DOI:10.13718/j.cnki.xsxb.2022.03.013

基于模糊证据理论的物联网节点评估方法研究①

梁花[1], 李洋[1], 雷娟[1], 张森[1], 马创[2]

1. 国网重庆市电力公司电力科学研究院, 重庆 401120; 2. 重庆邮电大学 软件工程学院, 重庆 400065

摘要: 在物联网中, 如何充分挖掘网络环境中节点之间的信任关系是识别网络环境中恶意节点的重要工作. 针对现有节点评估方法不能有效应对节点恶意行为以致无法抵御网络内部攻击的问题, 提出了一种基于模糊证据理论的物联网节点评估方法. 首先, 我们使用模糊集理论并添加各种置信度因子来计算网络节点的直接置信度, 从而实现节点置信度等级的划分; 然后由相邻节点的推荐得到该节点的间接置信度, 并将 D-S 证据理论中的基本置信度函数定义为模糊隶属度函数; 最后通过证据差异来修改节点的两种置信度值的权重, 并依据 Dempster 组合规则对节点的置信度进行合成, 以获得节点的完整置信度. 仿真结果表明, 该方法与同类方法相比, 在网络的动态适应性、鲁棒性和安全性方面, 均具有更好的性能和更高的准确性以及可信度, 且该方法能够及时准确地发现恶意节点, 体现了节点置信度"难获取、易丢失"的特点.

关 键 词: 物联网; 模糊证据理论; 节点评估; 网络安全

中图分类号: TN915.08 **文献标志码**: A **文章编号**: 1000-5471(2022)03-0111-14

Research on Evaluation Method of Internet of Things Nodes Based on Fuzzy Evidence Theory

LIANG Hua[1], LI Yang[1],
LEI Juan[1], ZHANG Sen[1], MA Chuang[2]

1. *Electric Power Research Institute of State Grid Chongqing Electric Power Company, Chongqing 401120, China;*
2. *School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Abstract: In the Internet of Things(IoT), how to tap the trust relationship fully between nodes in the network environment is an important task to identify malicious nodes in the network environment. Aiming at the problem that existing node evaluation methods cannot effectively deal with the problem of malicious behavior of nodes, which leads to the problem that they cannot withstand internal attacks on the network, we propose an IoT node evaluation method based on fuzzy evidence theory. Firstly, we use fuzzy set theory and add various confidence factors to calculate the direct confidence of network nodes, so as to achieve the division of node confidence levels. Then the indirect confidence of the node is obtained from the recommendation of neighboring nodes, and the basic confidence function in D-S evidence theory is defined as a fuzzy

① 收稿日期: 2021-01-05
基金项目: 国家电网有限公司总部科技项目: 面向电力物联网端到端安全防护体系关键技术研究及应用资助(520626190067).
作者简介: 梁花, 中级工程师, 硕士, 主要从事网络与信息安全工作.

membership function. Finally, the weights of the two confidence values of the node are modified through the evidence difference, and the confidence of the node is synthesized according to the Dempster combination rule to obtain the complete confidence of the node. The simulation results show that compared with the similar methods, the method has better performance, higher accuracy and credibility in terms of network dynamic adaptability, robustness and security. This method can find malicious nodes in a timely and accurate manner, which reflects the characteristics of "difficult to obtain and easy to lose" node trust value.

Key words: Internet of Things; fuzzy evidence theory; node evaluation; cyber security

近年来，物联网(Internet of Things，IoT)作为一种新兴技术，开始应用于能源、科技、医疗、教育等多个领域[1]. 在物联网中，虽然网络节点通过传感器以及各种智能设备能为载体实时采集所需数据，为实现环境感知和智能决策带来了极大的便利，但是这些数据也包含了隐私数据和保密数据[2]. 同时，由于物联网本身具有的网络环境开放、网络节点能量有限、设备服务多样等特点，使得其网络中的节点极有可能受到恶意节点的攻击. 因此如何让物联网络中的节点免受恶意节点攻击是物联网网络部署过程中面临的重要挑战. 在物联网中，由于不同设备节点的计算资源和存储能力有着很大差异，并且网络中的节点合作与资源交互频繁，使得传统的安全认证技术和加密技术无法合适地部署在物联网的网络中，因为它不能及时发现和拦截恶意节点发起的内部攻击. 与此同时，网络中不同的业务属性和节点置信度也会影响网络中节点之间的信任关系. 例如，某些隐藏在网络中的恶意节点会利用合法身份发起内部攻击. 除此之外，物联网网络安全的主要威胁还包括恶意节点利用节点之间的信任关系来获取相关服务. 如果不能及时识别物联网网络中的恶意节点，则有可能使得整个网络受到攻击，从而导致隐私数据和保密数据泄露，对网络安全带来威胁. 因此，保障物联网的节点安全和改善节点合作关系的首要条件是充分挖掘网络环境中节点之间的信任关系，并以此来识别网络环境存在的恶意节点.

传统的基于加密和认证的安全机制只能抵御外部攻击，对网络内部的攻击缺乏有效的抵御手段，而信任管理是检测内部攻击[3]最常用的算法. 在该方法中，主要根据不同特征对网络节点进行评估和分类，保证节点之间的传输安全，从而保证整个网络的安全性. 基于信任的安全机制被认为是对传统密码安全方法的改进. 在物联网中，各设备之间的协作和交互可以描述为网络节点彼此之间的信任程度，通过记录节点之间的行为，以便维护在决策过程中使用的信息[4]. 如果网络中包含恶意节点则会限制节点之间的通信，只有当网络中所有节点都以可信赖的方式进行操作，才能保证节点之间交互的成功性和可靠性. 因此，应用信任管理机制增强物联网网络的安全性和健壮性，保证网络节点之间安全传输是个不错的方法.

网络节点置信度的主观模糊性会造成现有节点评估方法不能有效应对节点恶意行为以致无法抵御网络内部攻击的问题. 为解决这一问题，文献[5]定义了3种信任因子作为模型的输入，但这3种信任因子还不足以描述对节点的信任影响，因此本文在此基础上提出了一种基于模糊证据理论的物联网节点评估方法，通过节点行为策略添加多种信任因子并利用模糊证据理论实现节点信任值的评估. 首先，使用模糊集理论并添加各种置信度因子来计算网络节点的直接置信度，从而实现节点置信度等级的划分；然后，由相邻节点的推荐得到该节点的间接置信度，并将D-S证据理论中的基本置信度函数定义为模糊隶属度函数；最后通过证据差异来修改节点的两种置信度值的权重，并依据Dempster组合规则对节点的置信度进行合成，以获得节点的完整置信度. 本文的主要贡献包括以下几个方面：

1) 根据节点的行为策略添加了7种置信度因子，通过多种置信度因子的综合计算得到节点的直接置信度，提高了网络节点直接置信度的准确性；

2) 针对物联网网络中由于节点置信度存在主观模糊性和不确定性而导致评估模型无法有效抵御内部攻击的问题，通过利用模糊理论和D-S证据理论融合的方法，评估得到节点的完整置信度；

3) 仿真实验表明，相较于对比方法，该方法在网络的动态适应性、鲁棒性和安全性方面，均具有更好的性能、准确性以及可信度.

1　相关工作

国内外研究人员通过不同的信任评估方法(模糊逻辑、贝叶斯推理、熵理论、博弈论等)建立了各种信任评估模型[6-7]. 文献[8]提出了对信任度评估的各种要素，这对物联网中节点信任评估模型的建立具有指导性作用. 在物联网中，关于信任评估机制的研究主要包括基于策略的信任评估机制[9-10]和基于信誉度的信任评估机制[11-12]. 基于策略的信任评估机制主要是利用公钥和数字证书来定义节点的可信度；基于信誉的信任评估机制主要使用节点置信度来评估节点的可靠性. 其中，基于信誉的信任评估机制被广泛用于分布式网络中，它主要包括基于层次化[13]、节点行为[14]和角色[15]的信任评估模型. 为保障网络的安全性和可靠性，信任评估管理机制会根据节点的行为特征评估节点的可信度，确定节点是否是信任节点，以便于可以自定义网络的安全措施[16]. 文献[17]提出了一种框架，该框架通过考虑节点的信任来克服物联网中涉及的不确定性. 文献[18]提出了一种信任管理框架，该框架可以改善物联网网络中的访问控制机制，简化网络节点不确定性下的决策过程. 文献[19]提出了一种基于分布式分账技术的信任框架，该框架通过自我身份管理机制实现对任意身份的自动信任评级，从而得到物联网中节点的身份可量化信任和身份验证. 在反映网络节点的实时信任状态方面，文献[14]基于对节点行为的检测和直接信任值、推荐信任值和统计信任值的融合来建立信任评估模型，并通过计算节点的总信任值来确定网络上是否存在恶意攻击，仿真实验表明该模型取得了良好的效果. 文献[20]提出了一种基于贝叶斯理论的置信度评分模型，并进行了不确定性分析，利用全局信任迭代的方法计算网络节点的总体信任值，从而提高了信任收敛的速度. 文献[21]基于节点相似性、评价差异性、节点信任度值等角度提出了一种综合信任度评估模型对网络中推荐节点的可靠性进行全面评估，并取得了不错的效果. 文献[22]为了提高节点的信任值，充分考虑了邻居节点的推荐可靠性、关系熟悉度以及节点自身的直接信任值. 但在上述模型中，通常采用纯概率统计的方法进行可行性评估，难以从实际中获得先验知识，从而容易将信任的主观模糊性等同于随机性，不可避免地导致不合理的结果. 此外，上述方法中大多是采用单一的信任因素来获取节点的信任值，不能完全反映节点的信任属性，也会对节点的信任值造成一定影响.

在解决节点信任的不确定性和主观模糊性问题时，D-S 证据理论以及模糊集合理论是处理该类问题的有效方法. 基于 D-S 证据理论，文献[23]提出了一个基于 D-S 证据理论的多维度信任评估方法，对实体间的信任关系进行表示，并根据推荐信任值得到综合信任值，较好地解决了证据不确定性问题. 文献[24]给出了节点信任度的正式定义，基于 D-S 证据理论计算了节点置信度，并纠正了直接和间接置信度值，从而获得了对网络故障的良好容错性和动态适应性. 文献[25]通过改进 D-S 证据理论而提出了一种新的信任管理方案来解决主观信任问题，尽管此方案降低了功耗，但获得的节点置信度值并不太准确. 基于 D-S 证据理论的方法通常基于 mass 函数和证据之间的支持度为基础，但上述模型中构造的 mass 函数由于相互支持度的计算倾向于绝对计算，从而导致精度差和不稳定的问题. 文献[26]指出基于模糊理论进行决策时的结果更加可靠也更加符合实际. 因此基于模糊理论，为了消除网络节点信任的主观模糊性，文献[27]虽然通过使用模糊规则的方法对信任进行了数学建模，但是他们只给出了推理机制，没有给出具体的计算方法. 文献[28]提出了一种主观信任度模型，其权重随评估值而动态变化，并使用模糊决策理论提供了一种划分置信度的机制和一个完整评估机制，通过实例论证了模型的有效性和合理性. 文献[29]虽然利用 D-S 证据理论提高了信任分类的准确性，但节点的主观信任模糊性对结果造成了一定的影响. 对于问题的随机性，D-S 证据理论限制了通过收集证据得出的假设，并为信任问题的随机性提供了一种可行的方法. 对于问题的不确定性描述，模糊理论可以使用模糊隶属度函数将其分解为 D-S 证据理论的基本置信度函数，实现对证据可信度的精确描述. 因此，将模糊理论和证据理论结合起来形成模糊证据理论进行节点置信度评估是一个不错的方法，可以提高模型的有效性和准确性.

在部署物联网时，可以将信任管理机制用于评估网络节点的可信度，从而抵御来自网络内部恶意节点的攻击，保障网络运行的安全性和可靠性. 针对以上研究存在的问题，本文提出了一种基于模糊证据理论

的物联网节点评估方法. 使用模糊理论和D-S证据理论形成模糊证据理论，评估节点的整体置信度. 通过全局考虑节点的直接和间接信任度，消除恶意节点对网络中节点置信度的影响，从而确保物联网中节点的信任信息传输的安全性.

在部署物联网时，可以将信任管理机制用于评估网络节点的可信度，从而抵御来自网络内部恶意节点的攻击，保障网络运行的安全性和可靠性. 针对以上研究存在的问题，本文提出了一种基于模糊证据理论的物联网节点评估方法. 使用模糊理论和D-S证据理论形成模糊证据理论，评估节点的整体置信度. 通过全局考虑节点的直接和间接信任度，消除恶意节点对网络中节点置信度的影响，从而确保物联网中节点的信任信息传输的安全性.

2 相关理论基础

2.1 模糊理论

模糊理论是1965年由美国学者Zadeh提出的[30]，其目的是为了有效解决现实世界中大量不确定信息的问题，该理论逐渐发展为模糊数学这样一个数学分支. 由相关研究[27]可知，节点的信任关系可以分为描述对客体信任的相信关系和描述主体之间信任的主观信任. 对于网络节点之间的置信度的判定存在着人为判定的主观性以及含糊性，无法用精确语言来描述. 因此，迫切需要一种能反映实体信任的模糊性并能直观表达数量关系的描述机制. 模糊理论这样一个数学分支能很好地解决这一问题.

定义1 假设给定的论域A，其模糊子集T对任意的$A_i \in A(i=1,2,\cdots,n)$都可以确定一个数$\mu_T(A_i)\in[0,100]$来表示$A_i$属于$A$的程度. 映射$\mu_T: A\longrightarrow[0,100]$，$A_i\longrightarrow\mu_T(A_i)\in[0,100]$称为$T$的隶属度函数，$\mu_T(A_i)$称为$A$中元素对模糊子集$T$的隶属度.

一般地，论域Z中有n个模式M_1，M_2，…，M_n，有m个网络节点μ_1，μ_2，…，μ_m，那么对于任意一个识别对象x，m个网络节点分别给出它属于各个模式的隶属度矩阵如下：

$$\begin{bmatrix}\mu_{1\cdot M_1}(x) & \mu_{1\cdot M_2}(x) & \cdots & \mu_{1\cdot M_n}(x)\\ \mu_{2\cdot M_1}(x) & \mu_{2\cdot M_2}(x) & \cdots & \mu_{2\cdot M_n}(x)\\ \vdots & \vdots & & \vdots\\ \mu_{m\cdot M_1}(x) & \mu_{m\cdot M_2}(x) & \cdots & \mu_{m\cdot M_n}(x)\end{bmatrix}_{m\times n} \tag{1}$$

所以，对象x属于各个模式的基本概率分配值表示如下：

$$m_i(M_j)=\frac{\lambda_i\mu_{i\cdot M_j}(x)}{\sum_{j=1}^{n}\lambda_i\mu_{i\cdot M_j}(x)} \tag{2}$$

其中：$i=1,2,\cdots,m$，$j=1,2,\cdots,n$；$m_i(A_j)$表示第i个网络节点属于模式M_j的基本概率分配值；λ_i表示第i个网络节点被其他节点所支持的程度.

2.2 D-S证据理论

D-S证据理论[31]是建立在“识别框架Θ”上的理论，由互相排斥和有限的基本命题构成. 其中，2^Θ是Θ的幂集，它表示基于Θ的所有可能命题的集合. 我们可以定义$\{T,-T\}$为网络节点的信任状态，T和$-T$分别表示节点的可以信任和不能信任状态，则2^Θ就可以表示为$\{\varnothing,\{T\},\{-T\},\{T,-T\}\}$的集合，从而可以知道$\varnothing$表示“不可能事件”，$\{T\}$表示“节点可信状态”，$\{-T\}$表示“节点不可信状态”，$\{T,-T\}$表示“不确定状态”.

定义2 如果一个基本置信度函数$m: 2^\Theta\longrightarrow[0,1]$，则满足：$\sum_{A\subset\Theta}m(A)=1$，$A\neq\varnothing$且$m(\Phi)=0$始终成立；如果信度函数$Bel: 2^\Theta\longrightarrow[0,1]$，则满足：$Bel(A)=\sum_{B\subset\Theta}m(B)$，$\forall A\subseteq\Theta$始终成立；如果似然函数$Pl: 2^\Theta\longrightarrow[0,1]$，则满足：$Pl(A)=1-Bel(\overline{A})$，$\forall A\subseteq\Theta$始终成立.

其中，A表示为2^Θ中的任意一个命题，$m(A)$表示为A的基本置信度，即证据支持A发生的程度；

$Bel(A)$ 为 A 的信度，表示证据给予 A 的赞成程度；$Pl(A)$ 为 A 的似然度，表示证据不赞成 A 的程度.

除此之外，对一个命题的信任程度仅利用可信度函数来描述还不是很合理，须引入一个能表示怀疑 A 的程度的量，即定义一个怀疑函数 $Dou: 2^{\Theta} \longrightarrow [0, 1]$，则满足：$Dou(A)=Bel(\overline{A})$，$\forall A \subseteq \Theta$ 始终成立，其中 $Dou(A)$ 为 A 的怀疑度，表示证据怀疑 A 的程度. $[Bel(A), Pl(A)]$ 表示证据的不确定性区间，$[0, Bel(A)]$ 表示为 A 的完全可行区间，$[0, Pl(A)]$ 表示 A 的不可怀疑区间，并且 $m(A)$，$Bel(A)$，$Pl(A)$ 可以相互确定.

3　基于模糊证据理论的物联网节点评估方法

本文提出的基于模糊证据理论的物联网节点评估方法在文献[5]的基础上添加了多种置信度因子，综合考虑节点行为策略对信任值的影响. 首先，我们使用模糊集理论并添加各种置信度因子来计算网络节点的直接置信度，从而实现节点置信度等级的划分；然后由相邻节点的推荐得到该节点的间接置信度，并将 D-S 证据理论中的基本置信度函数定义为模糊隶属度函数；最后通过证据差异来修改节点的两种置信度值的权重，并依据 Dempster 组合规则对节点的置信度进行合成，以获得节点的完整置信度，其结构如图 1 所示. 该方法使用分布式算法评估节点的置信度，并定量评估网络中节点之间的置信分数，以计算每个节点的置信度. 在本文中，评估主体的节点是指评估节点，评估客体的节点是指被评估节点，评估节点与被评估节点之间互为邻居关系. 一般来讲，网络节点的置信度主要取决于主体对客体的观察还有第三方的推荐，并且其置信度会随着客体的变化而变化.

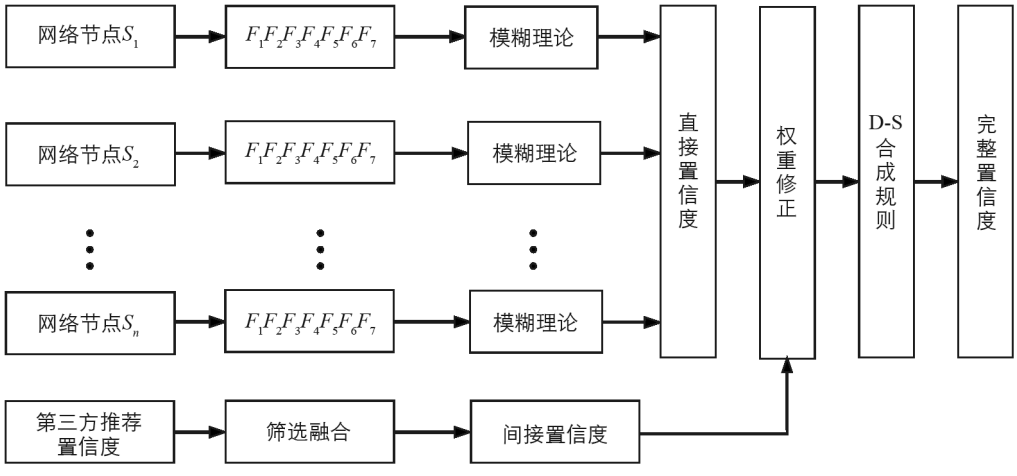


图 1　基于模糊证据理论的物联网节点评估方法结构图

3.1　节点信任计算

物联网网络节点的置信度取决于主体(评估节点)对客体(被评估节点)的观察以及第三方的推荐. 在理想情况下，通过无中心节点的信任评估机制以及邻居节点之间相互监控 f_2，f_3，f_4，可以计算节点的直接置信度，并充分考虑其他节点的推荐置信度. 网络中节点间的信任评估关系可以由图 2 具体表示.

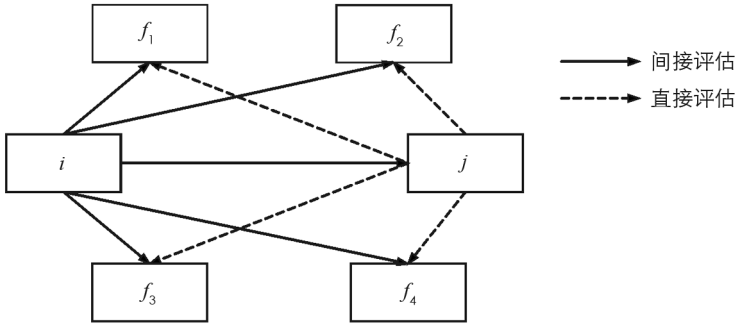


图 2　网络节点间置信度评估关系

如图2所示，节点 i 和 j 的信任评估关系是推荐信任关系，主要包括直接评估和间接评估两部分，推荐信任链是指其他节点到被评估节点的通路. 由于单个直接置信度计算和多个间接置信度计算之间是相互独立的，根据D-S证据理论中的Dempster组合规则，可以通过直接置信度和间接置信度共同获得节点的总置信度值.

因此，在利用模糊集合理论来判定节点信息时，可利用各信任评估集的隶属度来反映节点的评估信息，节点的置信因子在不同的评估集上的隶属度可以组成在该因素上的模糊向量，表示节点在该信任因素上的信任评估大小，最后根据置信因子在各信任模糊集上的隶属度大小来划分节点的信息. 为描述各节点之间的信任关系，我们根据节点之间的相互评价构建了一个模糊关系矩阵 $\boldsymbol{R}$ 来表示节点之间的信任关系：

$$\boldsymbol{R}=\begin{bmatrix} \boldsymbol{r}_{11} & \boldsymbol{r}_{12} & \cdots & \boldsymbol{r}_{1n} \\ \boldsymbol{r}_{21} & \boldsymbol{r}_{22} & \cdots & \boldsymbol{r}_{2n} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{r}_{n1} & \boldsymbol{r}_{n2} & \cdots & \boldsymbol{r}_{nn} \end{bmatrix} \tag{3}$$

其中 $\boldsymbol{r}_{ij}$ 表示节点 i 对节点 j 的信任. $\boldsymbol{r}_{ij}=(1,0,0,0)$ 时表示对节点绝对信任，$\boldsymbol{r}_{ij}=(0,0,0,0)$ 时表示节点自己对自己的信任评估，这里我们设定为无效.

另外，需要定义一个权重向量 $\boldsymbol{W}=[\omega_1,\omega_2,\omega_3,\omega_4]$ 反映对各个置信因子的关注程度，同时定义一个模糊评价子集，其元素 $T_i(i=1,2,3,4)$ 分别表示节点的信任程度为不信任、一般信任、非常信任、完全信任. 权重向量和模糊关系矩阵由合适的模糊合成算子组合在一起，以获得每个评估对象的模糊评估结果，计算过程如下所示：

$$\boldsymbol{P}=\boldsymbol{W}\cdot\boldsymbol{R}=[p_1,\ p_2,\ p_3,\ p_4] \tag{4}$$

其中：$\boldsymbol{P}_i$ 表示物联网网络信任评分的模糊子集 U_i 中被评估节点的隶属程度，$\boldsymbol{W}$ 为权重向量，$\cdot$ 为模糊合成算子，$\boldsymbol{R}$ 为节点之间的模糊关系矩阵.

我们通过模糊子集 $T_j(j=1,2,3,4)$ 定义不同信任集合时，采用离散标度$\{1,2,\cdots,M\}$来描述实体信任的等级

$$\begin{cases} T_1 \text{ 表示“不信任”} & \mu_T(A)\in[0,25) \\ T_2 \text{ 表示“有点信任”} & \mu_T(A)\in[25,50) \\ T_3 \text{ 表示“一般信任”} & \mu_T(A)\in[50,75) \\ T_4 \text{ 表示“完全信任”} & \mu_T(A)\in[75,100) \end{cases} \tag{5}$$

在实际的评估过程中，实体的信任度对某个 $T_a(a=1,2,3,4)$ 的隶属关系可以通过信任隶属度函数 $\mu_T(A)$ 的某个区间进行判断. 为了便于利用数值直接进行评估，我们通过引入定量化处理，根据节点各个信任等级进行百分制计分. 例如，可以用 $0\leqslant\mu_{T_1}<25$(不信任)，$25\leqslant\mu_{T_2}<50$(一般信任)，$50\leqslant\mu_{T_3}<75$(非常信任)，$75\leqslant\mu_{T_4}<100$(完全信任) 表示信任等级. 从而得到信任等级分数向量 $\boldsymbol{C}=(\mu_{T_1},\mu_{T_2},\mu_{T_3},\mu_{T_4})$，基于此计算得分 S 如下所示：

$$S=\frac{\boldsymbol{T}\boldsymbol{C}^{\mathrm{T}}}{\sum_{i=1}^{4}T_i}=\frac{\sum_{i=1}^{4}T_i\mu_{Ti}}{\sum_{i=1}^{4}T_i} \tag{6}$$

由于节点信任等级处于一个区间内，为准确表示节点所归属的信任区间，我们选择一个代表性分数

$$S'=\frac{\sum_{i=1}^{4}T_i\mu'_{Ti}}{\sum_{i=1}^{4}T_i} \tag{7}$$

其中 μ'_{T_i} 为各信任区间的中间值组成的兴奋等级分数，可以表示为$(\mu'_{T_1},\mu'_{T_2},\mu'_{T_3},\mu'_{T_4})=(12.50,37.50,62.50,87.50)$. 举例说明如下：假设某一节点的信任分数向量表示为 $\boldsymbol{E}=(0.20,0.25,0.25,0.30)$，则有

$$S'=\frac{(0.20,0.25,0.25,0.30)\cdot(12.50,37.50,62.50,87.50)^{\mathrm{T}}}{0.20+0.25+0.25+0.30}=54.17 \tag{8}$$

因为 $50 \leqslant 54.17 < 75$，故该节点的信任等级为“非常信任”. 因此，在模糊集的基础上来进行定量描述，不仅没有丢失节点信任的模糊信息，反而综合各等级因素，使得评估结果更具直观性. 有点信任和一般信任的信任等级状态均不是十分确定的状态，因此可以将这两种信任状态合并为一种不确定状态对节点进行判定.

因此，我们将信任的模糊分类表示为不信任、不确定和完全信任 3 类信任状态. 根据这 3 个信任等级，在节点信任值区间[0，1] 构造 3 个模糊子集 T_1, T_2, T_3，其隶属度函数分别为 $\mu_1(t), _2(t), \mu_3(t)$，且有 $\mu_1(t)+\mu_2(t)+\mu_3(t)=1$.

3.2　直接置信度的计算

物联网中存在各种类型的攻击，所以在计算节点信任度时，必须充分考虑多种置信因子，以获得更加精确的信任值. 物联网中的节点能量都极其有限，为保障数据的正确发送，需要在侦听和传输数据时进行中继，因此，可以通过分析节点的数据成功发送率 F_1 来分析和判断节点是否受到攻击；当一个节点的数据包发送到下一个节点时，源节点会在一定时间内监控数据包是否被篡改，确保节点的数据完整性 F_2 对于节点的传输安全具有重要作用；当物联网的网络信道处于极端恶劣的环境时，节点可能会无法使用，因而需要通过发送和检查节点的数据可用性 F_3 来证明被评估的节点；如果节点确定被评估节点发送了多少公共 ACK 分组，就可以得到被评估节点的数据接收分组率 F_4，因而根据比值的变化情况可以知道节点是否存在伪造行为；由于大多数节点不可能直接与基站进行通信，因此节点对于数据的转发率 F_5 也能反映出节点的信任值. 另外，节点的信任值在时间和空间上存在关联，也即节点的信任值会在之前基础上发生变化，因此时间因素 F_6 对节点信任值有重要影响. 时间等级的大小取决于具体情况，我们基于网络安全程度的规则，当安全度较高时取 $F_6=0.8$，相对较低时取 $F_6=0.2$，一般正常情况下取 $F_6=0.5$. 在物联网的网络中会有不同的环境和应用场景，从而也会区分不同的安全等级 F_7，当安全等级较高时取 $F_7=3$，相对较低时取 $F_7=1$，一般正常情况下取 $F_7=2$. 因此，本文从信任准确性和反映攻击行为的角度选取 7 个置信因子，包括数据成功发送率、数据完整性、数据可用性、数据接收分组率、数据转发率，时间因素、安全等级，分别用 $F_1, F_2, F_3, F_4, F_5, F_6, F_7$ 表示：

$$F_1=\frac{ACK_{i,j}(t)}{TP_{i,j}(t)} \tag{9}$$

$$F_2=\frac{IP_{i,j}(t)}{FP_{i,j}(t)} \tag{10}$$

$$F_3=\frac{RACK_{i,j}(t)}{RACK_{i,j}(t)+NRACK_{i,j}(t)} \tag{11}$$

$$F_4=\frac{RP_{i,j}(t)-RP_{i,j}(t-1)}{RP_{i,j}(t)+RP_{i,j}(t-1)} \tag{12}$$

$$F_5=\frac{FP_{i,j}(t)-FP_{i,j}(t-1)}{FP_{i,j}(t)+FP_{i,j}(t-1)} \tag{13}$$

其中：F_1 表示数据发送率因子，$ACK_{i,j}(t)$ 表示相邻节点之间转发成功的数据包数目，$TP_{i,j}(t)$ 是节点所要求转发的数据包数目；F_2 表示数据完整性因子，$IP_{i,j}(t)$ 表示没有被篡改并成功发送的数据包数目，$FP_{i,j}(t)$ 表示需要发送的数据包数目；F_3 表示数据可用性因子，$RACK_{i,j}(t)$ 表示被响应的数据包数目，$NRACK_{i,j}(t)$ 表示未被响应的数据包数目；F_4 表示数据接收分组率因子，$RP_{i,j}(t)$ 表示接收分组的数据包数目，$RP_{i,j}(t-1)$ 表示上一个时刻接收的分组数据包数目；F_5 表示数据转发率因子，$FP_{i,j}(t)$ 表示节点传输分组的数量，$FP_{i,j}(t-1)$ 表示上一时刻节点传输分组的数量.

为了保证信任评估方法的合理性，在不同的时间内设置不同的参数，因为不同的节点交互次数中成功交互所占的比例的物理意义不一样. 我们定义该参数如下：

$$\eta=\frac{\dfrac{SR_{i,j}(t)}{FR_{i,j}(t)+SR_{i,j}(t)}}{\dfrac{SR_{i,j}(t-1)}{FR_{i,j}(t-1)+SR_{i,j}(t-1)}} \tag{14}$$

其中：$SR_{i,j}(t)$表示成功交互的次数，$FR_{i,j}(t)$表示失败次数，$SR_{i,j}(t-1)$表示上一时刻成功交互的次数，$FR_{i,j}(t-1)$表示上一时刻失败的次数.

假设节点i对节点j发起信任评估，评估节点i采用加权的方式计算被评估节点j的直接置信度，则节点i对节点j在当前时刻的直接置信度由以下式子计算：

$$NDT_{i,j}^{\boldsymbol{D}}(t)=\eta^{F_7}\times F_6\times(w_1F_1+w_2F_2+w_3F_3+w_4F_4+w_5F_5) \tag{15}$$

其中：$\boldsymbol{D}$表示直接置信度向量；w_1,w_2,w_3,w_4,w_5为置信因子的权重系数并且满足$w_1+w_2+w_3+w_4+w_5=1$. 本文将权重系数分别设置为$w_1=w_2=w_3=w_4=w_5=0.2$.

但是，在物联网中的节点还会受到防御开关的攻击，这会对节点的直接置信度造成一定影响. 为了消除此类影响，基于历史直接置信度对上述计算的直接置信度进行修正，修正后的直接置信度表示为：

$$DT_{i,j}^{\boldsymbol{D}}(t)=\alpha NDT_{i,j}^{\boldsymbol{D}}(t)+(1-\alpha)FDT_{i,j}^{\boldsymbol{D}}(t) \tag{16}$$

其中：$NDT_{i,j}^{\boldsymbol{D}}(t)$表示未校正的直接置信度，$FDT_{i,j}^{\boldsymbol{D}}(t)$表示上一个更新周期的历史直接置信度，$\alpha$表示为权衡当前信任度和历史信任度的自适应因子，定义为：

$$\alpha=\begin{cases}\xi_1 & NDT_{i,j}^{\boldsymbol{D}}(t)\geqslant FDT_{i,j}^{\boldsymbol{D}}(t)\\ \xi_2 & NDT_{i,j}^{\boldsymbol{D}}(t)<FDT_{i,j}^{\boldsymbol{D}}(t)\end{cases} \tag{17}$$

其中$0<\xi_1<\xi_2<1$. ξ_1取值较小，是为了防止恶意节点通过伪装欺骗等恶意行为积累自身的信任值，而ξ_2取值较大，是为了体现出对节点恶意行为的处罚以保证节点信任值的准确性.

3.3 间接置信度的推荐

网络节点的间接置信度主要是通过查询第三方节点获得的. 通常，将第三方节点k在要评估的节点j上的直接置信度称为该节点的间接置信度. 间接置信度的推荐原理如图3所示. 两个节点之间存在间接置信度的条件是它们同时具有一个公共的邻居节点，即只有评估节点i和被评估节点j共同的邻居节点k,l才有间接置信度. 我们令$\boldsymbol{IT}_{k,j}$是节点k对节点j的间接置信度，$\boldsymbol{IT}_{l,j}$是节点l对节点j的间接置信度，当节点k,l在收到来自评估节点的查询请求后，就直接将自己对被评估节点j的直接置信度$\boldsymbol{DT}_{k,j}$和$\boldsymbol{DT}_{l,j}$作为间接置信度$\boldsymbol{IT}_{k,j}$和$\boldsymbol{IT}_{l,j}$推荐给节点i，得到间接置信度.

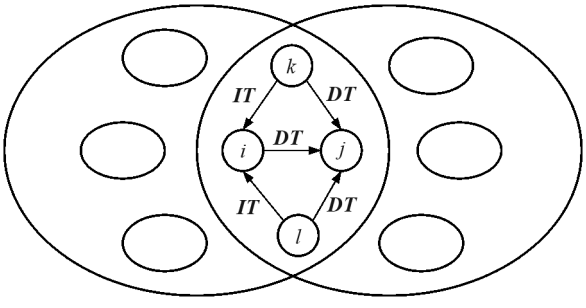


图3 间接置信度推荐示意图

在本文中，我们在计算节点的间接置信度时，首先对节点收集到的推荐信任进行过滤，然后为推荐信任分配权重信息，再计算节点的间接置信度，计算过程表示如下：

$$IT_{i,j}^{\boldsymbol{I}}(t)=\sum\nolimits_{k\in C}\eta_k\times RT_{i,j}^{k}(t) \tag{18}$$

$$RT_{i,j}^{k}(t)=DT_{i,k}^{\boldsymbol{D}}(t)\times DT_{k,j}^{\boldsymbol{D}}(t) \tag{19}$$

其中：上标$\boldsymbol{I}$表示间接置信度向量，η_k表示某一共同节点k的权重，$RT_{i,j}^{k}(t)$表示相邻节点k对j的推荐置信度，$DT_{i,k}^{\boldsymbol{D}}(t)$表示节点$i$对节点$k$的直接置信度，$DT_{k,j}^{\boldsymbol{D}}(t)$表示节点$k$对节点$j$的直接置信度.

但是，由于网络存在各种攻击类型，节点的推荐置信度可能存在一定的偏离度，如果偏离度过大，则要将其舍去，避免对节点的间接置信度产生影响. 节点i的某一个共同邻居节点k的推荐信任偏离度d_k可以表示为：

$$d_k=\frac{1}{n-1}\sum\nolimits_{l=1,\,l\neq k}^{n}\sqrt{\left[RT_{i,j}^{k}(t)-RT_{i,j}^{l}(t)\right]^2} \tag{20}$$

其中：如果 d_k 的值越大，则节点 k 的推荐置信度就越有可能是恶意节点操作的虚假推荐，可行性越低. 为保证推荐信任的可靠性，本文设置偏离度阈值 $\tau=0.2$，如果 $d_k>\tau$，则舍去，如果 $d_k<\tau$，则存入集合 C 中.

在物联网网络中，节点的部署通常较为密集且随机分布，从而会出现没有共同节点的情况(如图 4 所示)，这时节点 p 就无法获取对节点 j 的间接置信度. 因此，节点 p 就不再进行间接置信度的计算，而是直接将其直接置信度 $DT_{p,j}$ 作为对节点 j 的完整置信度.

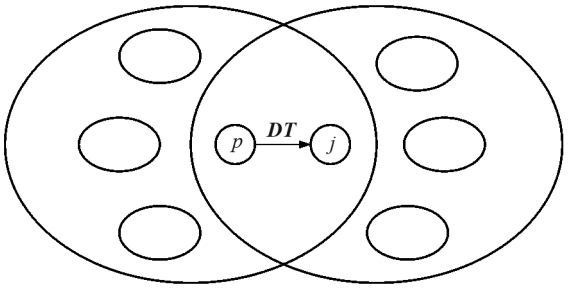


图 4　置信度推荐的特殊情况

3.4　完整置信度的计算

3.4.1　置信度的表示

为了识别网络中的恶意节点的行为，通常将节点的直接置信度和间接置信度联合考虑后得到的节点的完整置信度更具有可靠性，主要是因为在节点完整置信度的计算过程中包含多个评价指标的有效信息. 网络中的节点在计算直接置信度和间接置信度的时候存在一定的信任主观模糊性，导致对节点信任信息造成一定的影响. 因此，可以使用模糊理论中的模糊隶属度函数根据 3 种置信状态“完全不可信”“不确定”和“完全可信”来计算节点 i 的隶属度，并将其直接置信度 $\boldsymbol{DT}_{i,j}$ 的隶属度 $\mu_1^{\boldsymbol{D}}$，$\mu_2^{\boldsymbol{D}}$，$\mu_3^{\boldsymbol{D}}$，间接置信度 $\boldsymbol{IT}_{k,j}$ 的隶属度 $\mu_1^{\boldsymbol{I}}$，$\mu_2^{\boldsymbol{I}}$，$\mu_3^{\boldsymbol{I}}$ 分别表示如下：

$$\begin{cases}\mu_1^{\boldsymbol{D}}=\mu_1(\boldsymbol{DT}_{i,j})\\ \mu_2^{\boldsymbol{D}}=\mu_2(\boldsymbol{DT}_{i,j})\\ \mu_3^{\boldsymbol{D}}=\mu_3(\boldsymbol{DT}_{i,j})\end{cases},\quad \begin{cases}\mu_1^{\boldsymbol{I}}=\mu_1(\boldsymbol{IT}_{i,j})\\ \mu_2^{\boldsymbol{I}}=\mu_2(\boldsymbol{IT}_{i,j})\\ \mu_3^{\boldsymbol{I}}=\mu_3(\boldsymbol{IT}_{i,j})\end{cases}\tag{21}$$

其中：

$$\begin{cases}\boldsymbol{DT}_{i,j}^1=(\boldsymbol{h}_{i,j}^1(\{T\}),\boldsymbol{h}_{i,j}^1(\{T,-T\}),\boldsymbol{h}_{i,j}^1(\{-T\}))\\ \boldsymbol{DT}_{i,j}^2=(\boldsymbol{h}_{i,j}^2(\{T\}),\boldsymbol{h}_{i,j}^2(\{T,-T\}),\boldsymbol{h}_{i,j}^2(\{-T\}))\\ \cdots\\ \boldsymbol{DT}_{i,j}^q=(\boldsymbol{h}_{i,j}^q(\{T\}),\boldsymbol{h}_{i,j}^q(\{T,-T\}),\boldsymbol{h}_{i,j}^q(\{-T\}))\\ \boldsymbol{DT}_{i,j}^{\boldsymbol{D}}=(\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{T\}),\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{T,-T\}),\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{-T\}))\end{cases},\quad \begin{cases}\boldsymbol{IT}_{i,j}^1=(\boldsymbol{h}_{i,j}^1(\{T\}),\boldsymbol{h}_{i,j}^1(\{T,-T\}),\boldsymbol{h}_{i,j}^1(\{-T\}))\\ \boldsymbol{IT}_{i,j}^2=(\boldsymbol{h}_{i,j}^2(\{T\}),\boldsymbol{h}_{i,j}^2(\{T,-T\}),\boldsymbol{h}_{i,j}^2(\{-T\}))\\ \cdots\\ \boldsymbol{IT}_{i,j}^q=(\boldsymbol{h}_{i,j}^q(\{T\}),\boldsymbol{h}_{i,j}^q(\{T,-T\}),\boldsymbol{h}_{i,j}^q(\{-T\}))\\ \boldsymbol{IT}_{i,j}^{\boldsymbol{I}}=(\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{T\}),\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{T,-T\}),\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{-T\}))\end{cases}\tag{22}$$

通过将$\{-T\}$，$\{T,-T\}$，$\{T\}$分别作为节点分类隶属度函数的基本置信度函数，根据 D-S证据理论，μ_1 代表“完全不可信任”状态的认可程度、μ_2 代表“无法确定信任”状态的认可程度、μ_3 代表“完全可以信任”状态的认可程度，那么在直接置信度中就有 $\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{T\})$ 和 $\mu_1^{\boldsymbol{D}}$ 相等、$\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{T,-T\})$ 和 $\mu_2^{\boldsymbol{D}}$ 相等、$\boldsymbol{h}_{i,j}^{\boldsymbol{D}}(\{-T\})$ 和 $\mu_3^{\boldsymbol{D}}$ 相等，类似地，间接置信度中就有 $\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{T\})$ 和 $\mu_1^{\boldsymbol{I}}$ 相等、$\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{T,-T\})$ 和 $\mu_2^{\boldsymbol{I}}$ 相等、$\boldsymbol{h}_{i,j}^{\boldsymbol{I}}(\{-T\})$ 和 $\mu_3^{\boldsymbol{I}}$ 相等. 因此，综合前两节的直接置信度、间接置信度，得到节点 i 对 j 的当前完整置信度表示为

$$CT_{i,j}^c(t)=\varphi\times DT_{i,j}^{\boldsymbol{D}}(t)+\theta\times IT_{i,j}^{\boldsymbol{I}}(t)\tag{23}$$

其中：$DT_{i,j}^{\boldsymbol{D}}(t)$ 为节点 i 对节点 j 的直接置信度；$IT_{i,j}^{\boldsymbol{I}}(t)$ 为节点 i 对节点 j 的间接置信度；φ，θ 分别是直接置信度和间接置信度的权值，并且满足 $\varphi+\theta=1$. 本文设置 $\varphi=\theta=0.5$.

3.4.2　置信度的修正

在物联网网络中评估节点可能会收到不正确的推荐信息，并且评估节点本身也可能会受到网络环境的

影响而给出不正确的置信度. 当使用直接和间接置信度计算完整置信度时，也存在权重分配的问题. 基于此，在修改直接置信度和间接置信度时，我们使用测量证据距离的方法来分配权重，从而获得更合理的节点完整置信度.

我们将节点 i 收到节点 $k(k=1,2,\cdots,q)$ 关于节点 j 的 q 个间接置信度 $IT_{i,j}^{I}=(\boldsymbol{h}_{i,j}^{I}(\{T\}),\boldsymbol{h}_{i,j}^{I}(\{T,-T\}),\boldsymbol{h}_{i,j}^{I}(\{-T\}))$ 称为节点 i 关于节点 j 的完整置信度的第 $1,2,\cdots,q$ 个子置信度，同样地，节点 i 关于节点 j 的直接置信度 $DT_{i,j}^{D}=(\boldsymbol{h}_{i,j}^{D}(\{T\}),\boldsymbol{h}_{i,j}^{D}(\{T,-T\}),\boldsymbol{h}_{i,j}^{D}(\{-T\}))$ 称为第 $q+1$ 个子置信度. 为了表达任意两个证据之间的冲突程度，我们使用证据距离公式获得这 $q+1$ 个子置信度之间的距离：

$$l_{u,v}=\sqrt{\frac{1}{2}(\|\overrightarrow{\boldsymbol{h}_{u,j}}\|)^2+(\|\overrightarrow{\boldsymbol{h}_{v,j}}\|)^2-2\times(\overrightarrow{\boldsymbol{h}_{u,j}},\overrightarrow{\boldsymbol{h}_{v,j}})} \tag{24}$$

其中：$\overrightarrow{\boldsymbol{h}_{u,j}}$ 表示第 u 个子置信度向量，$\overrightarrow{\boldsymbol{h}_{v,j}}$ 表示为第 v 个子置信度向量；$\|\overrightarrow{\boldsymbol{h}_{u,j}}\|$，$\|\overrightarrow{\boldsymbol{h}_{v,j}}\|$ 分别表示子置信度的模；$(\overrightarrow{\boldsymbol{h}_{u,j}},\overrightarrow{\boldsymbol{h}_{v,j}})$ 表示这两个子置信度向量的内积；$u,v=1,2,\cdots,q+1$.

因此，证据之间的相互支持程度可以表示为任意两个子置信度之间的相似度 $s_{u,v}=1-l_{u,v}$，相似度矩阵 $\boldsymbol{S}$ 表示如下：

$$\boldsymbol{S}=\begin{bmatrix}1 & s_{1,2} & \cdots & s_{1,q+1}\\ s_{2,1} & 1 & \cdots & s_{2,q+1}\\ \vdots & \vdots & \vdots & \vdots\\ s_{q+1,1} & s_{q+1,2} & \cdots & 1\end{bmatrix}_{(q+1)\times(q+1)} \tag{25}$$

根据相似度矩阵知，若一个证据与其他大多数证据相似度越高，则其得到的支持度也越高，也就是说该证据对最终的结果影响也比较大. 设第 u 个子置信度的综合支持度为 SP_u，则 SP_u 的计算如下所示：

$$SP_u=\sum_{v=1,\,u\neq v}^{q+1}s_{u,v} \tag{26}$$

设第 u 个子置信度的相对权重为 λ_u，则有：

$$\lambda_u=\frac{SP_u}{\sum_{u=1}^{q+1}\sum_{v=1,\,u\neq v}^{q+1}s_{u,v}} \tag{27}$$

因此，节点 i 可以根据式(27)的相对权重对每个子置信度中的基本置信度进行修正，修正过程如下：

$$\begin{cases}\boldsymbol{h}'_{u,j}(\{T\})=\lambda_u\boldsymbol{h}_{i,j}^{u}(\{T\})\\ \boldsymbol{h}'_{u,j}(\{T,-T\})=\lambda_u\boldsymbol{h}_{i,j}^{u}(\{T,-T\})\\ \boldsymbol{h}'_{u,j}(\{-T\})=\lambda_u\boldsymbol{h}_{i,j}^{u}(\{-T\})\end{cases} \tag{28}$$

3.4.3 置信度的综合

根据 Dempster 组合规则，节点 i 关于节点 j 的完整置信度 $\boldsymbol{VT}_{i,j}$ 可以由下式进行融合得到：

$$\boldsymbol{VT}_{i,j}=(\boldsymbol{h}_{i,j}^{V}(\{T\}),\boldsymbol{h}_{i,j}^{V}(\{T,-T\}),\boldsymbol{h}_{i,j}^{V}(\{-T\}))$$

组合规则如下所示：

$$\begin{cases}\boldsymbol{h}_{i,j}(A)=\boldsymbol{h}'_{1,j}(A)\oplus\boldsymbol{h}'_{2,j}(A)\oplus\cdots\oplus\boldsymbol{h}'_{q+1,j}(A),\ A\neq\Phi,\ A\subseteq\Theta\\ \boldsymbol{h}_{i,j}(\Phi)=0\end{cases} \tag{29}$$

如果节点 j 满足以下条件：

$$\begin{cases}\boldsymbol{h}_{i,j}(\{T\})-\boldsymbol{h}_{i,j}(\{-T\})>\alpha_1\\ \boldsymbol{h}_{i,j}(\{T,-T\})<\beta\\ \boldsymbol{h}_{i,j}(\{T\})>\boldsymbol{h}_{i,j}(\{T,-T\})\end{cases} \tag{30}$$

则节点 i 认为节点 j 是值得信任的，并将节点 j 添加到其可行性列表中；相反，当 $\boldsymbol{h}_{i,j}(\{T\})-\boldsymbol{h}_{i,j}(\{-T\})<\alpha_2$ 时，则认为节点 j 是不值得信任的或者不确定信任状态的节点，从而拒绝与其通信. 其中，α_1,α_2 分别表示节点可信和不可信时，$\{T\}$ 与 $\{-T\}$ 基本置信度差的阈值，β 表示 $\{T\}$ 或 $\{-T\}$ 命题成立时中性证据区间的上限值.

4　实验结果分析

4.1　实验参数设置

本文利用 NS2 仿真工具进行仿真实验，以分析所提出的节点置信度评估方法的性能. 在 100 m×100 m 的正方形区域进行仿真实验，并且该区域内有 100 个节点遵循随机分布，其数据的传输速率设置为 60 bit. 在不验证恶意节点比例对信任值的影响时，我们将恶意节点均设置为节点数量的 10%，通信半径设置为 20 m. 同时，为模拟网络中由于恶意节点造成的数据异常，设置数据丢包率和数据包篡改率均为[0.7，1]上的随机数，并将节点直接置信度的更新周期设置为 10s，为了使节点能够实现合理分类，其信任分类的阈值设置为：$\alpha_1=0.3$，$\alpha_2=-0.3$，$\beta=0.09$. 有些参数会根据实验目标的不同而改变，从而达到合理的效果，这些参数会在实验中再次进行说明.

4.2　动态适应性分析实验

只有信任评估的方法具有更好的动态适应性，才能正确识别恶意节点的攻击行为. 由于网络的正常节点很容易在物联网的网络环境中受到攻击，从而危及整个网络的安全性. 除此之外，一些恶意节点为了不被发现会通过一些隐蔽性方法来对网络发起攻击，对于这种恶意节点的准确识别就需要节点评估的方法具备良好的动态适应性. 在仿真实验中，我们为了验证该方法的动态适应性，模拟了恶意节点的隐蔽性攻击行为，并对其直接置信度进行了采样. 实验过程中，将采样的周期定义为 $T_s=10$ s，在 0～20 个周期内，目标节点提供正常服务，从第 21 个周期开始，将 20%的节点设置为恶意节点，产生随机性的选择性丢包、转发重复的分组数据等恶意行为，图 5 显示了采样的结果. 在网络运行的初始阶段，网络中的恶意节点首先对信任进行补偿，以便获得更好的分数来实现欺骗模型的目标. 如图 5 所示，网络中的恶意节点从第 21 个采样周期开始对网络进行恶意攻击，原因是当恶意节点发起攻击时，其置信度就会快速下降，图中刚好在第 21 个采样周期时，置信度出现骤降的趋势. 另外，从图中可以明确，在采样周期的前期阶段，即信任补偿阶段，$m(\{T\})$以较慢速度增加，$m(\{-T\})$以较慢速度减少，当恶意节点开始发起恶意攻击时，$m(\{T\})$迅速降低，$m(\{-T\})$迅速增加，这也就是说，这时的置信度积累花费的时间比置信度消失的时间长得多，体现了节点的置信度很难获得但极其容易失去的特点，同时也证明了本文提出的节点信任评估方法表现出了高度的敏感性.

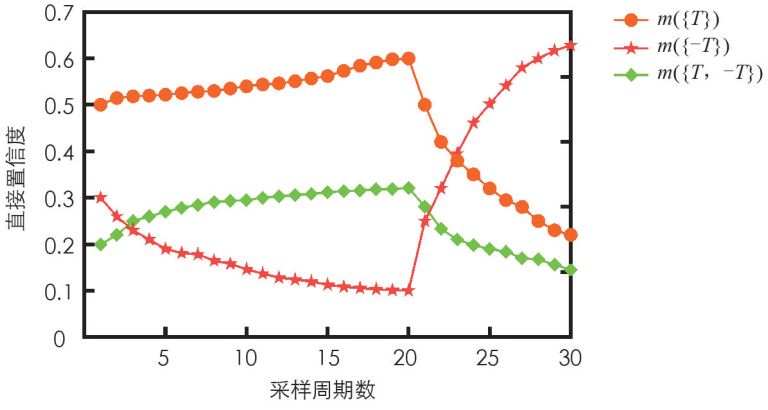
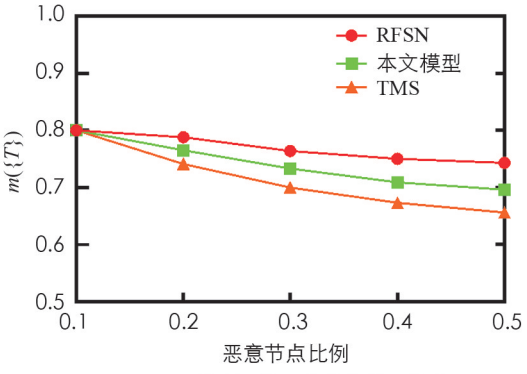


图 5　隐蔽性攻击的恶意节点的直接置信度变化

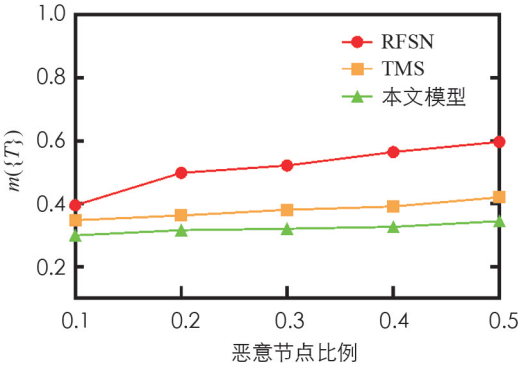
4.3　鲁棒性分析实验

网络中的恶意节点可能创建虚假信任以抹黑正常节点或吹捧恶意节点的方式实现对网络的攻击效果. 为此我们将诋毁正常节点的这一类恶意节点称为 A 类恶意节点，吹捧同伙的这一类恶意节点称为 B 类恶意节点. 为解决此问题，我们通过比较子置信度和所有其他子置信度之间的相似度并使用证据距离来校正置信度以确定节点的可靠性，即如果存在某个子置信度，则将该值与其他所有子置信度进行比较，相似度

越高，它所获得的支持度就越高，在集成节点完整置信度的过程中所占的比例也就越高，从而减少了推荐信任对恶意节点完整置信度的影响. 在实验中，我们模拟了物联网中恶意节点推荐行为的场景，分别在仿真网络中将A，B两类恶意节点的比例设置为10%，20%，30%，40%，50%，计算各类方法得到的目标节点的完整置信度. 同时，根据计算得到的置信度值选择相应的服务节点，没有推荐行为的节点则随机选择节点进行交互. 为了分析本文方法的鲁棒性方面的性能，将本文提出的节点评估方法与RFSN方法、TMS方法分别进行对比，结果见图6. 从图6(a)中可以发现，当网络中恶意节点发起攻击时，RFSN方法的置信度会缓慢下降但幅度较小，本文方法的置信度比RFSN方法影响大，比TMS方法影响小，TMS方法中节点的置信度下降幅度最大，表示受到的影响也最大. 出现这种结果的主要原因是在RFSN方法中，节点只采纳其他节点的善意推荐，而对于其他节点的恶意推荐重视不够，因而这样计算得出的置信度就会不够全面，缺乏一定的客观性，从而对节点置信度的影响较小. 而我们提出的方法通过对完整置信度的修正，基于权重的分配对恶意节点的推荐置信度进行阈值判定，从而减少恶意节点对结果的影响. 从图6(b)中可以看出，RFSN方法对恶意节点吹捧时的置信度影响也最小，因而也不能有效抑制恶意节点对其他节点的鼓吹影响. 通过对比本文方法和TMS方法，可以发现本文提出的方法在恶意节点攻击正常节点和鼓吹同伙的两种情形下，性能都略强于TMS方法，其主要原因在于本文的方法综合考虑了直接置信度和间接置信度，并通过D-S证据理论对直接置信度和间接置信度做了基于权重的修正，从而计算得到的节点的完整置信度更为客观、精确. 这同时也说明了我们提出的方法在物联网网络的恶意攻击中具有较好的鲁棒性.



(a) 不同比例A类恶意节点的置信度



(b) 不同比例B类恶意节点的置信度

图6 不同比例的恶意节点在不同情况下的置信度

4.4 网络安全性分析实验

物联网网络面临的各类攻击都是为了破坏网络的安全性，以便达到自己的目的. 在实验过程中，为对本文提出方法的网络安全性进行分析，我们将网络运行时间设置为0～50 s，通过在该网络运行时间内对恶意节点的所占比例进行检测，并将本文方法与RFSN,TMS方法进行对比，检测结果如图7所示. 物联网网络中信任评估方法的安全性很大程度上依靠恶意节点的检测率来进行评估，检测率高说明信任评估方法具有敏感性，能及时识别网络中的恶意节点，从而保障网络的安全. 从图7中可以看出，本文方法的恶意节点检测率明显优于对比方法，且趋于平稳，主要原因可能是本文方法引入了多种置信因子，从多个角度考虑综合计算节点的直接置信度，利用模糊理论对节点的置信状态进行了精确描述，从而实现节点的划分，并利用模糊理论和证据理论相融合的方法，避免了人为判定的主观假设性，在一定程度上提高了节点置信度评估的客观性. 另外，本文

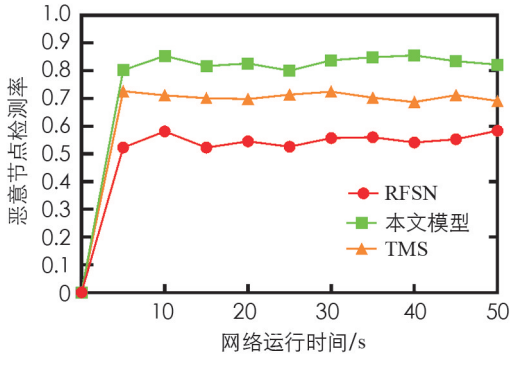


图7 恶意节点检测率

提出的方法通过权重分布修正了节点的直接置信度和间接置信度，并使用 D-S 证据理论的 Dempster 组合规则综合节点的完整置信度，加快了信任的融合. 因此，该方法在一定程度上提高了准确性和鲁棒性，同时，也表明该方法可以准确地识别恶意节点，提高网络安全性.

5　结论

本文提出了一种基于模糊证据理论的物联网节点评估方法. 首先，我们使用模糊集理论并添加多种置信度因子来计算网络节点的直接置信度，从而实现节点置信度等级的划分；然后由相邻节点的推荐得到该节点的间接置信度，并将 D-S 证据理论中的基本置信度函数定义为模糊隶属度函数；最后通过证据差异来修改节点的两种置信度值的权重，并依据 Dempster 组合规则对节点的置信度进行合成，以获得节点的完整置信度. 仿真实验表明，该方法与同类方法相比，在网络的动态适应性、鲁棒性和安全性方面，均具有更好的性能和更高的准确性以及可信度，能及时准确地发现恶意节点，提高网络的安全性. 但是本文仍存在一些不足的地方，比如没有考虑物联网中各设备间的合作方式，因此在未来的研究工作中，将考虑节点之间的合作方式来进一步优化节点的信任评估方法，以提高网络应对恶意节点攻击的能力.

参考文献：

[1] 余文科，程媛，李芳，等. 物联网技术发展分析与建议 [J]. 物联网学报，2020，4(4)：105-109.

[2] 杨洋，陈红军. 隐私保护数据挖掘技术研究综述 [J]. 微型电脑应用，2020，36(8)：41-44，54.

[3] LI X Y，ZHOU F，DU J P. LDTS：a Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks [J]. IEEE Transactions on Information Forensics and Security，2013，8(6)：924-935.

[4] GOVINDAN K，MOHAPATRA P. Trust Computations and Trust Dynamics in Mobile Adhoc Networks：a Survey [J]. IEEE Communications Surveys & Tutorials，2012，14(2)：279-298.

[5] 周治平，赵晓晓，邵楠楠. 结合模糊集合与 D-S 证据理论的 WSN 信任评估模型 [J]. 系统仿真学报，2018，30(4)：1229-1236.

[6] DUAN J Q，GAO D Y，YANG D，et al. An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications [J]. IEEE Internet of Things Journal，2014，1(1)：58-69.

[7] YU H，SHEN Z Q，MIAO C Y，et al. A Survey of Trust and Reputation Management Systems in Wireless Communications [J]. Proceedings of the IEEE，2010，98(10)：1755-1772.

[8] VILJANEN L . Towards an Ontology of Trust[C]// International Conference on Trust. Berlin：Springer，2005.

[9] FANG W D，ZHANG W X，CHEN W，et al. TMSRS：Trust Management-Based Secure Routing Scheme in Industrial Wireless Sensor Network with Fog Computing [J]. Wireless Networks，2020，26(5)：3169-3182.

[10] ABDLRAZAQ A，VAROL S. A Trust Management Model for IoT [C]//2019 7th International Symposium on Digital Forensics and Security (ISDFS). New York：IEEE Press，2019：1-6.

[11] YE Z W，WEN T，LIU Z Y，et al. An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks [J]. Journal of Sensors，2017，2017：7864671.

[12] SUN N，XU J H，WEI H L，et al. A Network State Based Reliability Evaluation Model for WSNS [C]//2017 18th IEEE/ACIS International Conference on Software Engineering，Artificial Intelligence，Networking and Parallel/Distributed Computing (SNPD). New York：IEEE Press，2017：303-308.

[13] HE D J，CHEN C，CHAN S，et al. A Distributed Trust Evaluation Model and Its Application Scenarios for Medical Sensor Networks [J]. IEEE Transactions on Information Technology in Biomedicine：a Publication of the IEEE Engineering in Medicine and Biology Society，2012，16(6)：1164-1175.

[14] 刘宴兵，龚雪红，冯艳芬. 基于物联网节点行为检测的信任评估方法 [J]. 通信学报，2014，35(5)：8-15.

[15] AYDAY E，FEKRI F. An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks [J]. IEEE Transactions on Mobile Computing，2012，11(9)：1514-1531.

[16] ZHOU H，WU Y M，FENG L，et al. A Security Mechanism for Cluster-Based WSN Against Selective Forwarding [J].

Sensors (Basel, Switzerland), 2016, 16(9): 1537.

[17] FERNANDEZ-GAGO C, MOYANO F, LOPEZ J. Modelling Trust Dynamics in the Internet of Things [J]. Information Sciences, 2017, 396: 72-82.

[18] PAL S, HITCHENS M, VARADHARAJAN V. Towards the Design of a Trust Management Framework for the Internet of Things [C]//2019 13th International Conference on Sensing Technology (ICST). New York: IEEE Press, 2019: 1-7.

[19] LUECKING M, FRIES C, LAMBERTI R, et al. Decentralized Identity and Trust Management Framework for Internet of Things [C]//2020 IEEE International Conference on Blockchain and Cryptocurrency. New York: IEEE Press, 2020: 1-9.

[20] 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.

[21] 徐欢, 夏浩军, 李孟娟. 面向物联网节点的综合信任度评估模型建立 [J]. 电脑知识与技术, 2020, 16(9): 51-52.

[22] JIANG J F, HAN G J, WANG F, et al. An Efficient Distributed Trust Model for Wireless Sensor Networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228-1237.

[23] 吴旭, 王杨, 袁耀. 基于D-S证据理论的多维度信任评估方法 [J]. 计算机与数字工程, 2019, 47(2): 367-372, 456.

[24] 成坚, 冯仁剑, 许小丰, 等. 基于D-S证据理论的无线传感器网络信任评估模型 [J]. 传感技术学报, 2009, 22(12): 1802-1807.

[25] FENG R J, CHE S Y, WANG X, et al. Trust Management Scheme Based on D-S Evidence Theory for Wireless Sensor Networks [J]. International Journal of Distributed Sensor Networks, 2013, 9(6): 948641.

[26] 徐泽水, 张申. 概率犹豫模糊决策理论与方法综述 [J]. 控制与决策, 2021, 36(1): 42-51.

[27] 唐文, 胡建斌, 陈钟. 基于模糊逻辑的主观信任管理模型研究 [J]. 计算机研究与发展, 2005, 42(10): 1654-1659.

[28] 左双勇, 陈光喜, 丁勇, 等. 基于模糊决策理论的主观信任模型评估 [J]. 微电子学与计算机, 2011, 28(9): 89-92.

[29] 梁锺烨, 曹奇英, 沈士根. 无线传感网络节点模糊信任演化模型 [J]. 计算机应用与软件, 2016, 33(8): 131-135.

[30] ZADEH L A. Fuzzy Sets [J]. Information and Control, 1965, 8(3): 338-353.

[31] DEMPSTER A P. Upper and Lower Probabilities Induced by a Multivalued Mapping [J]. The Annals of Mathematical Statistics, 1967, 38(2): 325-339.

责任编辑 张枸