计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240600153

基于边缘计算的区块链网络节点信任评估方法

赵婵婵　尉晓敏　石　宝　吕　飞　刘利彬　张子阳
内蒙古工业大学信息工程学院　呼和浩特 010080
(cczhao@imut.edu.cn)

摘　要　针对现阶段在边缘计算中出现的恶意设备或者提供恶意数据的问题,提出了一种基于边缘计算的区块链网络节点信任评估方法。首先,采用区块链技术以及搭建云边端框架的方法,建立边缘设备之间的信任关系;其次,在整体的信任评估方法中添加了基于信任的共识机制,并且引入时间敏感函数,根据不同场景对信任值要求的时效性来确定;最后,在计算信任值时,为了避免主观因素造成的偏差,提出了增加稳定系数的方法,来保障信任值的可靠性。经过仿真实验验证,所提出的信任评估方法在不同恶意节点比例下,节点的交互成功率要优于其他传统的信任评估方法,当恶意节点在20%时,所提方法与其他方法相差不大,而当恶意节点的比例达到40%时,交互成功率为0.82,当恶意节点所占比例高达60%时,所提方法交互成功率也达到了0.68%;随着时间的进行,正常节点和恶意节点的信任值变化呈相反趋势,正常节点的信任值在最终达到0.9,而恶意节点的信任值降低至0.2;为了更好地观察信任值节点的信任值变化情况,设置了恶意节点执行恶意行为的概率为50%,结果同样也表明所提信任评估方法在面对恶意节点时可以有效地做出反馈;最后,比较了在不同节点情况下的时间消耗,结果表明所提方法在处理节点数量越大时,时间消耗越低于传统的信任评估方法。因此,所提方法在面对大量的恶意节点时,可以做出有效的信任评估,这一方法旨在确立如何选择可信节点作为数据存储传输的目标节点,并计算边缘节点的信任值,减少恶意节点带来的影响。

关键词:边缘计算;区块链;信任评估;身份验证
中图分类号　TP393

Edge Computing Based Approach for Node Trust Evaluation in Blockchain Networks

ZHAO Chanchan,WEI Xiaomin,SHI Bao,LYU Fei,LIU Libin and ZHANG Ziyang
School of Information Engineering,Inner Mongolia University of Technology,Hohhot 010080,China

Abstract　To solve the problem of malicious devices or malicious data in edge computing,this paper proposes a method of node trust evaluation based on edge computing. Firstly,the blockchain technology and the method of building a cloud-edge framework are used to establish the trust relationship between edge devices. Secondly,a trust-based consensus mechanism is added to the overall trust evaluation method,and a time-sensitive function is introduced to determine the timeliness of trust value requirements in different scenarios. Finally,in order to avoid deviations caused by subjective factors in calculating the trust value,a method of adding stability coefficients is proposed to ensure the reliability of the trust value. Simulation experiments validate that the proposed trust evaluation method has a higher success rate of node interaction than other traditional trust evaluation methods at different malicious node ratios. When the malicious node ratio is 20%,the proposed method is similar to other methods,while when the malicious node ratio is 40%,the success rate is 0.82,and when the malicious node ratio is 60%,the success rate is 0.68%. As the normal nodes and malicious nodes' trust values change over time,they follow opposite trends. The trust value of normal nodes reaches 0.9 in the end,while the trust value of malicious nodes decreases to 0.2. To better observe the change of trust values of nodes,this paper sets the probability of malicious nodes performing malicious behaviors at 50%. The results also show that the proposed trust evaluation method can effectively respond to malicious nodes. Finally,the time consumption is compared in different node conditions,and the results show that the proposed method has lesser time consumption than traditional trust evaluation methods when dealing with a larger number of nodes. Therefore,the proposed method can make effective trust evaluations when facing a large number of malicious nodes. This method aims to determine how to select trusted nodes as target nodes for data storage and transmission,calculate the trust value of edge nodes,and reduce the impact of malicious nodes.

Keywords　Edge computing,Blockchain,Trust evaluation,Identity authentication

基金项目:内蒙古自治区自然科学基金项目(2023LHMS06016);内蒙古自治区直属高校基本科研业务费项目(JY20240010,JY20230082)
This work was supported by the Natural Science Foundation of Inner Mongolia Autonomous Region(2023LHMS06016) and Basic Scientific Research Business Fee Project of Universities Directly under the Inner Mongolia Autonomous Region(JY20240010,JY20230082).
通信作者:石宝(kshibao@163.com)

1 引言

边缘计算是一种新兴的计算模式，是近年来为了迎接新的计算需求而发展起来的。2016 年，韦恩州立大学的 Shi 等[1]率先提出了边缘计算的定义：边缘计算是一种新型的计算模型，主要在网络的边缘侧执行，包含了云服务和万物互联服务。现阶段的 5G 技术与物联网技术都已进入了飞速发展的时期，传统意义上的云计算在处理数以万计的数据时，已经无法满足现阶段的计算需求，所以边缘计算在此条件下被广泛应用。与此同时，在边缘网络中部署着大量的物联网设备，这些设备是被用来收集用户数据的，并且边缘网络拥有非常高的开放性，边缘设备拥有非常高的动态性，这些特点很可能会导致边缘设备遭受攻击或者滥用[2]。

由于 MEC 网络的分布性和异构性，边缘节点容易受到恶意设备的攻击。因此，MEC 的任务执行可能是不可信任的，存储在边缘节点上的用户数据面临泄露和伪造的风险[3]。同时，由于边缘网络环境复杂，当这些恶意设备加入网络时，辨别难度非常大。那么，在这个过程中便会产生非常严峻的信任问题。在数据收集和传输过程中，存在一些恶意设备可能会通过各种恶意手段干扰正常的操作，包括发布虚假信息，传播有害内容或导致数据部分丢失等。因此，挑选出可靠的节点非常关键。在通常情况下，信任评估体系是通过收集并分析节点的历史行为来反馈信息的，并运用数学方法预测该节点的未来行为。然而，在现实应用中，这些恶意设备可能通过提交虚假的反馈信息来误导云控制中心，使其做出错误的判断。因此，在边缘网络中确定边缘设备之间的信任关系，是提高网络服务可靠性和保护用户数据安全性的关键措施[4]。

为了解决上述问题，本文提出搭建云边端框架与区块链相结合的信任评估方法。边缘计算在计算、存储和网络层面的分布式特性，与区块链的去中心化特点相匹配，二者都是通过网络中的多个节点共同参与工作，并且每个节点都保存有一份数据记录，增加了系统的不可篡改性与透明性，提高了数据采集的可信度。因此，在探讨区块链与边缘计算融合的优势时，二者的优势显而易见。

2 相关工作

现阶段，国内外学者将边缘计算中的信任问题分为信任管理和信任评估两大类。本文将对信任评估的一系列方法进行研究。信任是边缘计算中一个非常复杂的概念，它会受到各种主客观的影响。在边缘计算这种计算复杂、动态变化的网络环境中，各个节点之间的信任很难保证，在此之间建立信任和维护是非常困难的。因此在对边缘网络中的节点进行信任评估时[5]，不但可以检测到异常节点，还可以帮助边缘网络进行合理的任务分配和资源调度，只有确保在边缘网络中各个节点的身份相互信任，才可以更好地构建可信网络，保障边缘计算的安全，为边缘智能提供更加安全的服务[6-8]。根据不同的网络架构，信任评估机制可以分为集中式和分布式两种[9]。随着边缘计算的普及，分布式系统架构的应用场景也越来越多。

在信任评估中，根据应用场景的不同，有很多评估方案，例如有集群化协同的信任评估、多层协同的信任评估、基于传统数理统计的信任评估和基于人工智能的信任评估等等。

文献[10]提出了一种全面信任的概念，并且将直接信任和间接信任等因素在物联网不同协作的不同阶段进行整合和利用，与现有的评估机制相比，加快了选择信任目标的速度，在降低时延的同时提供了更高的服务质量。文献[11]提出了互信区块链的概念，通过加入信任评估机制，有效地规避了对传统工作量证明(Proof of Work，POW)机制的依赖。该方法以 PBFT(Practical Byzantine Fault Tolerance)算法为基础，通过信任投票的方式实现了节点间的共识机制，不仅提升了系统的运行效率，并且充分展现了物联网在节点间协调与协作方面的卓越能力。文献[12]提出了一种 NTSC(Novel Trust-based Service Computing)框架，主要包括两种方案。第一种为信任评估方案，利用边缘计算中的可信静态传感器设备计算数据提供者的可信度，用时间和质量的综合因素计算可信度。第二种为基于信任的服务评估方案，为了提升评估精确度，通过用户的可信度计算服务评估。此方案的不足之处是，尽管通过边缘计算评估边缘设备的可信度，但是庞大的设备数量依然会给云服务器带来沉重的计算和存储压力。文献[13]提出了一种主动且可验证的信任评估(Active and Verifiable Trust Evaluation，AVTE)方法。该方案利用主动发起的可信检测路由的方法来获得设备信任。AVTE 方法的信任获取是基于可验证的方法，提高了数据收集率，使信任度具有更高的可靠性，使信任评估更加快速准确，有助于提高网络性能。文献[14]提出了使用联邦学习，并且融合数据在以往共识过程中的经历进行信任评估的方案。该方案将评估结果存储在区块链的公共账本中，解决了数据融合和模型融合中的信任问题。不足之处是，该方案没有分析信任权重的分配问题，导致信任值的准确度降低。文献[15]提出了一种基于传统数理统计的信任评估方法，该方法运用了一种主观逻辑策略，针对移动边缘节点中的传感器节点，精确计算节点的信任值。通过设定一个动态窗口，在评估边缘服务器声誉时保持时效性。为了更接近实际情况，还引入了基于时间因素的权重机制，这一机制可以捕捉到边缘节点声誉值在不同时间点的动态变化，为信任评估提供更为全面和准确的视角。文献[16]提出一种基于人工智能的信任评估方法，将信任的预测模型转化为一个网络套索问题，同时融入了随机交替乘法的概念。该策略在移动边缘场景下非常有效，可以精准提炼出最为显著的信任特征，适应各种多变的移动边缘计算(Mobile Edge Computing，MEC)环境中的信任需求。该方法的核心是对边缘信任数据的聚合分析，让信任评估更准确、高效。

在边缘计算这种分布式网络架构中，所有的节点都应该加入网络，进行数据交互，这样的行为在很大程度上避免了数据孤岛的问题。因此，很多研究人员使用身份验证的方法与信任评估模型进行结合，以此来提高信任评估的准确度。文献[17]提出了一种基于区块链的远程相互认证(B-RMA)的方法，该方法考虑了智能设备和云网络来提供安全和隐私。文献中提出的 B-RMA 方法可以与基于物联网的智能环境共存，以分散用户认证请求的处理，并且可以使用非正式安全分析评估所提策略的重要性，该方法是轻量级的并且能够显著缩短认证的等待时间。文献[18]提出了一种基于区块链和域信任度的物联网跨域信任关系评估模型(TD-BCCD)，该文献

通过多维度对节点的信任值进行评估,让不同域之间的节点通过域信任度进行数据交互,有效解决了数据交互单一与跨域交互的信任安全问题。文献[19]提出了一种分布式边缘协作群认证方法和两种在边缘设备端本地生成令牌进行相互认证的策略,分别为随机令牌生成和隐私保护令牌生成。每个令牌通过重复学习过程来同时认证同一组中的其他设备。如果该过程收敛到预期结果,则所有设备将同时作为合法组成员进行身份验证。该文献简化了身份认证的过程,实现了较短的时间延迟和较低的计算、存储成本。分布式协作与边缘计算相结合的方式,为边缘设备间的安全通信提供了一种高效的解决方案。

针对以上问题,本文所采用的边缘计算与区块链技术相结合的方式,可以更好地解决信任评估的问题。区块链由分布式存储技术、密码学、共识算法和智能合约这 4 种核心技术组成;并且区块链所具有的去中心化的特点,与边缘计算在很大程度上契合。二者都是不依赖云控制中心,而是通过网络中的多个节点共同参与工作,并且每个参与的节点都保存有一份数据记录,增加了系统的不可篡改性与透明性,提高了数据采集的可信度。

3 云边端框架与区块链技术相结合的信任评估方法

3.1 云边端框架与区块链的模型结构设计

边缘计算为区块链提供必要的计算资源和存储能力。特别是在多节点共存的环境下,边缘计算有效突破了高速传输的瓶颈,满足了区块链平台在边缘侧的实际应用需求。与此同时,区块链技术为边缘计算网络服务搭建了一个更加安全、更加可信的环境,为数据传输提供了更为周全的保障方法。它确保了多个边缘设备之间数据的安全流转与共享,实现了资源的高效协同管理,保障了数据存储的完整性与真实性,构建了一个值得信任的边缘网络生态环境。

为了更好地对边缘网络中的节点进行信任评估,本文引入了区块链技术,并且搭建云边端框架与区块链相结合的模型结构。该结构分为 3 层,分别为云层、边缘层和终端层,如图 1 所示。

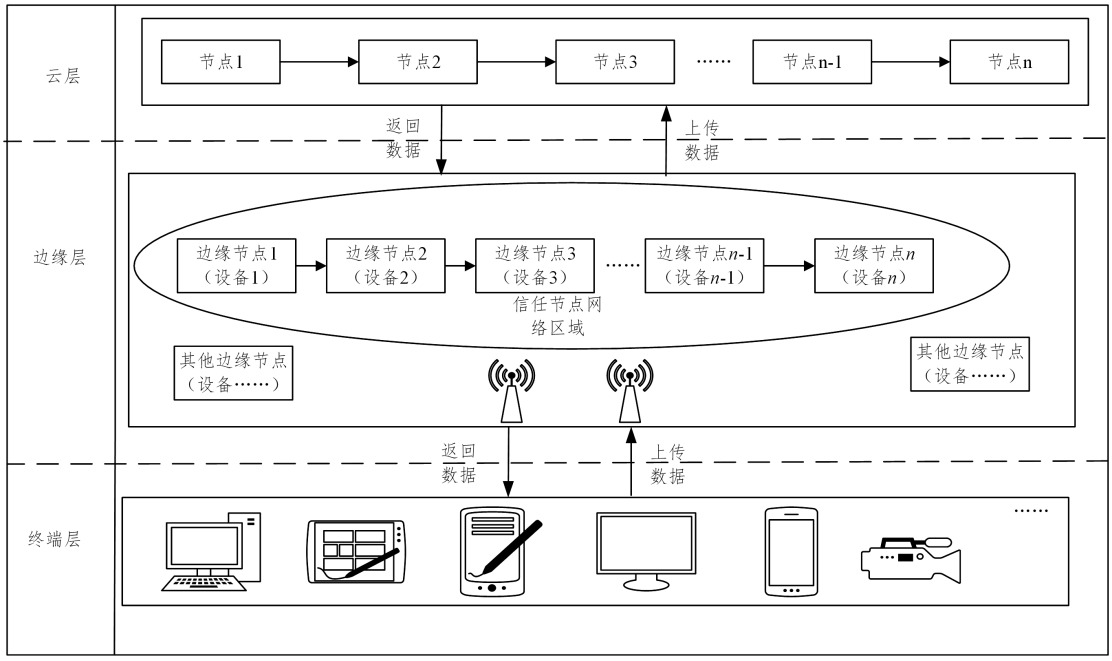

图 1 云边端结合区块链的结构图

Fig. 1 Structure diagram of cloud-edge combined with blockchain

1)云层中的区块链节点通过自身强大的计算能力来处理其中的复杂计算。随后将数据下放到边缘层,利用边缘计算提升响应速度。

2)边缘层中的边缘节点分为两类,一类是值得信任的节点所构成的区块链网络,另一类是还未通过验证而没有加入区块链的节点。区块链中的节点对数据进行处理分析之后上传到云层。

3)终端层负责收集数据并上传到边缘层。

3.2 信任区块结构

对节点进行信任评估,关键在于对信任值的计算中。本文在进行信任值计算之后,将所得到的信任值存储在信任区块中。信任区块采用默克尔树(Merkle Tree)结构。它是一种典型的二叉树结构,是由一个根节点、一组中间节点和叶子节点组成。存储信任值的区块结构如图 2 所示。区块结构主要是由两部分组成,分别是区块头和区块体。

区块头本身是存储版本号、时间戳、前一区块的哈希值、当前区块的哈希值和默克尔根等内容。此外,本文还将可信节点名单、恶意节点名单一并存储到区块头当中。可信节点名单和恶意节点名单中包括该节点的 ID、地址、端口号和信任值等信息。

区块体中存储上一个区块到这一区块所产生的信息内容,例如节点发送真实消息、虚假消息的记录。在更新信任值时,根据区块体中存储的记录来调整信任值的变化。同时,也可以发现,如果有人想要篡改区块中的内容,那么默克尔根的值也一定会发生变化,这也是本文使用区块链的一个原因——正是由于它具有不可篡改性,可以更好地保障数据安全,使信任值的变化更加具有真实性。信任区块结构如图 2 所示。

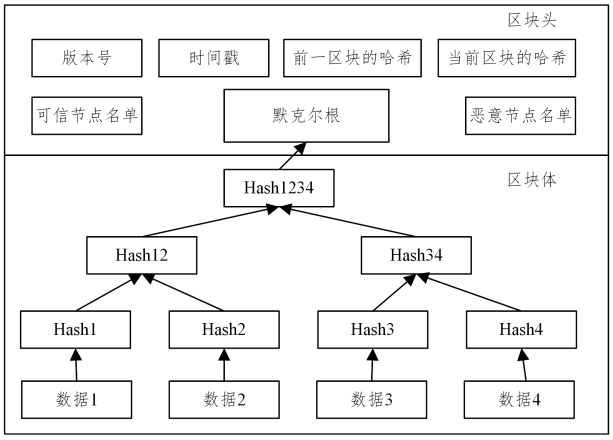

图 2 信任区块结构图

Fig. 2 Trust block structure diagram

3.3 椭圆曲线数字签名算法

当节点首次进入网络当中时，对节点的身份进行验证，本文采用椭圆曲线数字签名算法(Elliptic Curve Digital Signature，ECDSA)进行验证。假设有 A，B 两个节点，A 对 B 进行身份验证的验证过程如下。

1)在密钥生成阶段，证明者 B 在 1 到 n 的范围内随机选择私钥 d，之后通过以式(1)来计算公钥 Q。

$$Q=d*g \tag{1}$$

其中，d 为私钥，g 为椭圆曲线子群的生成器(基点)。

2)在签名生成阶段，证明者使用 SHA256 哈希函数计算要签名的消息 m 的哈希值 h。

$$h=H(m) \tag{2}$$

3)证明者从 1 到 $n-1$ 中选择一个随机数 k，之后使用其所选择的随机数来定位椭圆曲线上的随机点 R，并且记录此点的 x 坐标。r 为椭圆曲线点的 x 坐标：

$$R=k*g \tag{3}$$

$$r=R.x \tag{4}$$

4)签名证明使用式(5)计算，s 为签名证明。

$$s=k^{-1}*(h+r*d)(\mathrm{mod}\ n) \tag{5}$$

其中，k 为随机数，h 为哈希值。

5)位于 r 的随机点与签名证明 s 形成签名(r,s)，签名与消息 m 相连接并且转发给验证者 A。如果 r 和 s 其中一个为 0，则需要从第 3)步重新开始执行。

6)验证者 A 在收到消息 m 和签名值(r,s)后，进行如下计算：

$$s_1=s^{-1}(\mathrm{mod}\ n) \tag{6}$$

其中，s_1 为 s 的模逆。

7)曲线上的随机点 R'的位置采用式(7)计算。

$$R'=(h*s_1)*g+(r*s_1)*Q \tag{7}$$

8)最后通过计算 r'来判断 r'是否与 r 相等，若相等，则身份验证通过。

$$r'=R'.x \tag{8}$$

其中，r'是此点的 x 坐标。

在身份验证通过之后，生成密钥并广播至全网，之后查验对方的时间戳。若通过，则开始计算评价节点对于被评价节点的信任值。

3.4 信任值计算

信任值的计算分为 3 个部分：直接信任值、间接信任值和综合信任值。与此同时，在这些信任关系中存在信任、不信任和不确定 3 种情况，分别用 α，β，γ 来表示，我们根据情况设定 $\alpha+\beta+\gamma=1$。

在计算过程中，本文加入了时间敏感函数，如式(9)所示。

$$T(t)=T_0*e^{(-\varphi*t)} \tag{9}$$

其中，$T(t)$表示在时间 t 时的综合信任值；T_0 表示初始的综合信任值；φ 表示衰减参数，衰减参数根据实际问题的应用场景确定。

3.4.1 直接信任值

直接信任值基于历史交互记录计算，且随着时间的逐渐增加而衰减。假设节点 A，B 的历史交互成功次数与失败次数分别为 a 和 b，直接信任用 D 来表示，节点 A 对于节点 B 的信任值表示为DT_{ab}，该值服从 β 分布，因此有$D_{ab}\sim\beta(a+1,b+1)$，由此可得节点 A 对于节点 B 的直接信任值为：

$$D_{ab}=E(\beta(a+1,b+1))=\frac{a+1}{a+b+2} \tag{10}$$

3.4.2 间接信任值

当直接信任不足以完整地表达彼此之间的信任关系时，需要采用间接信任的计算方式。在间接信任值的计算中，节点采用特殊的计算方法。首先要找到被评价节点的邻居节点，对该节点进行直接信任评估，之后再去获取邻居节点对于被评价节点的直接信任值，所得到的信任值可以作为间接信任值。假设有 A，B 两个节点，A 为评价节点，B 为被评价节点，根据式(11)计算间接信任值 IT_{AB}。

$$IT_{AB}=\frac{\sum_{k=0}^{n}T_{kB}*W_k}{\sum_{k=0}^{n}T_{Ak}} \tag{11}$$

其中，T_{kB}表示邻居节点 k 对于被评价节点 B 的直接信任值，W_k表示邻居节点的直接信任值，n 为合适的邻居节点的数量，T_{Ak}表示 A 对邻居节点 k 的直接信任值，$W_k\neq T_{Ak}$。

3.4.3 综合信任值

综合信任值 $Trust$ 按式(12)进行计算。

$$Trust=D*\phi+I*\theta \tag{12}$$

其中，D 代表直接信任值，I 代表间接信任值，ϕ 代表直接信任值在综合信任值中所占的权重，θ 代表间接信任在综合信任值中所占的权重，且 $\phi+\theta=1$。ϕ 和 θ 的取值需要根据实际过程中的情况进行判断设定，在不同的应用场景下，对于信任值的需求有所不同，因此所占的权重也不相同。在传统的比较稳定的静态权重设置的算法中，主要是根据经验来决定的。除此之外，还可以固定设置为 0.5。

由于信任具有主观性，不同的评价者会根据自己的判断对于其他相同的被评价者有不同的主观想法，这也就导致了所计算的直接信任值和间接信任值在最后的综合信任值中的占比各不相同。本文根据评价者有不同的参考标准这一情况，提出了增添稳定系数这一方法。

首先设置稳定系数 $S=\frac{\eta}{\varepsilon}$，$\eta$ 为信任值的标准差，ε 为信任值的平均数。S 的值越大，表示信任值的差距越大，即稳定性越差；反之稳定性越好。由此可得出 ϕ 和 θ 的权重计算公式如下所示：

$$\phi=\frac{S_I}{S_D+S_I} \tag{13}$$

$$\theta=\frac{S_D}{S_D+S_I} \tag{14}$$

其中，S_D 和 S_I 分别表示直接信任值和间接信任值的稳定系数。

根据上述公式可得出：当直接信任值的稳定性较差时，间接信任值所占的权重较大，即评价节点更倾向于其他节点对于被评价节点的判断；当间接信任值稳定性较差时，直接信任值所占的权重较大，即评价节点更倾向于自己的主观判断。

3.5 基于信任的共识机制

除此之外，本文在计算信任值时还增添了基于信任的共识机制（Proof of Trust，PoT）。该机制是以信任值为基础的。

1）首先，在评估双方完成身份验证之后，评价者对被评价者进行信任评估，并将评估后的结果广播到全网。

2）网络中的其他节点会把此消息存储到自己的区块中，之后将自己所收集到的信息按照信任值的高低进行排序，得出信任值最高的节点。

3）该节点会将所有的评估信息进行打包，在打包成自己的区块之后，用自己的私钥广播到全网。

4）其他所有的节点使用公钥对此消息进行验证。

5）验证通过之后，才可以将此区块记录到区块链当中。

基于信任的共识机制流程图如图 3 所示。

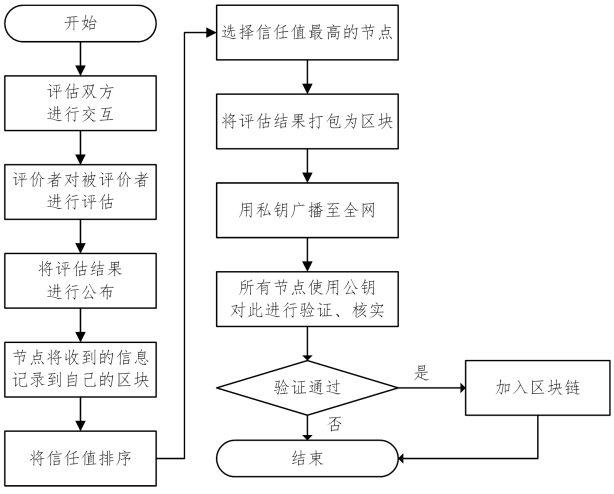

图 3 基于信任的共识机制

Fig. 3 Trust-based consensus mechanism

在基于信任的共识机制中，本文加入了信任值的衰退和恢复方法。尤其在面对物联网中庞大的节点数量时，该方法可以有效对节点的信任值的变化做出应对。信任衰退指的是在一段时间中，节点由于参与一些恶意事件，而做出了一些恶意行为。具体表现行为如下：

1）负面事件：当节点在网络中有不当行为或者传播虚假消息时，其他节点对该节点的信任程度会下降。

2）信息丢失：当节点在进行信息传播时，丢失部分信息或者隐瞒部分信息时，其他节点对该节点的信任程度会下降。

3）长时间不活跃：该节点在一段时间内不参与网络中信息的共享、传播时，会被判定为消极节点，这也会导致其他节点对该节点的信任程度下降。

针对以上情况，设定了以下恢复信任值的方法。

1）信任建立：节点通过持续的良好表现，完成任务，提供准确的数据信息，以此方式来重新建立信任关系。

2）信息共享：该节点主动参与网络中的信息共享行为，在传播信息时做到全面、正确。衡量传播信息的全面性取决于该节点传播的信息是否到达了所有相关的节点，确保信息的覆盖范围；而正确性需要对比该节点传播信息的实际情况和验证其消息来源是否可靠。可以通过区块链网络节点中记录的数据信息进行判断。

3）参与活动：该节点主动参与网络中的互动，做好信息收集和记录工作，逐步成为活跃节点。

信任衰退和恢复是信任共识机制过程中的重要一环，影响着网络中节点的互动和在计算信任值中直接信任和间接信任的稳定性。综上所述，可得出整体的信任评估流程如图 4 所示。

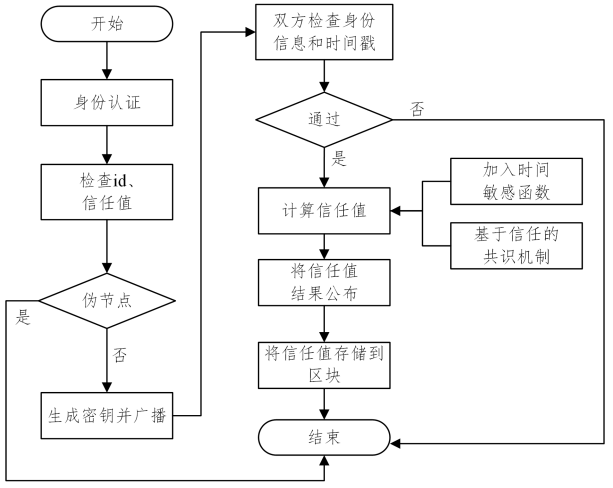

图 4 信任评估流程图

Fig. 4 Flowchart of trust assessment

除此之外，本文还增添了信任值查询的方法。在双方节点交互之前，评价节点可以主动去查询被评价节点的信任值，并根据所查到的综合信任值信息判断是否进行交互。查询方法如图 5 所示。

1）假设有 A，B 两个节点，A 为请求交互节点，B 为被请求节点，节点 A 请求与 B 交互，即与 B 建立信任关系，访问 B 的信息。

2）B 在同意交互请求前可先查询信任值，先查看自己所存储的信任值信息，看之前是否有交互记录。

3）若有，则将相应的综合信任值返回给节点 B；若没有，则查询与自己交互的邻居节点对于节点 A 的直接信任值记录，以此来获得间接信任值。

4）根据所查到的综合信任值信息，判断是否与节点 A 进行交互。

若同意与 A 进行交互，则计算综合信任值，并且建立新的信任关系。

在该方法中，邻居节点的选取无疑是非常重要的。若邻居节点选择得太多，将意味着需要处理更多的数据和进行更多的计算，会导致计算开销的增加；同时会导致信息的冗余，增加系统的复杂性，可能会需要额外的机制对数据进行过滤筛选。而邻居节点太少，会导致信息覆盖不足，影响间接信任的准确性和可靠性，进而导致信任评估不准确，无法反映节点的信任情况；容易受到单个节点的影响，导致鲁棒性较差。因此，本文在选择邻居节点时采用节点的度中心性方法，对于某个节点，其度越高，代表着该节点在网络中连接的节点数量越多，选择度较高的邻居节点可以确保信息覆盖的全面性。在数据分布较为密集的情况下，选择较少的邻居节点就可以提供准确的信息；在数据分布稀疏的情况下，需要选择更多的邻

居节点。因此，根据实际应用场景的不同与数据分布的情况，具体制定选择的策略。

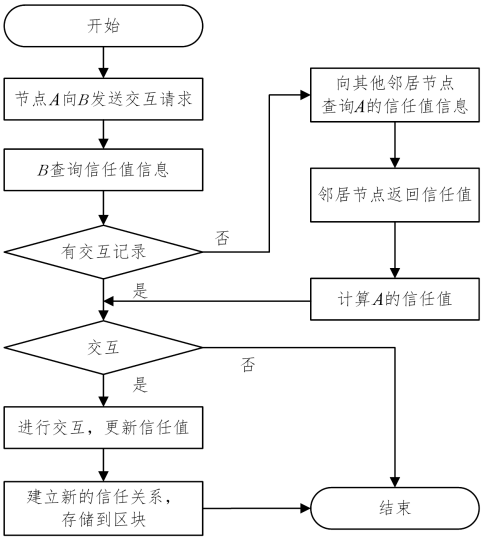

图 5 信任值查询方法流程图

Fig. 5 Flowchart of trust query method

4 仿真结果与分析

4.1 仿真环境

为了进一步验证文中所提信任评估方法，选用 C++作为主要的编程语言，采用 NS-3(Network Simulator version 3)仿真工具来进行实验。NS-3 是用于互联网系统的离散事件网络模拟器，并且提供 C++编程接口。详细的实验设置如表 1 所列。

表 1 实验环境设置

Table 1 Experimental environment settings

软/硬件	版本/规格
处理器	Intel © CoreTMi7-10700，2.90 GHz
内存	4 GB
仿真平台	NS-3 v3.41
编程语言	C++
操作系统	Ubuntu 22.04

为了让实验环境更加接近真实的边缘计算中的环境，利用 NS-3 中的随机路径点模型(Random Waypoint Mobility Model)，随机生成 1 000 个移动的节点，并将所有节点部署到一个规模大小为 1 km×1 km 的区域当中。本文所设置的恶意节点比例为 10%～60%，若在网络中绝大部分都是恶意节点，那么可以判断这是一个不可信的网络空间，在此探讨信任评估也就没有了意义。详细的仿真实验设置如表 2 所列。

表 2 仿真参数设置

Table 2 Simulation parameters setting

实验参数	取值范围
仿真区域	1 km×1 km
仿真时间/min	60
节点数量	100～1 000
恶意节点比例	10%～60%
初始信任值	0.7
信任阈值	0.5

4.2 安全性分析

在信任评估方法中，不仅要准确地对节点行为进行信任评估，还要保障评估的安全性。本文提出的信任评估方法采用云边端框架与区块链相结合的方法，因为区块链具有去中心化、不可篡改的特性，区块链网络中的数据不单一集中在中央服务器上，而是分布在多个节点当中，节点中的数据一旦被写入区块链中，将会难以更改和删除。该特性保障了数据的安全性和完整性。其次，在进行身份验证时采用了椭圆曲线数字签名算法，该算法的安全性基于椭圆曲线离散对数问题(ECDLP)的计算困难性。解决 ECDLP 需要对椭圆曲线上的大整数进行指数级计算，这在现有计算技术下非常困难，签名信息又不可伪造，因此，将二者结合能为信任评估提供充分的安全保障。

4.3 交互成功率验证

文中首先进行的是在不同恶意节点的占比下，节点交互成功率的实验。跟据仿真实验的设置，1 000 个随机节点在固定区域范围内进行交互，通过 3.2 节中的方法，在进行信任值计算之前，验证节点的身份信息，判断是否交互。图 6 给出了节点的交互过程。

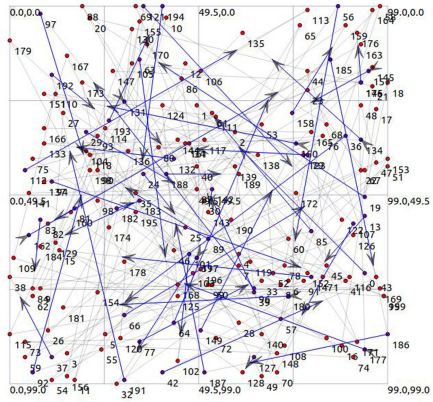

图 6 节点交互过程

Fig. 6 Node interaction procedure

实验结果如图 7 所示。可以看出，当该网络中没有恶意节点时，所有节点都会成功进行交互，在不使用任何信任评估方法的条件下，当恶意节点的比例达到 20%及以上时，节点的交互成功率出现了明显的下降；对比其他的信任评估方法和本文所提出的方法，可以非常直观地看到在恶意节点占比为 10%时，其余的方法效果都要比 Peer Trust 好；当恶意节点占比达 30%及以上时，本文所提出的方法效果要明显优于其他的方法。因此，可确定文中所设计的信任评估方法可以有效辨别恶意节点，减少与恶意节点交互的情况，降低恶意节点所带来的风险。

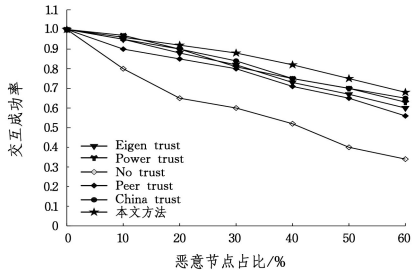

图 7 交互成功率对比

Fig. 7 Comparison of success rates in interactions

4.4 信任评估效果验证

为了验证信任评估的效果，本文设置一轮的仿真时间为

60 min，在这一个仿真周期内来观察在不同信任评估方法下信任值的变化情况。由 4.2 节中的实验结果可知，当恶意节点的比例达到 20%时，节点交互的成功率开始出现较明显的变化，因此，在这一部分中将会对比在一个仿真周期内，恶意节点和正常节点的信任值的变化情况。实验结果如图 8 所示，在初始信任值为 0.7 的情况下，随着仿真时间的增加，正常节点的信任值在逐步平缓地上升，而恶意节点的信任值在第 10 min 时下降幅度较大，在之后的时间内依然保持下降，在第 30 min 降低到信任阈值之下。

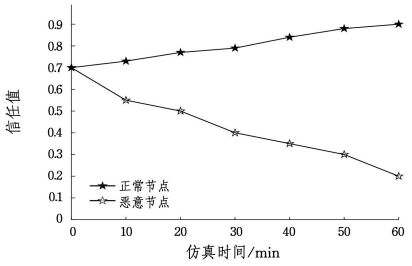

图 8　信任值变化情况 1

Fig. 8　Trust value change case 1

为了更加直观地看出本文所提出的信任评估方法的有效性，在本实验的基础上，再设置一组实验。设置恶意节点执行恶意行为的概率为 50%，这表明恶意节点同样也会像正常节点一样发送真实信息。实验结果如图 9 所示。

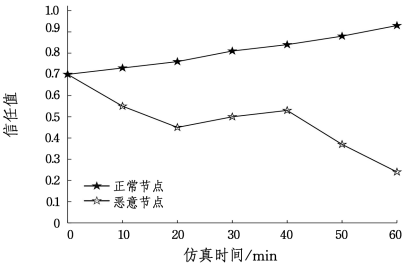

图 9　信任值变化情况 2

Fig. 9　Trust value change case 2

从图 9 中可以明显地观察到恶意节点的信任值在 20 min 后由降转升，这是因为在恶意节点执行完恶意行为之后，它与正常节点一样发送了真实的信息，因此它的信任值开始上升；而在 40 min 后由上升突然转为下降，且下降后的信任值比 20 min 之前的信任值还要低，这是因为本文所提出的信任评估方法在计算信任值时，由于恶意节点执行了恶意行为，且在之后与正常节点一样，此行为具有迷惑性，有可能会误导其他节点，因此信任值上升幅度较小，只有连续执行正常节点的行为，信任值才可以继续恢复，而当恶意节点的行为在恶意与正常两种情况下反复进行时，信任值上升的幅度会越来愈小，而下降的幅度会越来越大。因此，本文所提出的方法通过信任值的变化情况可以有效识别恶意节点。

4.5　时间消耗验证

信任评估方法的时间消耗是在计算信任值这一部分当中，传统的信任评估方法在计算信任值时较为单一，本文所提出的云边端框架和区块链相结合的方式来进行信任评估，利用边缘计算的优势，在计算方面更加快速准确，且将计算压力分配到边缘端，以此来缓解传统方法中来自控制中心的计算压力。由于时间消耗受到恶意节点比例不同以及其他客观因素的影响，本组实验将重复进行 10 次，并且设定恶意节点的占比为 30%，取 10 次实验结果的平均数，以此来计算节点数量由 100 增加至 1000 时，传统评估方法与本文所提出的方法所花费的时间。实验结果如图 10 所示。

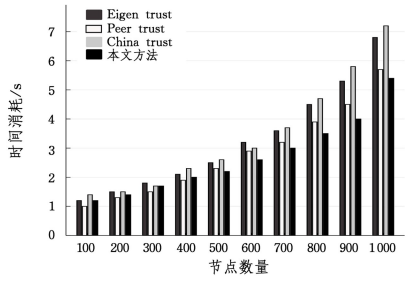

图 10　不同数量节点情况下的时间消耗对比

Fig. 10　Comparison of time consumption with different number of nodes

从图 10 中可以看出，在节点数量较少时，传统的信任评估方法与本文所提出的方法在时间花销上没有明显的差距；节点数量达到 500 及以上时，本文所提方法的时间花销时明显低于传统的信任评估方法。这正是因为边缘计算的优势，在处理节点数量逐渐增多时，其花费的时间要优于其他传统评估方法。

结束语　针对传统信任评估方法中出现的问题，本文主要完成了以下工作内容：搭建云边端框架并且与区块链技术相结合，使二者的优势得到充分的发挥；在计算信任值的过程中加入了时间敏感函数，并且根据不同的应用场景，确定不同的衰减因子，使得出的信任值更加具有时效性；在计算过程中，为了避免主观因素所带来的影响，提出了增添稳定系数这一方法，根据不同场景对于直接信任和间接信任所占权重的不同，来计算信任值，有效避免了主观因素所带来的结果偏差；同时，加入基于信任的共识机制和信任值衰退和恢复的方法，使文中所提出的信任评估方法更加有效。

为了对信任评估方法进行更深入的研究，下一步将对不同类型的恶意节点的恶意行为提出针对性的评估方法，提高辨别恶意节点的能力，同时在进行信任评估时设计评估方法来更好地减少时间消耗。在面对复杂的网络环境时，通过制定更加有效的信任评估方法，适应不同环境的实际需求。

参 考 文 献

[1] SHI W S, CAO J, ZHANG Q, et al. Edge Computing: Vision and Challenges [J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[2] TANG X Y, CAO C, WANG Y X, et al. Computing power network: The architecture of convergence of computing and networking towards 6G requirement [J]. China Communications, 2021, 18(2): 175-185.

[3] YANG W, SHI L, LIANG H, et al. Blockchian Empowered Reliable Computation Offloading and Resource Allocation for Mobile Edge Computing Networks [C]// 2023 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2023.

[4] ALWARAFY A, AL-THELAYA K A, ABDALLAHM, et al. A Survey on Security and Privacy Issues inEdge-Computing-Assisted Internet of Things [J]. IEEE Internet of Things Journal, 2021, 8(6): 4004-4022.

[5] NIKRAVAN M, HAGHI K. A review on trust management in fog/edge computing: Techniques, trends, and challenges [J]. Journal of Network and Computer Applications, 2022, 204: 103402.

[6] ZHENG W Y, CHEN B, HE D B. An adaptive access control scheme based on trust degrees for edge computing[J]. Computer Standards&Interfaces, 2022, 82: 103640.

[7] ZHANG L J, ZOU Y F, WANG W Z, et al. Resource allocation and trust computing for blockchain-enabled edge computing system[J]. Computers & Security, 2021, 105: 102249.

[8] KONG W P, LI X Y, HOU L Y, et al. A Reliable and Efficient Task Offloading Strategy Based on Multifeedback Trust Mechanism for IoT Edge Computing[J]. IEEE Internet of Things Journal, 2022, 9: 13927-13941.

[9] WEN M, WANG T, ZHANG S B, et al. An active and verifiable trust evaluation approach for edge computing[J]. Journal of Cloud Computing, 2020, 9(1): 1-19.

[10] CHEN J Z, WANG X B, SHEN X M. RTE: Rapid and Reliable-Trust Evaluation for Collaborator Selection and Time-Sensitive Task Handling in Internet of Vehicles [J]. IEEE Internet of Things Journal, 2024, 11(7): 12278-12291.

[11] JAYAKUMAR D, SANTHOSH KUMAR K. Design of mutual trust between the IoT nodes using adaptive network-based fuzzy inference system in edge computing systems [J]. Materials Today: Proceedings, 2022, 56: 1795-1801.

[12] LI T, HUANG G S, ZHANG S B, et al. NTSC: a novel trust-based service computing scheme in social internet of things [J]. Peer-to-Peer Networking and Applications, 2021, 14(6): 3431-3451.

[13] JIANG F L, ZENG X W. Trust model for wireless network security based on the edge computing[J]. Microsystem Technologies, 2019, 27: 1627-1632.

[14] WANG K, CHEN J M, LIANG Z D, et al. A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain [J]. Information Fusion, 2021, 72: 100-109.

[15] WU X, LIANG J B. A blockchain-based trust management method for Internet of Things [J]. Pervasive and Mobile Computing, 2021, 72: 101330.

[16] ABEYSEKARA P, HAI D, QINA K. Data-driven Trust Prediction in Mobile Edge Computing-based IoT Systems [J]. IEEE Transactions on Services Computing, 2021: 1-1.

[17] DEEBAK B D, MEMON F H, KHOWAJA S A, et al. A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems [J]. IEEE Internet of Things Journal, 2023, 10(8): 6652-6660.

[18] PAN X, YUAN L Y, HUANG M M. Cross-domain trust evaluation model for IoT based on blockchain and domain trust degree [J]. Computer Engineering, 2023, 49(5): 181-190.

[19] HE F, XIAO Z L, WANGX B, et al. Lightweight Flexible Group Authentication Utilizing Historical Collaboration Process Information [J]. IEEE Transactions on Communications, 2023, 71(4): 2260-2273.

ZHAO Chanchan, born in 1982, Ph.D, associate professor. Her main research interests include mobile edge computing and blockchain.

SHI Bao, born in 1982, Ph.D, associate professor. His main research interest is image processing.