•网络空间安全•

DOI:10.15961/j.jsuese.201900893

本刊网刊

基于图论的边缘计算信任评估优化模型

杜瑞忠[1], 许琨琪[1*], 田俊峰[2]

(1.河北大学 网络空间安全与计算机学院, 河北 保定 071002; 2.河北大学 河北省高可信信息系统重点实验室, 河北 保定 071002)

摘　要:针对边缘计算环境中的设备资源受限、现有信任模型忽略计算负载与信任路径冗余的问题, 提出了一种基于图论的边缘计算信任评估优化模型。首先, 基于边缘计算构建信任模型的体系架构, 将边缘设备间复杂庞大的信任关系抽象成有向加权图, 并对设备间的信任关系进行定义说明, 再采用基于信息熵理论的自适应聚合方法对信任值进行聚合计算, 修正多源信任之间的差异度; 其次, 通过添加信任阈值、路径长度限制、滑动窗口等多重约束条件, 事先过滤明显不符合信任要求的节点和信任边, 降低不必要的计算消耗; 最后, 利用改进后的深度优先搜索算法(depth first search, DFS), 在信任路径搜索过程中规避冗余信任边, 从而避免环路以及节点绕路问题, 并采用递归函数Combine聚合反馈信任值。使用MATLAB仿真软件确定实验参数, 验证模型区分恶意节点与正常节点的能力。并在交互成功率、时间开销以及能量开销3个方面进行实验, 将本文模型与PSM模型、RFSN模型以及随机选择模型进行对比。实验结果表明, 相较于其他模型, 本文模型在不同诚实程度的网络环境下都能快速达到稳定状态, 且时间与能量开销均低于其他模型, 证明该模型在保证有效性的同时, 能够在一定程度上减轻边缘设备的资源开销, 提高网络的生存周期。

关键词:边缘计算; 信任模型; 信任路径; 冗余优化

中图分类号:TP393.0　　**文献标志码**:A　　**文章编号**:2096-3246(2020)03-0150-09

Optimization Scheme of Trust Model Based on Graph Theory for Edge Computing

DU Ruizhong[1], *XU Kunqi*[1*], *TIAN Junfeng*[2]

(1.School of Cyberspace Security and Computer, Hebei Univ., Baoding 071002, China;
2.Key Lab. on High Trusted Info. System in Hebei Province, Hebei Univ., Baoding 071002, China)

Abstract: In order to solve the problems of the limited devices resources in the edge computing environment and the negligence of computing load as well as the redundant trust path in the existing trust models, a trust evaluation optimization model of the edge computing was proposed based on the graph theory. First, an architecture of trust model based on edge computing was built, of which the complex and huge trust relationship between edge devices was abstracted into a directed weighted graph, and the trust relationship between devices was defined and explained. Then, an adaptive aggregation method based on the information entropy theory was used to aggregate the trust value, which could correct the difference between multi-source trust. Secondly, the constraints of trust threshold, path length restriction and sliding window were added. With these multiple constraints, the nodes and trust edges that obviously do not meet the trust requirements were filtered in advance, which reduces unnecessary computing consumption. Finally, an improved depth first search algorithm was used to filter redundant trust edges, which could avoid loop and node detour problems in the trust path search process. The recursive function Combine was further used to aggregate the feedback trust value. The MATLAB simulation software was used to determine the experiment parameters, and verified the model's ability of distinguishing malicious nodes from normal nodes. The proposed model was compared with PSM model, RFSN model and random selection model in interaction success

收稿日期:2019 – 09 – 16

基金项目:国家自然科学基金项目(61572170; 61170254); 河北省自然科学基金项目(F2018201153); 河北省高等学校科学技术研究基金项目(ZD2016043); 河北省物联网数据采集与处理工程技术研究中心基金项目(河北065201)

作者简介:杜瑞忠(1975—), 男, 教授, 博士. 研究方向: 可信计算; 信息安全. E-mail: drzh@hbu.edu.cn

* 通信联系人 E-mail: 929207348@qq.com

网络出版时间:2020 – 05 – 08 11 : 32 : 45　　**网络出版地址**:http://kns.cnki.net/kcms/detail/51.1773.TB.20200507.1226.001.html

rate, time cost and energy cost. The experimental results show that compared with other models, the proposed model could achieve stable state quickly in network environments with different honesty degrees, and the time and energy costs are lower than that of other models. The proposed model can reduce the resource overhead of edge devices and improve the network life cycle while ensuring the effectiveness.

Key words: edge computing; trust model; trust path; redundancy optimization

边缘计算利用众多边缘设备为用户提供近地的实时计算与存储功能，将云端的部分或全部计算任务迁移到边缘设备上，能够满足用户低时延、快响应的需求[1]，在智能车联网、虚拟现实、医疗保健、智能家居、智慧城市等场景都有很好的应用效果[2−4]。边缘设备兼顾数据的消费者和生产者，大部分用户隐私信息都存储在了边缘层，但边缘计算缺乏像云计算一样稳定的基础保护设施，再加上边缘计算的内容感知、实时计算、并行处理等开放特性，导致设备间缺乏必要的信任，给边缘设备的安全性带来了挑战[5−7]。

信任机制能够有效抵御网络的内部攻击，是目前保证设备提供可靠服务的关键技术之一[8]，在云计算、P2P、无线传感器网络等计算模式中都应用广泛[9−11]。现有的信任模型研究成果非常多，除了基于主观逻辑、D−S证据理论、模糊证据理论、贝叶斯网络以及神经网络等评估模型，还有基于推荐节点相似度、评分偏差以及奖惩措施等其他方法的评估模型。但面对复杂多变的边缘计算环境，旧的信任模型会有一定的局限性。首先，边缘层包含着大量高频交互的设备，形成了复杂而庞大的信任网络，存储并查询这些信任信息会消耗大量的时间和空间；其次，边缘设备大多是资源受限设备，难以承担复杂的存储、查询任务。因此，构建适用于边缘计算环境的轻量级信任评估模型具有重要的现实意义。

基于边缘计算环境，Huang等[12]将信任分为熟悉度、相似度和及时性3个维度，并利用向量机和多权重主观逻辑的方法维护、更新本地车辆的信任信息。邓晓衡等[13]提出了基于综合信任的多目标优化协同方案，利用信任评估保障体系对边缘计算资源管理与协同系统进行了优化。Soleymani等[14]将雾节点视为车辆环境局部信息的可靠存储，并加入安全信任模型对车辆进行本地的信任管理，确保了授权车辆接收信息的准确性。吴启武等[15]则针对车物联网中节点的移动性和相遇临时性等问题，提出了一种基于贝叶斯理论的车联网安全路由信任模型，减轻了信任管理的复杂度并降低了端到端时延。针对边缘计算中信任机制共谋问题，Yuan等[16]提出了一种基于多源反馈的信任计算模型，在传统的信任关系中添加了来自基站的反馈信任，增强了信任模型的适应性。Ruan等[17]提出了基于测量理论的信任管理框架，将测量误差视为节点的置信度，以此衡量信任评估的可信度，提升了信任值的准确性。

这些研究工作有效地推动了边缘计算中信任评估模型的发展，但仍存在以下不足：1）大多模型都忽略了信任评估过程中的计算负载、资源消耗等问题；2）现有的信任模型很少考虑到信任路径数量与计算成本之间的权衡问题，忽略了冗余信任路径对评估结果以及资源开销的影响。

针对上述不足，本文利用有向加权图构建节点之间的信任关系，然后在信任路径搜索过程中通过多重约束条件排除大量无关的信任边，同时利用改进后的DFS算法避免环路以及节点绕路问题，降低无关信任信息的干扰。在信任聚合时采用熵权法对信任进行聚合，克服手动加权的局限性。此外，模型中信任子图的形成与优化完全是在边缘服务器层和边缘设备层完成，降低了数据传输时的带宽消耗，是适用于边缘计算环境的轻量级算法。

1　边缘计算信任评估体系架构

边缘计算信任模型的体系架构如图1所示，可信边缘计算体系包括云层、边缘服务器层以及边缘层3层。

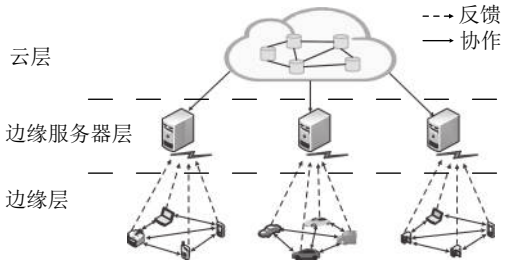


图 1　边缘计算信任模型体系结构

Fig. 1　Edge computing trust model architecture

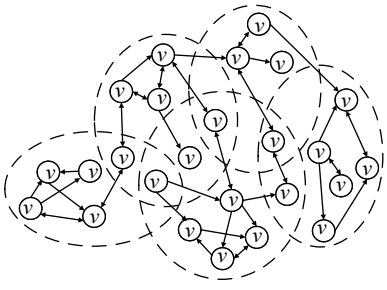
1）云层的数据中心存储着用户的各种数据，云层可将计算任务下发给边缘服务器，任务在边缘层执行完毕后返回给云层。

2）边缘服务器层主要负责云层与边缘层的通信以及数据传输，在本文中假设它是可信的。每一个边缘服务器（edge server, ES）都存储着区域中各种设备的交互信息，并负起监督责任，保障信任模型的运转以及信任评估结果的准确性，并对来自设备的反馈进行聚合计算，降低设备的资源成本。

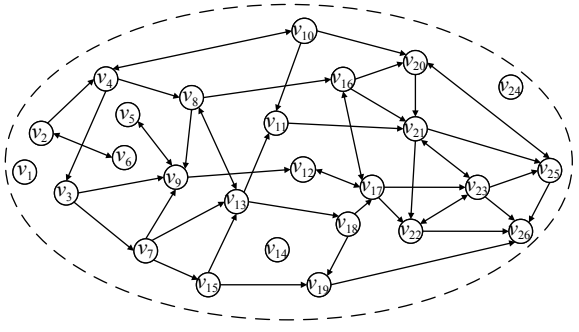
3）边缘层由各种在边缘执行任务的边缘设备（edge device, ED）构成，包括智能手机、摄像头、可穿戴设备、车辆等。边缘设备根据位置和特征等因素被

划分为不同的域，每个域都由一个边缘服务器管理。设备可以根据任务需求在域内或域间请求服务，实现交互合作。任务协作前，设备向边缘服务器发送请求信息，确保合作者的可信性；完成协作服务之后，设备会更新自身的信任列表，并定期向边缘服务器提交评价信息。

由图1可以看出，边缘层中设备间的交互形成了一个有向网络图。因此，边缘层的信任关系可以被看做一个大型的有向加权图（如图2所示），将参与交互的设备抽象为图中的节点，设备间的信任关系抽象为节点之间的有向边，模型中的每一个节点都可以通过路径搜索以及图融合来构造任意节点间的信任关系，并进一步聚合节点间信任信息从而得到全局信任关系。



(a) 域间信任图



(b) 域内信任图

图 2　信任图

Fig. 2　Trust graph

信任图可以用二元组$G=(V,E)$来进行说明。$V=\{v_1,v_2,v_3,\cdots,v_n\}$是信任节点集，其中$n$指区域内的节点个数，也就是该区域网络的大小。$E=\{e_1,e_2,e_3,\cdots,e_m\}$是指信任边集，$e_i$表示节点间的一条有向边，由三元组$e=\{v_i,v_j,\omega\}$表示，其中$\omega$是信任边的权重，表示节点$v_i$对节点$v_j$的综合信任值，取值范围为[0, 1]之间的实数。

2　基于图论的信任模型优化方案

2.1　信任关系

信任是对设备能否提供良好网络服务的主观性判断，在设备选择任务对象时提供指导信息，避免与自私节点或是恶意节点建立合作关系，保证设备间安全可靠的通信。一般，设备间的信任关系分为直接信任、推荐信任以及综合信任。本文添加了反馈信任的概念，能够更好地描述设备间的信任关系。

信任关系的定义和计算公式如下：

定义1　直接信任是设备基于自身的历史交互信息得出的信任评价。

直接信任是设备聚合多次交互结果所得出的信任评分。节点i对节点j提供的最近服务交互评分集合记为$L_{ij}=\{l_1,l_2,l_3,\cdots,l_n\}$，其中，交互成功评分为1，失败则为0，该信任序列将存储在节点中。直接信任DT_{ij}用风险概率模型[19]进行计算：

$$DT_{ij}=\frac{o^{\mathrm{s}}\times(o^{\mathrm{f}})^{(-1/\alpha)}}{o^{\mathrm{s}}+o^{\mathrm{f}}} \tag{1}$$

式中：o^{s}为交互成功的次数；o^{f}为交互失败的次数；利用惩罚因子α可以防止恶意节点在较高的信任累计后的突然攻击。

定义2　推荐信任是设备通过第三方的信任意见而获取的信任评价。

第三方节点对目的节点的直接信任，并将其推荐给源节点，推荐信任以矩阵的形式存放在区域内的边缘服务器中，由服务器进行管理与更新。为了防止自夸，服务器将$DT_{11}\sim DT_{nn}$的值设置为0。

$$\boldsymbol{R}=\begin{bmatrix} DT_{11} & DT_{21} & \cdots & DT_{n1} \\ DT_{21} & DT_{22} & \cdots & DT_{n2} \\ \vdots & \vdots & & \vdots \\ DT_{n1} & DT_{n2} & \cdots & DT_{nn} \end{bmatrix} \tag{2}$$

定义3　反馈信任是基于其他可信邻居的信任意见聚合而成的信任评价。

反馈信任是由直接信任和推荐信任形成的从主体到客体的信任路径，它综合考量了多条推荐信任路径的反馈，能够刻画客观可信度。根据信任传递与聚合规则，反馈信任FT_{ij}计算公式如下：

$$FT_{ij}=\frac{1}{k}\sum_{x=1}^{k}Q_{ij}^{x} \tag{3}$$

$$Q_{ij}^{x}=DT_{ia}\times DT_{ab}\times DT_{bc}\times\cdots\times DT_{nj} \tag{4}$$

式中：FT_{ij}是指两个节点间所有信任路径反馈信任的聚合值，即节点i对节点j的全局反馈信任；k表示节点间信任路径的总条数；Q_{ij}^{x}是指从源节点i到目的节点j的第x条信任路径中计算得到的反馈信任值；a、b、c、$\cdots$、n表示该条信任路径中经过的所有节点的编号。

定义4　综合信任是指基于自身经验以及其他可信邻居的信任意见聚合而成的信任评价。

综合信任是设备对另一个设备的全局信任，是通过某种方式聚合直接信任与反馈信任而得到的最终信任值。当节点间没有直接交互记录的时候，反馈信任就被视为综合信任来构建陌生节点间的信任。为了提高信任的可靠性，综合信任采用基于信息熵理论的自适应聚合方法，它能够有效衡量信任序列的无序程度，并对信任值之间的差异度进行修正。综合信任T_{ij}计算如下：

$$T_{ij}=\omega_1\times DT_{ij}+\omega_2\times FT_{ij} \tag{5}$$

式中，ω_1和ω_2分别为直接信任与反馈信任的自适应权重，它的计算公式如下：

$$\omega_1=\frac{1-\dfrac{H(DT_{ij})}{\mathrm{lb}\ DT_{ij}}}{\left[1-\dfrac{H(DT_{ij})}{\mathrm{lb}\ DT_{ij}}\right]+\left[1-\dfrac{H(FT_{ij})}{\mathrm{lb}\ FT_{ij}}\right]} \tag{6}$$

$$\omega_2=\frac{1-\dfrac{H(FT_{ij})}{\mathrm{lb}\ FT_{ij}}}{\left[1-\dfrac{H(DT_{ij})}{\mathrm{lb}\ DT_{ij}}\right]+\left[1-\dfrac{H(FT_{ij})}{\mathrm{lb}\ FT_{ij}}\right]} \tag{7}$$

式中，$H(TD_{ij})$和$H(FT_{ij})$分别为直接信任和反馈信任的信息熵，计算公式如下：

$$H(DT_{ij})=-DT_{ij}\mathrm{lb}\ DT_{ij}-(1-DT_{ij})\mathrm{lb}(1-DT_{ij}) \tag{8}$$

$$H(FT_{ij})=-FT_{ij}\mathrm{lb}\ FT_{ij}-(1-FT_{ij})\mathrm{lb}(1-FT_{ij}) \tag{9}$$

2.2　信任子图优化方案

一般情况下，得到的反馈信息越多就意味着节点信任值的计算结果越可靠，但路径的查找、聚合需要消耗大量的时间和空间资源，再加上恶意节点的恶意反馈、合谋攻击等，无形中增加了节点的计算成本，导致最终的信任值出现偏差。信任图的优化方法从以下两个角度来考虑：一是，事先过滤明显不符合要求的信任边以及节点，这样可以大幅度减少信任图的遍历次数；二是，在路径形成过程中过滤掉冗余的边，能够减少信任计算中的负载问题。

2.2.1　约束条件

1）信任阈值

信任阈值是节点可信度的边界值，当信任度低于阈值时，该节点就是不可信节点，也就意味着它所提供的推荐信任也是不可信的。在以往的研究中，阈值一般取中间值0.5，但当区域内大多节点都是高可信节点时，节点信任值的计算量就会增多。所以当节点可信度很高时，可以将阈值设定为该区域节点的平均信任度，这样既可以减少遍历次数，也能保证半数节点都能参与反馈信任的计算，提高信任的有效性。

$$th=\begin{cases}\overline{T},\ \overline{T}>0.5;\\ 0.5,\ \overline{T}\le 0.5\end{cases} \tag{10}$$

2）路径长度

在信任子图中，如果路径长度较长，信任信息的衰减较为严重，遍历次数与路径数量也会造成很大的时间消耗；如果对路径长度限制过为严苛，搜寻到的路径数量较少会使反馈信息变少，从而导致节点判断不准确。

根据六度分离理论[18]，一般认为信任的传递长度超过6后，信任信息就不再可靠。Lunze[19]研究了多Agent系统中的六度分离理论，并通过实验论证了在不同的连接概率下两节点的平均路径长度的上界。杜淑颖等[20]将六度理论应用到社交好友推荐算法研究中，验证了其可用性。综上，根据六度分离理论及现有研究，边缘服务器在构建信任子图时，将节点间的路径长度最大值设为6，避免路径过长造成的信任值失真以及资源消耗问题。

3）滑动窗口

对于边缘计算这种交互频繁的计算模式，间隔太久的信任信息会对节点的判断造成干扰。考虑到边缘层节点资源受限的特点，如图3所示，可以利用滑动窗口进行信任值的计算与更新。只有滑动窗口内的交互记录是有效的，即有效交互记录的最大值为W。这样既可以保证信息的时效性，又能节约节点的计算成本。

图 3　滑动窗口

Fig. 3　Sliding window

2.2.2　冗余优化

边缘服务器从源节点到目的节点构建一个信任网络时，如果将所有信任边都添加到信任子图中，会使信任子图产生大量冗余，导致信任路径通过一些不必要的节点甚至出现环路，造成计算负载的增加，信任值也会随之变得不确定。在大规模信任图中任选两个节点并构建两点间的信任子图，图中每条边都代表节点间的信任关系。图4为节点S与节点D构成的信任子图，由于篇幅有限，在图中省略部分节点与边。

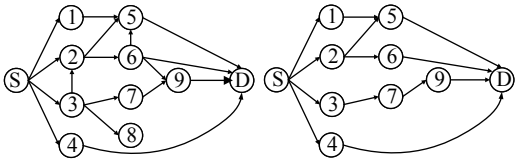


图 4　信任子图

Fig. 4　Trust subgraph

从图4(a)中可以看出，从节点S到节点D一共有11条信任路径，分别为S—1—5—D、S—2—5—D、S—2—6—D、S—2—6—5—D、S—2—6—9—D、S—3—2—5—D、S—3—2—6—D、S—3—2—6—5—D、S—3—2—6—9—D、S—3—7—9—D、S—4—D，其中，S—2—6—5—D、S—2—6—9—D、S—3—2—5—D、S—3—2—6—D、S—3—2—6—5—D、S—3—2—6—9—D等6条路径都通过了一些不必要的冗余边。例如，在S—2—6—5—D这条路径节点6与节点D有过直接交互，无需再从节点5获取节点D的推荐信任值，应将6—5这条信任边删除。同理，其他5条信任路径也是此类情况，需要删除此类冗余信任边，避免路径变长导致的信任偏差。

针对上述问题，本文提出了一种基于深度优先搜索思想的子图优化算法，将优化目标定义为子图中任意信任边连接的两个节点之间没有第2条可达路径。通过判断节点是否被多次访问以及任意两节点间是否有直达路径，去除节点间多余的信任边，从而避免信任路径中的环路以及节点绕路问题，优化后的信任子图如图4(b)所示。该方法克服了传统信任方案的局限性，减少了节点聚合路径的负载工作，大大提高了节点的工作效率。算法1伪代码如下。

算法1 信任路径优化算法

输入：信任图$G(V,E)$，源节点s，目的节点d；

输出：路径集合P_s。

1. 将源节点s加入到路径p中；
2. $u=Dst(s)$; //u为源节点的邻接节点表
3. while $p \neq \varnothing$ do
4. if $u \in N_v$ then //判断节点是否在访问列表中
5. $u=u\rightarrow next$; //更换下一邻接节点
6. end if
7. for $v \in p$ do //判断节点是否与路径中的节点有过交互
8. if $u \in Dst(v)$ then
9. $u=u\rightarrow next$;
10. end for
11. if $u \neq \varnothing$ then
12. $p \leftarrow p \cup \{u\}$, $N_v \leftarrow N_v \cup \{u\}$;
13. if $u==d$ then//判断节点是否为目的节点
14. $Pset \leftarrow Pset \cup p$;
15. $u=p.pop(\,)$, $N_v.pop(u)$; //移出当前节点
16. $u=u\rightarrow next$;
17. else
18. $u=Dst(u)$; //向下继续遍历
19. else
20. $u=p.pop(\,)$, $N_v.pop(\,)$;
21. $u=u\rightarrow next$;
22. end for
23. return P_s

算法1中，$Dst(v)$为与节点v交互过的节点集合，N_v为被访问过的节点集合，p用于存储从源点到目的节点的信任路径，P_s为两点间所有信任路径的集合。首先，按照约束条件将不符合要求的节点提前剔除；然后，遵循算法1来确定下一个节点或将其删除。每次访问一个新的节点，首先判断它是否在访问列表中，以及它是否在访问列表的邻接节点集合中，确定该节点是否可以加入到当前路径p中。直至新的节点为目的节点d，得到从源节点到目的节点的一条完整路径，并将当前路径加入到路径集合中。随后，初始化信任路径，回到前一个分支继续搜寻下一条信任路径，直到所有分支都被遍历，得到最后的路径集合P_s。

经过冗余优化删除部分不必要的节点以及信任边，能够减少信任查找次数和信任聚合的数量，降低信任计算的工作量，还可以使得到的信任值更加贴近于实际信任值。

2.2.3 路径合并算法

根据信任传递规则计算出k条信任路径源节点s对目的节点d的反馈信任值。信任路径合并算法的伪代码如算法2所示。

算法2 信任路径合并算法

输入：路径集合P_s，源节点s，目的节点d；

输出：反馈信任值FT。

1. Function Combine(s,d)
2. if $d \in$ Right(s) then//判断是否已搜索到目的节点d
3. return $FT=FT\times D_{sd}$;
4. else
5. if Right(s) >1 then//如果右邻接集合不为空
6. for $u \in$ Right(s) do
7. $FT= FT+D_{su}\times$Combine (u,d);
8. end for
9. else
10. $FT=D_{su}\times$Combine(u,d);
11. End Function

算法2中，Right(v)表示v节点的右邻接节点集合，利用递归函数Combine，将算法1中获取的路径进行信任值的合并计算。当Right(v)不为空时，从集合中依次取出节点开始向后搜寻路径，并在搜寻过程中将信任路径进行合并计算，直到找到d为右邻接点时返回得到的反馈信任值。

3 仿真实验

为了验证信任优化模型的有效性和资源开销情

况，本文利用MATLAB进行仿真实验，模拟节点间的信任关系网络，确定实验参数，并验证模型区分节点的能力，然后与PSM模型[12]、RFSN模型[21]以及随机选择算法进行比较。仿真检测区域设为200 m×200 m的正方形，随机放置200个节点模拟资源受限的边缘层设备，具体仿真参数如表1所示。

表 1　仿真参数

Tab. 1　Simulation parameters

参数	描述	数值
Z_n	节点总数量	200
Z_e	边缘服务器数量	2
M	恶意节点比例/%	10、20、40
W	滑动窗口	20
α	惩罚因子	2

为了使实验更接近于真实的边缘计算网络环境，将正常节点的交互成功率设为90%，模拟由于非入侵因素（节点繁忙等）导致的节点异常。实验中的恶意节点均为随机选取，并将恶意节点分为两类，一类提供恶意服务，并向其他节点提供虚假推荐信任，另一类提供诚实服务，但提供诋毁诚实节点、夸大同类节点的推荐值。这两类节点在恶意节点中的比例各为50%。此外，在实验部分对域内域间信任不进行区分，边缘服务器间可互相交换各自管理的信任信息。

3.1　参数设置

3.1.1　惩罚因子α

为了确认惩罚因子α的大小，考察在不同交互失败次数下α值对直接信任值的影响情况，实验结果如图5所示。为了便于计算与对比，对α进行取整处理。

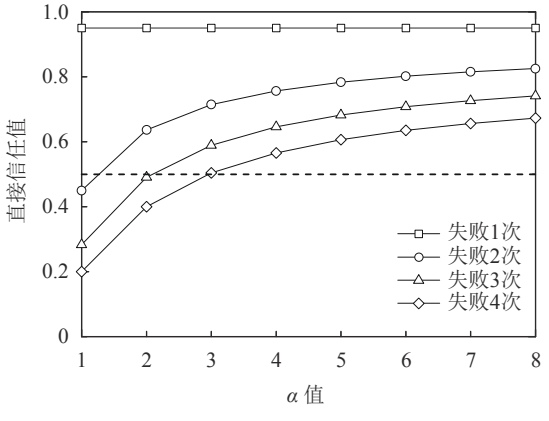


图 5　参数α对直接信任值的影响

Fig. 5　Impact of parameter α on the direct trust value

从图5中可以看出：随着α的增大直接信任值也越来越大，表明惩罚因子取值越大对交互失败节点的惩罚力度就越小。当α的值大于3时，失败4次后，信任值还高于信任阈值，惩罚效果并不显著。α=1时，两次以上交互失败就会导致节点的信任值低于信任阈值0.5。一般情况下，正常的节点也存在一定失误率，故选取有一定容忍度的值，将惩罚因子设为2。实际上，可以根据网络中节点对失误的容忍度对调整α的值。

3.1.2　滑动窗口

为了确认滑动窗口的大小，考察在不同滑动窗口大小下，目的节点的信任值随交互次数变化的情况，实验结果如图6所示。一开始，目的节点有90%的可能提供优质服务，在20次交互后，节点开始提供恶意服务。

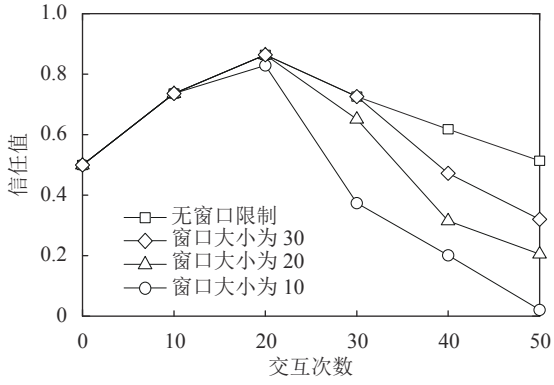


图 6　时间窗口大小对信任值的影响

Fig. 6　Influence of time window size on trust value

从图6中可以看出，在交互20次后，节点累积了较高的信任值，随后节点开始提供恶意服务。随着滑动窗口数量的减小，节点的信任值下降得越明显，表明其对恶意节点的惩罚更加严苛。但滑动窗口太小，也会存在恶意节点依靠短暂的诚实服务骗取高信任值的情况。综合考虑，根据上述分析以及现有研究，将滑动窗口的值取为20。

3.2　信任评估结果分析

为了分析本文模型区分恶意节点与正常节点的能力，将节点的初始信任值设为中间值0.5，节点的综合信任值在10个仿真周期内逐渐趋于平衡，实验结果如图7所示。

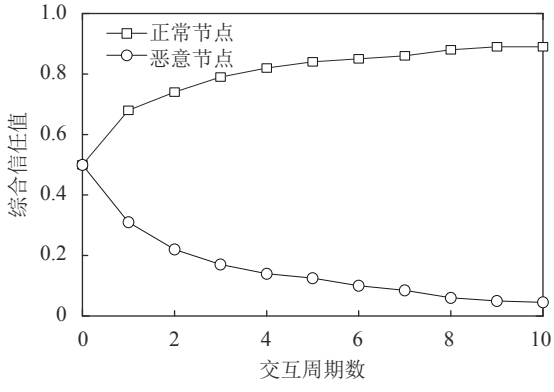


图 7　正常节点与恶意节点信任值对比

Fig. 7　Comparison of the trust value of normal and malicious nodes

随着节点间交互次数的增多，正常节点的信任值逐渐上升并趋近于1，恶意节点的信任值则递减并趋近于0。因此，该模型能够有效区分正常节点和恶意节点，得到的综合信任值也能很好地反映节点的行为。

3.3 有效性评价

交互成功率是指交互成功的次数占总交互次数的比例，它能够反映信任模型抵制恶意行为的能力，较大的交互成功率表明该信任模型具有更高的可靠性。当节点按要求完成协作任务就被视为交互成功。为了验证方案的有效性，进行了100个交互周期的仿真实验，每个节点在每个周期会发起一次服务请求，节点可同时作为服务请求者和服务提供者。

将恶意节点的比例设为10%、20%和40%，考察信任模型在不同比例恶意节点的网络环境下，信任模型交互成功率随交互次数变化的情况，实验结果如图8所示。

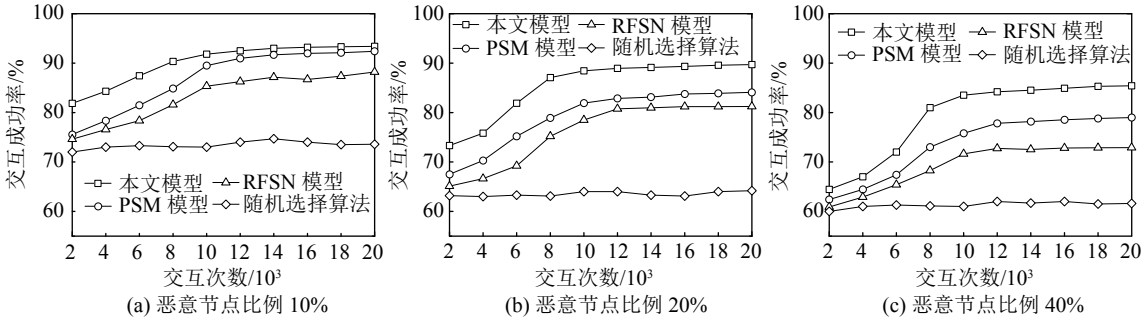


图 8 不同恶意节点比例下的交互成功率

Fig. 8 Interaction successful rate in different malicious node proportions

从图8(a)～(c)中可以看出，随着交互次数的增加，交互成功率会随着交互次数增多而变高，但增长速度逐渐变缓，最终趋近于一个值。但随着恶意节点比例的增多，模型的适应时间会变长，交互成功率也会有所下降。从图8(a)～(c)的对比来看，本文模型随着交互次数的增多能快速达到稳定状态，说明该模型能够有效抵制恶意节点，提高交互成功率。

在100个交互周期后，各模型交互成功率随着恶意节点比例增长的变化情况，如图9所示。

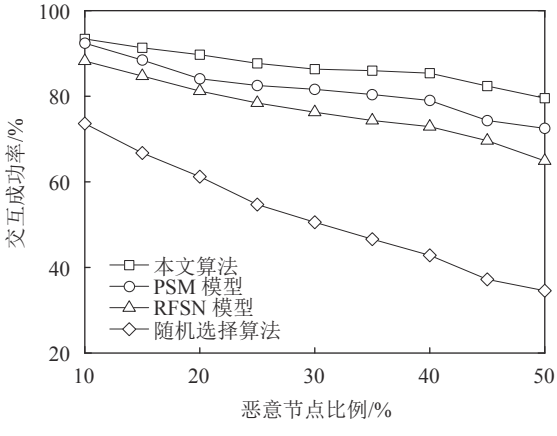


图 9 不同模型的交互成功率对比

Fig. 9 Comparison of interaction successful rate in different models

从图9中可以看出，随着恶意节点比例的增长，各信任模型的交互成功率均呈现了不同程度的下降趋势，但本文模型交互成功率较为稳定。这是由于通过多重约束剔除了恶意节点，使信任值能很好地反映节点的行为。

3.4 资源开销评价

边缘层大多都是资源受限设备，设备的存储空间不足、计算能力较差等问题是构建信任评估模型的一大挑战。因此，资源开销是判断信任模型性能的重要参数，本文从时间开销和能耗两方面考量模型的资源开销情况。

3.4.1 时间开销

信任模型的时间开销大部分来自信任值的计算，所以本文用综合信任聚合的总时间来评估整个网络的计算效率。在仿真环境中随机选取30%的恶意节点，每组实验进行5次取平均值，实验结果如图10所示。

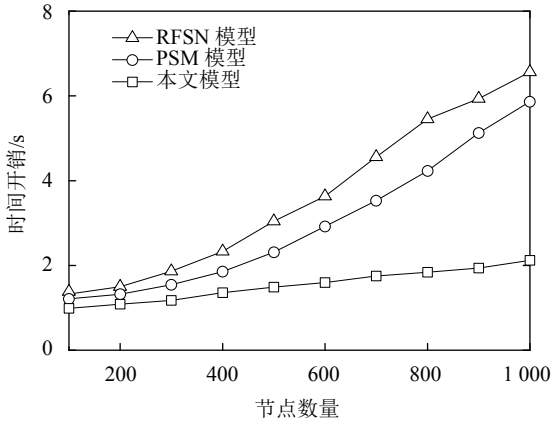


图 10 不同节点数量下的时间开销对比

Fig. 10 Comparison of time overhead under different number of nodes

图10展示了从100个节点增至1 000个节点时的时间开销变化情况。当节点数量较少时，两个模型之间的时间开销相差不大，但随着网络规模增大，逐渐低于PSM模型和RFSN模型的计算时间。这是由于该模型对信任图进行了化简计算，提前过滤信任值较低的节点，然后经过冗余优化步骤删除部分不必要的路径，减少了信任查找次数和信任路径，降低了信任计算的工作量。

3.4.2　能量开销

为分析本文模型的能量开销情况，假设每个节点的初始能量设为0.5 J，每次传输和接收数据包的能耗为50 nJ/bit，数据包单位为bit，在[3 000，4 000]的区间值内随机选取，同一交互周期两种模型数据包大小一样。实验一共进行100个仿真周期，区域内网络能量变化情况如图11所示。

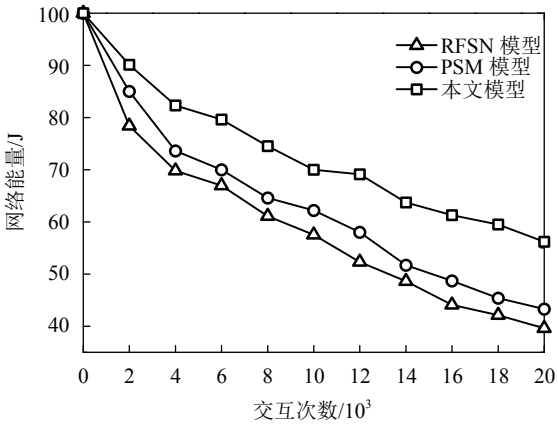


图 11　不同模型传输能耗随交互次数变化的对比

Fig. 11　Comparison of transmission energy consumption of different models with interaction times

随着节点间交互次数的增多，网络能量均呈下降趋势，本文模型网络能量消耗速率低于其他两个模型，最后整体网络剩余的能量也高于其他两个模型。这是因为反馈信任仅存储在边缘服务器中，边缘节点只需向服务器发送查询请求，而服务器只需返回一个反馈信任值。此外，每个节点不需要存储过多节点的信任信息，只需要定时向服务器发送推荐信任即可。因此，该模型能够有效降低信任度值传输过程中的能耗，提高网络的生存周期。

4　结束语

边缘计算环境中海量节点之间的数据交互导致了节点间信任链的爆炸性增长，形成了复杂而庞大的信任网络，边缘设备难以承担存储聚合任务，冗余的信任路径还会使最终的信任值出现偏差。因此，本文针对上述问题，提出了适用于边缘计算的基于图论的信任评估优化模型，仿真结果表明该方案能够有效节约网络资源，在信任模型的性能方面也有一定提升。

但是，本方案中关于区域内节点负载均衡等问题没有提出很好的解决办法，在接下来的工作中可以通过一定的奖惩措施，鼓励节点与信任度高但交互次数较少的节点协作，避免信任稀疏和过度消耗特定节点等情况的出现。

参考文献：

[1] Shi Weisong,Zhang Xingzhou,Wang Yifan,et al.Edge computing:State-of-the-art and future directions[J].Journal of Computer Research and Development,2019,56(1):69–89.[施巍松,张星洲,王一帆,等.边缘计算:现状与展望[J].计算机研究与发展,2019,56(1):69–89.]

[2] Li Xiaocui,Zhou Zhangbing,Guo Junqi,et al.Aggregated multi-attribute query processing in edge computing for industrial IoT applications[J].Computer Networks,2019,151:114–123.

[3] Zhang Ke,Mao Yuming,Leng Supeng,et al.Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks[J].IEEE Access,2016,4:5896–5907.

[4] Zhang Tan,Chowdhery A,Bahl P V,et al.The design and implementation of a wireless video surveillance system[C]// Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom'15). New York:ACM,2015:426–438.

[5] Shi Weisong,Sun Hui,Cao Jie,et al.Edge computing—An emerging computing model for the internet of everything era[J].Journal of Computer Research and Development,2017,54(5):907–924.[施巍松,孙辉,曹杰,等.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.]

[6] Zhang Jiale,Zhao Yanchao,Chen Bing,et al.Survey on data security and privacy-preserving for the research of edge computing[J].Journal on Communications,2018,39(3):1–21.[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.]

[7] Shi Weisong,Cao Jie,Zhang Quan,et al.Edge computing:Vision and challenges[J].IEEE Internet of Things Journal,2016,3(5):637–646.

[8] Guo Jingjing,Ma Jianfeng,Li Xinghua,et al.A situational awareness trust evolution model for mobile devices in D2D communication[J].IEEE Access,2018,6:4375–4386.

[9] Wang Tian,Zhang Guangxue,Cai Shaobin,et al.Survey on trust evaluation mechanism in sensor-cloud[J].Journal on Communications,2018,39(6):37–51.[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.]

[10] Ahmed A,Abu Bakar K,Channa M I,et al.A survey on trust

based detection and isolation of malicious nodes in ad-hoc and sensor networks[J].Frontiers of Computer Science,2015,9(2):280–296.

[11] Yang Kai,Yang Xiaoyuan,Ma Jianfeng.A novel detection scheme based on D–S evidence theory in wireless sensor networks[J].Journal of Sichuan University(Engineering Science Edition),2016,48(2):118–124.[杨凯,杨晓元,马建峰.无线传感器网络中一种基于D–S证据理论的监测机制[J].四川大学学报(工程科学版),2016,48(2):118–124.]

[12] Huang Xumin,Yu Rong,Kang Jianwen,et al.Distributed reputation management for secure and efficient vehicular edge computing and networks[J].IEEE Access,2017,5:25408–25420.

[13] Deng Xiaoheng,Guan Peiyuan,Wan Zhiwen,et al.Integrated trust based resource cooperation in edge computing[J].Journal of Computer Research and Development,2018,55(3):449–477.[邓晓衡,关培源,万志文,等.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.]

[14] Soleymani S A,Abdullah A H,Zareei M,et al.A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing[J].IEEE Access,2017,5:15619–15629.

[15] Wu Qiwu,Liu Qingzi.Trusted model of secure routing for VANET based on Bayesian theory[J].Journal of Sichuan University(Engineering Science Edition),2015,47(2):129–135.[吴启武,刘青子.基于贝叶斯理论的VANET安全路由信任模型[J].四川大学学报(工程科学版),2015,47(2):129–135.]

[16] Yuan Jie,Li Xiaoyong.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.

[17] Ruan Yefeng,Durresi A,Uslu S.Trust assessment for internet of things in multi-access edge computing[C]//Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA).Krakow:IEEE,2018:1155–1161.

[18] Travers J,Milgram S.An experimental study of the small world problem[J].Sociometry,1969,32(4):425.

[19] Lunze J.Six degrees of separation in multi-agent systems[C]//Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC).Las Vegas:IEEE,2016:6838–6844.

[20] Du Shuying,Ding Shifei.Research on recommendation algorithm of social friends based on six-degree segmentation theory[J].Journal of Nanjing University of Science and Technology,2019,43(4):468–473.[杜淑颖,丁世飞.基于六度分割理论的社交好友推荐算法研究[J].南京理工大学学报,2019,43(4):468–473.]

[21] 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.

（编辑 赵 婧）

引用格式: Du Ruizhong,Xu Kunqi,Tian Junfeng.Optimization scheme of trust model based on graph theory for edge computing[J].Advanced Engineering Sciences,2020,52(3):150–158.[杜瑞忠,许琨琪,田俊峰.基于图论的边缘计算信任评估优化模型[J].工程科学与技术,2020,52(3):150–158.]