算环境紧密地反映了实际情况，其中大多数代理是诚实的。

本文提出信任机制面临的威胁主要来源于两方面：边缘服务器的欺骗评分和边缘设备的恶意反馈评分。本节实验考虑了以下几种网络计算环境：1) 空闲诚实的边缘计算环境；2) 繁忙且不诚实的边缘计算环境；3) 繁忙且高度不诚实的边缘计算环境。

图 7～图 9 显示了不同百分比的恶意设备对应的任务失败率。在这组实验中，假设此物联网边缘计算环境是一个值得信赖的网络社区，所有代理人都对此诚实。将恶意设备的占比设置为 10%、20%和 40%，分别表示网络环境是诚实、不诚实和高度不诚实的。

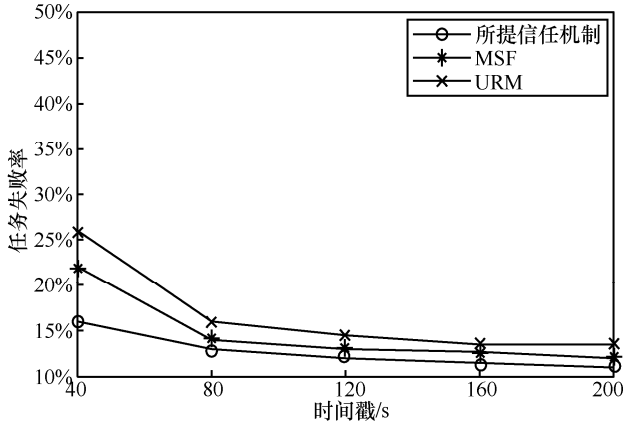

图 7 空闲诚实的边缘计算环境的任务失败率

图 7 显示了空闲诚实的网络环境，其中恶意设备的占比仅为 10%，相互协作的边缘服务器设备占比为 10%。通过比较发现，在空闲诚实的网络环境中，3 种信任机制的任务失败率均较低，平均低于 12.32%。这些结果表明，3 种类型的信任机制都具有很高的可靠性，几乎没有恶意节点。

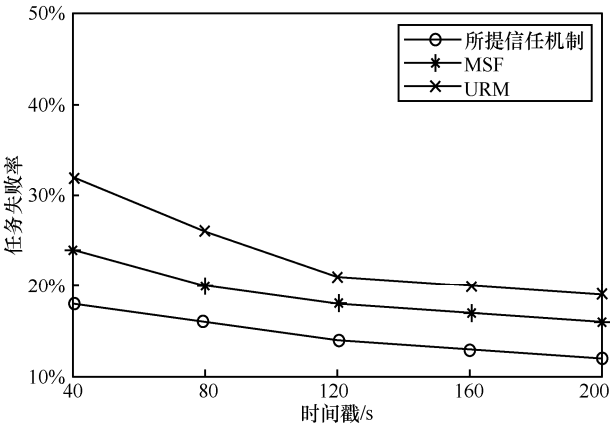

图 8 繁忙不诚实的边缘计算环境的任务失败率

为了在更动态的网络环境中评估信任机制的性能，逐渐增加了恶意设备 MD 的比例。在图 8 中，恶意设备比例为 20%，协作服务器为 20%，这意味着该系统环境是繁忙且不诚实的。通过比较发现，随着恶意设备的不断增加，任务失败率明显下降，与恶意设备为 10%时相比，差异更大，其中，MSF 和 URM 机制的性能下降明显。在图 8 中，当 MD 的比例设置为 20%时，MSF 的任务失败率增加至 19.8%，而 URM 机制的任务失败率则达到 24.36%。这表明，在繁忙且不诚实的边缘计算环境中，所提信任机制比 MSF 和 URM 具有更低的任务失败率。

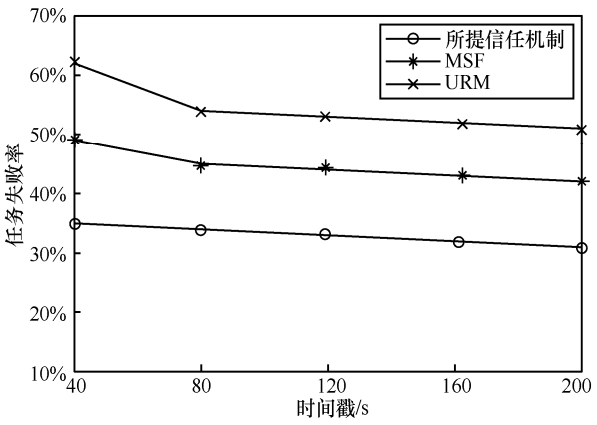

图 9 繁忙且高度不诚实的边缘计算环境的任务失败率

在图 9 中，MD 的比例为 40%，协作服务器为 40%，这意味着系统非常繁忙且高度不诚实，其中 40%的边缘设备不诚实，40%的边缘服务器要求与其他服务器协作。从图 9 可以看出，从 TFR 的角度来看，所提信任机制优于 MSF 和 URM。当 MD 的比例设置为 40%时，MSF 的任务失败率增加到 43.64%，URM 的任务失败率达到 52.83%甚至可能更高，而所提信任机制的任务失败率是 32.61%，因此本文提出的聚合信誉和反馈的信任机制的可靠性更好。实验结果与实际情况一致，即在高度不诚实的网络环境中，MD 可能会进行 ON-OFF 攻击，这可能会严重影响 IoT 边缘计算的性能。

如上所述，本文在 S2S 中采用了基于客观信息熵理论的反馈信息融合算法计算服务器内部信任，可以克服传统信任方案的局限性；在 D2D 中采用了基于同态加密算法的安全反馈，可以减少边缘设备的恶意反馈。同时由于交互过程中保护了设备层的隐私，可以鼓励设备做出诚实反馈，从而改善任务的成功执行率并降低任务失败率。最后，在整体信任度汇总计算中，采用数学算法自适应地聚合信誉和反馈，从而实现边缘服务器信任值的动态计算。

6　结束语

本文提出了一种针对边缘计算环境中服务器的新型信任评估算法，该算法结合了信誉和反馈特征，能够通过可信赖的边缘服务来增强基于云的物联网边缘环境的安全性。它还有助于物联网用户评估功能上等效的边缘服务器提供的云服务的可信赖性，并从中选择最可信赖的 ES 来部署云服务。值得注意的是，TERF 的优势在于，它可以将信誉和反馈作为衡量边缘网络信任的补充功能，从而获得定量评估边缘服务信任度。此外，为了将信誉指标纳入信任评估中，本文提出了一种基于协作的信任评估算法；为了提高基于反馈评级的信誉评估模型的安全性和可靠性，本文提出了一种基于安全性的反馈评估算法。此外，为了有效地结合 CRT 和 SFT，本文提出了一种集成的信任评估算法来评估边缘服务的总体可信度，并基于仿真实验验证了所提算法的性能和可用性。本文方案对设备层用户数据缺乏隐私保护，易带来安全隐患。下一步将针对交易过程中如何高效保护设备层隐私进行研究。

参考文献：

[1] SUN X, ANSARI N. EdgeIoT: mobile edge computing for the Internet of things[J]. IEEE Communications Magazine, 2016, 54(12): 22-29.

[2] SKALA K, DAVIDOVIĆ D, AFGAN E, et al. Scalable distributed computing hierarchy: cloud, fog and dew computing[J]. Open Journal of Cloud Computing, 2015, 2(1): 16-24.

[3] SONEKAR S V, KSHIRSAGAR M M, MALIK L. Cluster head selection and malicious node detection in wireless ad hoc networks[C]// Next-Generation Networks. Berlin: Springer, 2018: 547-554.

[4] YIM H J, SON Y H, LEE K C. A data distribution service quality of services policy configuration for data/events/services in the Internet of things[J]. Advanced Science Letters, 2016, 22(11): 3612-3617.

[5] 乐光学, 戴亚盛, 杨晓慧, 等. 边缘计算可信协同服务策略建模[J]. 计算机研究与发展, 2020, 57(5): 1080-1102.
YUE G X, DAI Y S, YANG X H, et al. Model of trusted cooperative service for edge computing[J]. Journal of Computer Research and Development, 2020, 57(5): 1080-1102.

[6] HASHEM E M, NI Q, SHI Q. Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(10): 7868-7881.

[7] CONOSCENTI M, VETRÒ A, DE MARTIN J C. Peer to peer for privacy and decentralization in the Internet of things[C]//Proceedings of 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). Piscataway: IEEE Press, 2017: 288-290.

[8] JIN B, JIANG D S, XIONG J B, et al. D2D data privacy protection mechanism based on reliability and homomorphic encryption[J]. IEEE Access, 2018, 6: 51140-51150.

[9] SCIANCALEPORE S, PIRO G, CALDAROLA D, et al. OAuth-IoT: an access control framework for the Internet of things based on open standards[C]//Proceedings of 2017 IEEE Symposium on Computers and Communications. Piscataway: IEEE Press, 2017: 676-681.

[10] GUAN Z T, SI G L, WU J, et al. Utility-privacy tradeoff based on random data obfuscation in Internet of energy[J]. IEEE Access, 2017, 5: 3250-3262.

[11] ZHENG W T, WANG Z Y, LV T T, et al. K-anonymity algorithm based on improved clustering[C]//Algorithms and Architectures for Parallel Processing. Berlin: Springer, 2018: 462-476.

[12] WANG Q, HUANG J, CHEN Y J, et al. PROST: privacy-preserving and truthful online double auction for spectrum allocation[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 374-386.

[13] WANG X, LUO T, LI J F. An efficient fully homomorphic encryption scheme for private information retrieval in the cloud[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2020, 34(4): 2055008.

[14] 张佳乐, 赵彦超, 陈兵, 等. 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.
ZHANG J L, ZHAO Y C, CHEN B, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21.

[15] HUANG X M, YU R, KANG J W, et al. Distributed reputation management for secure and efficient vehicular edge computing and networks[J]. IEEE Access, 2017, 5: 25408-25420.

[16] 邓宇乔, 杨波, 唐春明, 等. 基于密文策略的流程加密研究[J]. 计算机学报, 2019, 42(5): 1063-1075.
DENG Y Q, YANG B, TANG C M, et al. Research of ciphertext policy process-based encryption[J]. Chinese Journal of Computers, 2019, 42(5): 1063-1075.

[17] 霍星, 张阳洋, 景永俊, 等. MAS 环境中一种基于反馈可信度的多维信誉计算算法[J]. 软件学报, 2020, 31(2): 374-394.
HUO X, ZHANG Y Y, JING Y J, et al. Multidimensional reputation calculation method based on feedback reliability in MAS environment[J]. Journal of Software, 2020, 31(2): 374-394.

[18] 王田, 张广学, 蔡绍滨, 等. 传感云中的信任评价机制研究进展[J]. 通信学报, 2018, 39(6): 37-51.
WANG T, ZHANG G X, CAI S B, et al. Survey on trust evaluation mechanism in sensor-cloud[J]. Journal on Communications, 2018, 39(6): 37-51.

[19] NAGARAJAN R, THIRUNAVUKARASU R, SHANMUGAM S. A fuzzy-based intelligent cloud broker with MapReduce framework to evaluate the trust level of cloud services using customer feedback[J]. International Journal of Fuzzy Systems, 2018, 20(1): 339-347.

[20] SIADAT S, RAHMANI A M, NAVID H. Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model[J]. The Journal of Supercomputing, 2017, 73(6): 2682-2704.

[21] 邱磊, 蒋文贤, 李玉泽, 等. 基于边缘计算与信任值的可信数据收集算法[J]. 软件学报, 2019, 30(S1): 71-81.
QIU L, JIANG W X, LI Y Z, et al. Trustworthy data collection method based on edge computing and trust value[J]. Journal of Software, 2019, 30(S1): 71-81.

[22] LI X, LI J, YIU S, et al. Privacy-preserving edge-assisted image retrieval and classification in IoT[J]. Frontiers of Computer Science, 2019, 13(5): 1136-1147.

[23] HAN G J, HE Y, JIANG J F, et al. A synergetic trust model based on SVM in underwater acoustic sensor networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11239-11247.

[24] HUANG L T, DENG S G, LI Y, et al. A trust evaluation mechanism for collaboration of data-intensive services in cloud[J]. Applied Mathematics & Information Sciences, 2013, 7(1L): 121-129.

[25] WU Q T, ZHANG X L, ZHANG M C, et al. Reputation revision method for selecting cloud services based on prior knowledge and a market mechanism[J]. The Scientific World Journal, 2014, 2014: 1-9.

[26] AZIZ B, FREMANTLE P, WEI R, et al. A utility-based reputation model for the Internet of things[C]//ICT Systems Security and Privacy Protection. Berlin: Springer, 2016: 261-275.

[27] REDDY V B, NEGI A, VENKATARAMAN S, et al. A similarity based trust model to mitigate badmouthing attacks in Internet of things (IoT)[C]//Proceedings of 2019 IEEE 5th World Forum on Internet of Things. Piscataway: IEEE Press, 2019: 278-282.

[28] YUAN J, LI X Y. 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.

[29] TRUONG N B, LEE G M, UM T W, et al. Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of things[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(10): 2705-2719.

[作者简介]

张琳（1980− ），女，江苏丰县人，博士，南京邮电大学副教授、硕士生导师，主要研究方向为网络安全、可信计算、隐私保护等。

魏新艳（1993− ），女，江苏宿迁人，南京邮电大学硕士生，主要研究方向为网络安全、可信计算等。

刘茜萍（1981− ），女，四川攀枝花人，博士，南京邮电大学副教授、硕士生导师，主要研究方向为分布式计算、服务计算等。

黄海平（1981− ），女，福建三明人，博士，南京邮电大学教授、博士生导师，主要研究方向为物联网、网络安全、隐私保护等。

王汝传（1943− ），男，安徽合肥人，南京邮电大学教授、博士生导师，主要研究方向为计算机软件、计算机网络和网格、信息安全、无线传感器网络等。