(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108600271 B
(45)授权公告日 2020.05.22

(21)申请号 201810444073.8

(22)申请日 2018.05.10

(65)同一申请的已公布的文献号
申请公布号 CN 108600271 A

(43)申请公布日 2018.09.28

(73)专利权人 重庆邮电大学
地址 400065 重庆市南岸区崇文路2号

(72)发明人 吴大鹏 范蕾 王汝言 熊余

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 107707530 A,2018.02.16,
CN 105430638 A,2016.03.23,
WO 2011123750 A1,2011.10.06,
CN 106789947 A,2017.05.31,
Qinghua Li .etc.Providing Privacy-Aware Incentives in Mobile Sensing Systems.《IEEE TRANSACTIONS ON MOBILE COMPUTING》.2016,第15卷(第6期),
Haleh Amintoosi .etc.Trust Assessment in Social Participatory Networks.《3rd International Conference on Computer and Knowledge Engineering》.2013,

审查员 刘磊

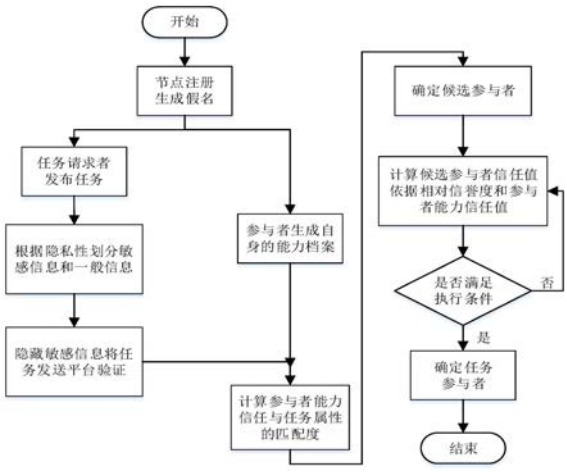
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种信任状态评估的隐私保护方法

(57)摘要

本发明公开一种信任状态感知的群智感知隐私保护方法,由于现有的解决方法大多基于同态加密等加密方法,这种方法隐私安全性较高,但是计算开销大,难以在移动终端上运行。另一方面,虽然面向任务分配的群智感知策略不断完善,但现有的任务分配策略大多侧重于开销、完成时间,忽视了参与者的隐私性和可靠性对任务感知结果的影响。因此,本发明通过对群智感知网络中的参与者基本能力属性与任务属性匹配,使用布隆过滤器,筛选符合基本条件的参与者,进而在候选参与者中,通过进一步计算参与者的能力权值与任务权值的相似度得到参与者的能力信任,并利用参与者与任务发布者的相对信誉值,完成参与者信任值的评估,在此基础上实现整个参与者选择的过程。本发明所提出的设计方法能够在保护参与者和请求者隐私的同时,招募合适的参与者,达到了均衡隐私保护和感知质量的目的。



CN 108600271 B

1.一种信任关系动态评估的隐私保护方法,其特征在于,节点注册,获得能够隐藏身份信息的假名N_p;任务请求者通过将任务属性按照隐私度分割为一般信息ComInfo和敏感信息SenInfo,通过部分盲签名算法将一般信息设为公开信息,在保护敏感信息的前提下将任务发送到平台进行签名完成验证;网络中的参与者构建自身的信任档案,任务发布后,将参与者能力属性与任务属性进行布隆过滤器匹配,初步选取候选参与者,进而分别考虑参与者与计算任务对属性的偏好估计参与者的能力信任,并结合参与者的相对信誉度最终确定参与者的信任值,选取信任值最高的参与者执行任务; 其中,节点的最终信任值计算方式如下:

$$Fturst(n_{a,b})=\frac{h^{\frac{3}{2}}}{h^{\frac{3}{2}}+time(t)}\bullet R(P,Q)+\frac{time(t)}{h^{\frac{3}{2}}+time(t)}\bullet Cturst(P,Q)$$

其中,Fturst($n_{a,b}$)为节点的最终信任值,R(P,Q)表示参与者的相对信誉度,Cturst(P,Q)表示参与者的能力信任,h表示候选参与者与任务发布者的交互次数,time(t)为参与者的时效能力。

2.根据权利要求1所述的方法,其特征在于,其中,节点注册过程具体为:参与者通过真实身份进行注册,感知平台根据签名$sign_{s_k}$和节点真实身份N_{id}通过一个哈希函数H(•)返回给节点一个秘钥种子$\tau=H(sign_{s_k}\|N_{id})$,参与者使用这个秘钥种子通过伪随机序列函数$f_k$生成假名$N_p=h(f_k(\tau))\bmod M$,作为参与者在执行任务的过程中与其他参与者交互的身份标识,其中M为素数。

3.根据权利要求1所述的方法,其特征在于,其中,任务发布者Q_j与候选参与者P_i之间的相对信誉度R(P_i,Q_j)计算过程为:根据参与者之间的历史交互记录E_{ij},由公式

$$R(P_i,Q_j)=\begin{Bmatrix}\sum_{k=1}^{h}e_{ij}^{(k)}\dfrac{\gamma(k)}{\sum_{k=1}^{h}\gamma(k)}, & h\neq 0\\ 0, & h=0\end{Bmatrix}$$

估计参与者间的相对信誉度,其中,P表示任务的参与者,i代表任务参与者的第i个,Q表示任务请求者,j代表任务请求者的第j个,E_{ij}表示参与者间h次交互的满意度集合$E_{ij}=\{e_{ij}^{(1)},e_{ij}^{(2)},...,e_{ij}^{(h)}\}$,$\gamma(k)=\frac{k}{k+1}$表示衰减因子,用于给不同时间满意度分配权重值,在所有的历史交互次数中,最新交互的满意度权重值最大。

4.根据权利要求1所述的方法,其特征在于,根据参与者完成任务的时效值time(t)和经历$Attributes_{P_i}$作为评估参与者的能力信任的评估因子,根据公式

$time(t)=1-[(1-x)e^{-be^{-ct}}]$计算参与者能完成任务的时效值,时效值越高表示参与者完成任务的时间越快; x表示参与者执行感知任务的归一化速率,0<x<1;b、c均为大于0的正数,意为参与者响应时间的比例因子。

5.根据权利要求1所述的方法,其特征在于,带有隐私保护的参与者选择过程中,利用对参与者的信任度评估选择完成优化,进一步具体包括:根据参与者属性与任务要求属性的匹配度选择候选参与者,为了隐藏节点的其余属性特征,参与者针对自身的信任档案构建布隆过滤器,并发送给任务发布者进行评估,任务发布者通过将任务要求的每个属性插

入BF以此判断参与者是否满足完成任务的基本条件，以此选择候选参与者；进一步的，考虑每个候选参与者的每个属性的偏好程度，根据公式

$$Fturst(n_{a,b})=\frac{h^{\frac{3}{2}}}{h^{\frac{3}{2}}+time(t)}\bullet R(P,Q)+\frac{time(t)}{h^{\frac{3}{2}}+time(t)}\bullet Cturst(P,Q)$$ 计算候选参与者的最终信任度，其中，$Ctrust(P,Q)=\frac{2\sum_{w_{c\mu}=w_{Q\eta}\in W_{P\cap Q}}\min(w_{c\mu},w_{Q\eta})}{\sum_{i=1}^{l}w_{ci}+\sum_{j=1}^{l}w_{Qj}}$ 表示候选节点的能力信任度，通过评估节点各属性偏好程度与任务要求各属性偏好程度的相似度得到；BF意为布隆过滤器，$W_{P\cap Q}$ 表示候选参与者的各项属性偏好程度，$w_{c\mu}$ 为参与者属性集合中包含的任务要求属性中的任意属性值，w_{Qn} 表示任务属性集合中的任意属性的数值，w_{ci} 为参与者属性集合中包含的任务要求属性的第i个属性的数值，w_{Qj} 为任务属性集合中的第j个属性的数值，l表示参与者/任务属性集合中的属性数量。

一种信任状态评估的隐私保护方法

技术领域

[0001] 本发明涉及群智感知网络隐私保护策略，特别涉及信任状态感知的参与节点选择的隐私保护机制设计。

背景技术

[0002] 随着移动互联网技术和应用的快速发展，移动智能终端设备得到了广泛使用和极大普及。移动智能终端设备集成丰富的传感器和无处不在的感知网络，使得普通用户能够参与到感知和收集周围环境状况的活动中来，在此背景下，移动感知和众包思想的结合产生了新型物联网感知模式，即群智感知。当前，群智感知已经进入快速、深度的发展阶段，深入地渗透到智能交通出行、基础设施与市政管理服务、环境监测预警、社会关系与公共安全服务等各个方面，正深刻地影响和改变着人们的工作和生活。

[0003] 与传统无线网络相比，群智感知有着部署费用低、覆盖范围广、感知数据类型和内容丰富灵活等优点。然而，由于群智感知的参与者主体是具有社会属性的人，因此其面临着许多传统无线网络未曾遇到的问题，参与者在任务分配过程中的安全与隐私问题便是其中之一。群智感知的任务分配方式分为两种：主动式和协调式。主动式是指参与者可以访问一组任务，并自主选择一个或多个任务执行，这种方案中参与者几乎不分享自己的属性信息给任务分配的实体，披露较少的个人信息，然而缺乏协调和全局优化的任务分配导致用户资源分配的不平等，会大大降低群智感知的服务质量和感知效率。协调式任务分配旨在通过优化参与者进行的任务来提高感知数据的质量，为了促进和协调感知平台与参与者的交互，使得感知服务的性能更优，协调式的任务分配需要根据任务请求者的要求，招募合适的参与者以此提升感知平台的服务质量。然而在这个选择合适参与者的过程中，需要对参与者的一些隐私信息如地理位置，职业经历等能力属性进行分析，参与者分享自己个人信息的同时，其隐私将暴露给网络中的其他实体，同时，恶意节点也可能谎报个人信息以成功获得任务，从而大大降低感知的服务质量。

[0004] 根据上述，由于群智感知任务和任务分配的特性，设计一个同时保障隐私和感知质量的任务分配模型具有极大的挑战性。目前所研究的攻击行为均假设上述三个实体中的某一个存在潜在攻击行为，显然，在实际的环境中，此类假设过于理想化，严重地高估了所提出方法针对隐私信息的保护能力。发起攻击行为的节点可以是任务发起者，相同感知任务的节点，甚至是感知平台。在任务分配过程中的攻击主要包括三种：(1)狭窄任务攻击：攻击者为了锁定目标，尝试向感知平台请求一个只有少数参与者才符合感知条件的任务，这样在获得的返回结果中会有很高的概率包含攻击目标的信息，以此大大降低攻击者的推断范围。(2)选择性任务攻击：控制多个相关任务分配，而不是请求单个任务，攻击者利用多个请求之间的相关性，将任务分配给有限几个参与者，如果已知只有一个参与者下载了某一个任务，那么与该任务相同的请求容易链接同一个参与者。(3)任务追踪攻击：这种攻击是大多由于诚实但好奇的感知平台造成的，或者是感知平台与恶意攻击者串谋，当参与者从感知平台接收一个任务时，需要向感知平台分享一些属性例如时间、地点、兴趣等，单独的

这些信息不会暴露参与者隐私，但是，攻击者通过追踪链接多种任务信息可能会导致参与者的一些敏感属性泄露。

[0005] 针对群智感知任务分配中的隐私信息匹配问题，大部分的解决方法基于交换加密，同态加密等加密方法，这种方法隐私安全性较高，但是计算开销大，难以在移动终端上运行。另一方面，虽然面向任务分配的群智感知策略不断完善，但现有的任务分配策略大多侧重于开销、完成时间，忽视了参与者的隐私性和可靠性对任务感知结果的影响。任务分配机制与信任机制的分离导致当前的任务分配系统难以在开放，动态的环境中有效运行。因此研究基于信任评估的任务分配策略具有重要的意义。

发明内容

[0006] 本发明所要解决的问题是：针对现有技术存在的上述问题，提出一种信任状态评估的群智感知隐私保护方法，能够在保护参与者和请求者隐私的同时，招募合适的参与者，达到了均衡隐私保护和感知质量的目的。

[0007] 本发明解决上述问题的技术方案是：通过对群智感知网络中的参与者基本能力属性如职业、兴趣、专业等，与任务属性匹配，使用布隆过滤器，筛选符合基本条件的参与者，进而在候选参与者中，通过进一步计算参与者的能力与任务权值的相似度得到参与者的能力信任，并利用参与者与任务发布者的相对信誉值，完成参与者信任值的评估，在此基础上实现整个参与者选择的过程。同时为了防止任务请求者在请求任务的过程中向感知平台泄露自身隐私，在任务请求的过程中，对任务信息分类，分为一般信息和敏感信息，敏感信息可能会泄露请求者隐私信息，本发明使用部分盲签名算法将一般信息作为公开信息，对敏感信息进行盲签名处理，在保护了请求者隐私的基础上，使平台可以对任务进行签名以使任务合法化。在此基础上，任务请求者对任务的敏感信息进行序列化，为选择合适的任务参与者做准备。

[0008] 本发明在充分考虑参与者能力属性的基础上通过感知参与者与任务请求者信任强度，基于历史交互信息计算参与者对请求者而言的相对信誉程度，完成网络结构的检测，基于节点自身兴趣、专业、完成任务时效等属性对节点进行能力信任的评估，通过布隆过滤器隐藏节点的具体属性值，在保护节点的隐私信息的前提下，计算节点能力信任与任务要求的匹配度，由此判断节点是否可以胜任该任务。本发明所提出的设计方法能够在保护参与者和请求者隐私的同时，招募合适的参与者，达到了均衡隐私保护和感知质量的目的。

附图说明：

[0009] 图1为本发明的整体结构框图；

[0010] 图2为本发明中候选参与者选择流程图；

具体实施方式

[0011] 以下结合附图和具体实例对本发明的实施作具体描述。

[0012] 针对群智感知中的带有隐私保护的任务分配问题，现有技术中通常采用的做法是：假设每个用户拥有一个属性集合例如地点、职业、兴趣、专业等。任务发布者请求感知任务时，将感知任务的各项要求也列在一个任务属性集合中，例如任务感知地点，要求时间，

感知类型等。在任务发布前，感知平台评估节点的属性集合与任务属性集合匹配，两个集合共有元素越多，则表示该用户对此任务的合适度越高。整个过程不泄露用户的个人属性信息，但是这些方案存在一定的局限性：匹配函数只考虑了共同属性的个数，忽略了用户对每个属性偏好程度的差异单纯的依靠对属性是否存在进行判断，攻击者容易通过狭窄任务攻击窃取用户隐私。任务分配是群智感知的重要组成部分，是提高系统运行质量的关键环节，信任可以有效地处理网络安全问题，现有的信任模型大多采用过于集中的信任管理方式，可能导致单点失效，在防御恶意攻击者方面成效也很小。

[0013] 如图1所示为本发明的整体结构框图，即信任状态评估的群智感知隐私保护策略流程图，包括以下步骤：节点注册及假名生成，发布任务及敏感信息保护，节点信任状态评估，参与者选择，其中包括候选参与者选择过程、参与者信任计算、最终参与者选择过程。

[0014] 具体包括以下步骤：

[0015] 1.节点注册及假名生成：

[0016] 假名是节点申请任务时使用的伪身份，与真实身份信息无关联。节点使用假名执行任务，从而隐藏自身的真实信息，在加入网络后，节点使用自己的真实ID进行注册，感知平台经过认证之后返回给节点一个种子$\tau = H(sign_{s_k} \| N_{id})$，用于表示节点随机产生的假名的合法性。其中$sign_{s_k}$表示感知平台的签名，$N_{id}$是节点的真实ID。节点使用τ作为随机种子，制造假名N_p，向中心和其他节点隐藏自己的真实身份，假名通过一个伪随机序列函数f_k产生，h表示一个长度匹配的哈希函数作为随机函数的生成器，M为素数。

[0017] $N_p = h(f_k(\tau)) \bmod M$ (1)

[0018] 2.发布任务及敏感信息保护：

[0019] 请求者Q向平台请求发布一个任务，平台需要对任务签名以即保证在任务分发的过程中，任务的可验证性。为了保障请求者对平台的隐私，本发明使用部分盲签名感知平台在不获知Q的任何敏感信息前提下，对Q的任务请求进行签名。任务内容包括一般信息ComInfo和敏感信息SenInfo。其中ComInfo指任务的基本要求如开始日期、结束日期、要求的感知数据数量，不会泄露Q的身份信息。而SenInfo指请求者对任务的具体细节要求例如感知地点，这其中有可能涉及到请求者的具体兴趣爱好，地理位置环境等。ComInfo部分是对平台可见的，而SenInfo是隐藏的。h()表示一个安全的加密哈希函数。r为一个随机数，m＝h(SenInfo)表示对用户敏感信息的一个随机数。

[0020] $Q \rightarrow S: m_b = h(SenInfo) r^e \bmod N, ComInfo$ (2)

[0021] 感知平台收到请求者的感知任务请求信息后，首先验证节点身份是否合法，验证成功后，对请求信息使用私钥s_k签名，并将签名后的信息m'返回给Q。这个过程中，感知平台仅仅对任务的一般信息和请求者身份进行验证，并不获知任务的具体情况，保证了请求者在申请任务时，感知平台无法通过分析任务的各项数据推断请求者的隐私。

[0022] $S \rightarrow Q: m' = [m_b]_{sk}$ (3)

[0023] Q收到的从感知平台处返回的信息m'去掉盲因子r后，得到带有感知平台签名的任务信息序列。

[0024] $Q: m^* = r^{-1} m' \bmod N = [h(SenInfo)]_{sk}$ (4)

[0025] 3.节点信任状态评估：

[0026] 群智感知网络中参与者的信任关系可根据信任内容不同分为基于过程的信任和基于特征属性的信任，前者是指在节点的历史交互中节点的行为表现，通过相互的满意度计算，而后者用于衡量节点与任务要求属性的相似性建立的信任关系，表示任务执行过程中参与者是否具有完成任务的能力，由节点的自身经历及与任务的相似性得到。

[0027] 优选地，基于过程的信任使用相对信誉度表示，旨在衡量参与者P_i与任务发布者Q_j的历史交互记录中满意度情况，在群智感知网络中，节点可能多次共同经历过同一任务，节点$e_{ij}^{(k)}$表示任务发布者Q_j对该任务执行者k_{th}次的满意程度。$E_{ij}=\{e_{ij}^{(1)},e_{ij}^{(2)},...,e_{ij}^{(h)}\}$表示最近h次的满意度集合。其中$-1\le e_{ij}^{(k)}\le 1$，$e_{ij}^{(k)}<0$表示$Q_j$对$P_i$总体不满意，且随着数值数值的减小不满意程度增大，$e_{ij}^{(k)}>0$表示$Q_j$对$P_i$总体满意，且随着数值的增大满意程度越高，h表示$P_i$与$Q_j$的交互总次数。因此$P_i$对$Q_j$的信誉度$R(P_i,Q_j)$可以表示为公式(5)，其中γ(k)表示衰减因子，用于给不同时间满意度分配权重值，在所有的历史交互次数中，最新交互的满意度权重值最大，这符合信任的认知模式。

[0028] $$R(P_i,Q_j)=\begin{cases}\sum_{k=1}^{h} e_{ij}^{(k)}\dfrac{\gamma(k)}{\sum_{k=1}^{h}\gamma(k)}, & h\neq 0\\ 0, & h=0\end{cases} \tag{5}$$

[0029] $$\gamma(k)=\frac{k}{k+1} \tag{6}$$

[0030] 任务发布者可以通过关系紧密程度高或能力属性与任务要求相似度高的节点转发信息，因此考虑基于特征属性的信任度表示参与者可以胜任感知任务的程度，由经历、时效作为评估因子进行评估。经历可以衡量参与者对任务的匹配程度，可以包括参与者的专业，兴趣爱好，行为特征等。时效可以衡量参与者是否可以及时地执行感知任务，这取决于参与者的响应时间和任务的截止时间。本发明使用生长曲线函数量化时效能力time(t)，如公式(7)所示，其中t为参与者空闲时间，d表示任务的截止时间，因为时效能力分数越高，表明节点完成任务的时间越早，随着分数的降低，完成任务的时间增加，最低值则表示在临近任务截止日期时可以完成。x表示参与者执行感知任务的归一化速率，0<x<1；b、c均为大于0的正数，意为参与者响应时间的比例因子。

[0031] $$time(t)=1-[(1-x)e^{-be^{-ct}}]\ \ if\ t<d \tag{7}$$

[0032] 为了防止参与者的隐私信息被一个恶意的任务发布者窃取，本发明不直接计算一个能力信任值，而是使用一个二维向量表示用户属性，用户属性中包含参与者的经历能力和完成任务时效，将参与者P_i的属性值通过以下的二维向量表示

[0033] $Attributes_{P_i}=\langle Time,time(t)\rangle,\langle A_{p1},w_{p1}\rangle,\langle A_{p2},w_{p2}\rangle,...,\langle A_{pn},w_{pn}\rangle$，其中$A_i$表示参与者的第i个属性，$w_i$表示与属性$A_i$对应的属性值，并且属性值中包含了公式(7)中计算的参与者的时效能力。

[0034] 4.隐私保护的参与节点选择：

[0035] 当请求者发布一个任务后，参与者首先用布隆过滤器编码敏感数据集合的所有元素，若直接简单的应用布隆过滤器处理敏感信息只能对一维向量进行处理，判断出属性是

否存在，而不能衡量属性的偏好程度，这在一定程度上保障了用户隐私却降低了参与者的选择质量，因此本发明在布隆过滤器的基础上，使用了一种通过相似函数随机化改造的隐私保护策略，在用户隐私保护的前提下，尽可能的选择最优的参与者完成任务。将私有数据集合的匹配问题转化为布隆过滤器的内积计算问题，无需可信的第三方，同时运用布隆过滤器作为属性存储结构，通过伪随机函数进行多轮迭代映射计算交集，有效减少存储空间，避免平台获知节点与任务要求无关的其他信息。

[0036] 在定义任务时，请求者可能希望定义一组要求，要求具有指定专业知识或有过类似经验的参与者执行任务，或者生活在一个特定地理区域的参与者。与参与者属性向量类似的，请求者的感知任务要求使用一个属性向量，其中包含对感知任务的各项要求以及偏好程度，即上文提到的感知任务的敏感信息$attributes_senInfo_{Qi}=\langle A_{Q1},w_{Q1}\rangle,\langle A_{Q2},w_{Q2}\rangle,...,\langle A_{Qn},w_{Qn}\rangle$。请求者可以指定作为参与者的声誉值最小值。参与者的属性表示为$attributes_Q=\{A_{Q1},A_{Q2},...,A_{Qn}\}$，任务要求的属性表示为$attributes_P=\{A_{P1},A_{P2},...,A_{Pn}\}$，因为请求者可能不满足任务的基本条件，考虑首先根据属性信息选择候选参与者，再进一步衡量参与者的属性权值，优化参与者的选择过程。

[0037] (1)候选参与者选择：通过确定参与者是否拥有任务的每项属性要求，此阶段不考虑参与者属性的偏好程度由此选择候选参与者，参与者在完成自己的档案资料后，参与者的经历属性可以表示为：$attributes\_P=\{a_{P1},a_{P2},...,a_{Pn}\}$，对于集合中的各项元素，参与者使用自己的私钥对集合attributes_P中每一个属性签名，签名后的属性可表示为：

[0038] $A_{P_i}=H_0(a_{P_i}\|ComInfo)(H(ComInfo)+x)^{-1}$其中H，$H_0$为哈希函数，由此可得到一个用户签名的属性集合$\overline{A}_p=\{A_{P_1},A_{P_1},...,A_{P_n}\}$，根据签名后的属性集合，参与者构建布隆过滤器(BF)，首先选定散列函数集合$H=h_0,h_1,\cdots,h_{k-1}$，其中散列函数$h_0,h_1,\cdots,h_{k-1}$，相互独立，并且值域均为[0,w-1]，将BFs的所有位初始值置为0，对所有$w_i\in W$和$0\leqslant i\leqslant k-1$令$BF[h_i(w_i)]=1$，即可得BF。在每参与一个任务时，参与者可将BF发送给请求者。

[0039] 请求者的任务要求属性集合$attributes_Q=\{a_{Q1},a_{Q2},...,a_{Qn}\}$，根据盲签名算法选择一个随机数r，并对每个任务属性计算出$A_{Q_i}=H_0(a_{Q_i}\|ComInfo)$，并得到一个盲化的任务的属性集合$\overline{A}_Q=\{A_{Q_1},A_{Q_1},...,A_{Q_n}\}$，并将$(N_P,\overline{A}_Q)$发送给待评估的参与者。参与者接收到$(N_P,\overline{A}_Q)$首先验证请求者身份的合法性，然后计算$U=(H(ComInfo)+x)^{-1}\overline{A}_Q$，并将U发送给请求者。请求者接收到U后，将盲化的信息解除，即$S_Q=r^{-1}V$，请求者根据接收到的参与者发送的信任档案BF，将任务要求的每一个部分依次插入BF，并检查计算结果，若$[BF[h_0(S_Q)]=1]\wedge[BF[h_1(S_Q)]=1]\wedge...[BF[h_{k-1}(S_Q)]=1]$，则证明参与者的经历包含了$S_Q$这个属性。由此选择出合适的候选参与者。

[0040] (2)最终参与者选择：候选参与者符合任务要求的属性偏好可表示为：

[0041] $attributes_{P\cap Q}=\{A_{C1},A_{C2},...,A_{Cn_1}\}$，进而计算参与者对这些共有属性的偏好程度，分别计算任务要求对属性的偏好程度与参与者的偏好程度，从而得到参与者与该任务的相似度，$W_{P\cap Q}$表示候选参与者的各项属性偏好程度，$W_{P\cap Q}=(w_{c1},w_{c2},...,w_{cn_1})$，其中

$w_{ci}=\left(\overbrace{1,1,...,1}^{w_{pi}},\overbrace{0,0,...,0}^{l-w_{pi}}\right)$；$W_Q$表示任务要求的各属性偏好程度$W_Q=(w_{Q1},w_{Q2},...,w_{Qn})$，其中$w_{Qi}=\left(\overbrace{1,1,...,1}^{w_{Qi}},\overbrace{0,0,...,0}^{l-w_{Qi}}\right)$。根据公式$Ctrust(P,Q)=\frac{2\sum_{w_{c\mu}=w_{Q\eta}\in W_{P\cap Q}}\min(w_{c\mu},w_{Q\eta})}{\sum_{i=1}^{l}w_{ci}+\sum_{j=1}^{l}w_{Qj}}$计算任务的要求向量与参与者属性的向量相似度函数，即参与者的能力信任。$w_{c\mu}$为参与者针对任务要求属性集合中的任意属性，w_{Qn}表示任务属性集合中的任意属性的数值，w_{ci}为参与者属性集合中包含的任务要求属性的第i个属性的数值，w_{Qj}为任务属性集合中的第j个属性的数值，l表示参与者/任务属性集合中的属性数量。

[0042] 候选节点是否可以参与任务，取决于节点的能力信任和相对信誉度，节点的最终信任值为$Fturst(n_{a,b})=\frac{h^{\frac{3}{2}}}{h^{\frac{3}{2}}+time(t)}\bullet R(P,Q)+\frac{time(t)}{h^{\frac{3}{2}}+time(t)}\bullet Cturst(P,Q)$。其中h表示候选参与者与任务发布者的交互次数，任务发布者将选择候选参与者中最终信任值高的节点执行任务，以此完成参与者的选择过程。

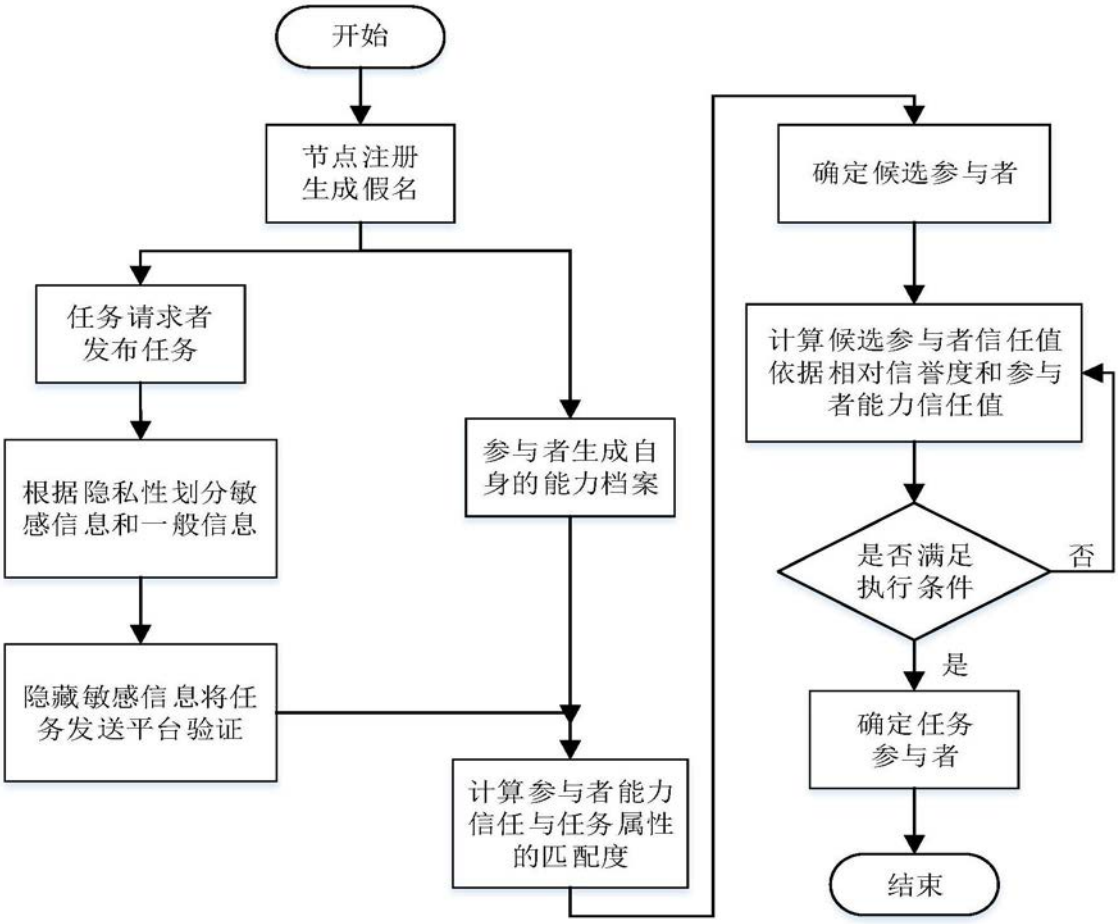

开始
节点注册
生成假名
任务请求者
发布任务
根据隐私性划分敏
感信息和一般信息
隐藏敏感信息将任
务发送平台验证
参与者生成自
身的能力档案
计算参与者能力
信任与任务属性
的匹配度
确定候选参与者
计算候选参与者信任值
依据相对信誉度和参与
者能力信任值
是否满足
执行条件
否
是
确定任务
参与者
结束

图1

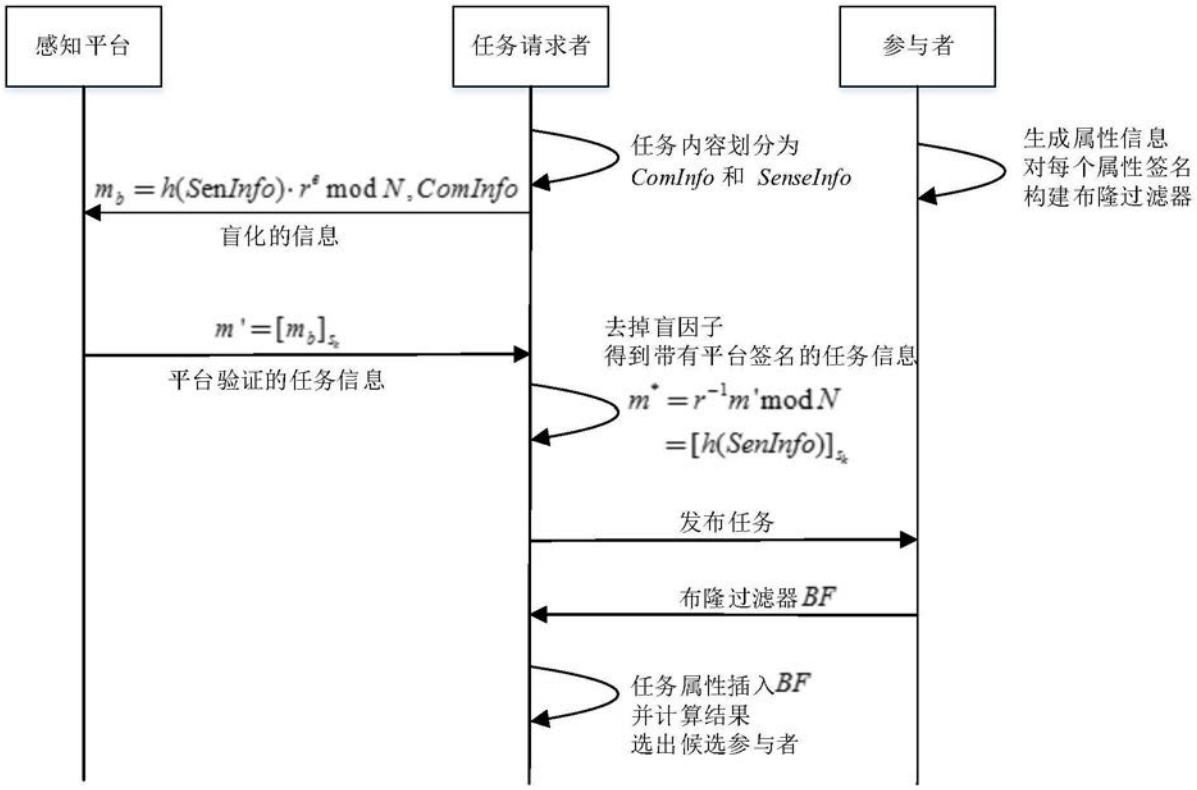

感知平台
任务请求者
参与者
任务内容划分为
ComInfo 和 SenseInfo
生成属性信息
对每个属性签名
构建布隆过滤器
$m_b = h(SenInfo) \cdot r^e \bmod N, ComInfo$
盲化的信息
$m' = [m_b]_{s_k}$
平台验证的任务信息
去掉盲因子
得到带有平台签名的任务信息
$m^* = r^{-1} m' \bmod N$
$= [h(SenInfo)]_{s_k}$
发布任务
布隆过滤器 BF
任务属性插入BF
并计算结果
选出候选参与者

图2