(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 107231363 B
(45)授权公告日 2021.06.08

(21)申请号 201710439228.4
(22)申请日 2017.06.12
(65)同一申请的已公布的文献号
申请公布号 CN 107231363 A
(43)申请公布日 2017.10.03
(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号
(72)发明人 陆以勤 甘玉宇 覃健诚 翟静
(74)专利代理机构 广州粤高专利商标代理有限公司 44102
代理人 何淑珍
(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 30/06(2012.01)
H04L 9/32(2006.01)
(56)对比文件
CN 101335618 A,2008.12.31
CN 103177201 A,2013.06.26
CN 102111385 A,2011.06.29
殷安生.可信网络中信任评估机制若干关键技术研究.《中国博士学位论文全文数据库信息科技辑》.2016,(第6期),正文摘要、第三章、第3.2.1、3.3-3.4、4.1节,图4.1.
刘东旭.GeTrust:基于担保的结构化P2P网络信任模型.《中国优秀硕士学位论文全文数据库信息科技辑》.2016,(第3期),正文摘要、第1.3、3.1、3.5.1节.
审查员 李晨

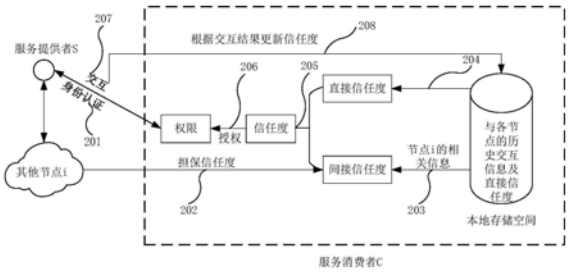
权利要求书3页 说明书6页 附图3页

(54)发明名称

一种分布式认证方法与认证模型

(57)摘要

本发明公开了一种分布式认证方法与认证模型。认证方法有别于一般的分布式认证模型中信任就进行交易,不信任就拒绝交易的方法;所述方法对信任度不小于阈值的节点进行交易,并把信任度和可以交易的有效信息量进行挂钩。所述方法的信任度由直接信任度和间接信任度组成,而间接信任度的计算借鉴了金融领域的担保方式,由邻居节点对目的节点的担保信任度确定。本发明还提供了一种分布式认证模型,包括身份认证模块、担保模块、信任度计算模块、有效信息量授权模块、担保节点奖罚模块。本发明的分布式认证有利于阻止有害信息的传播,并使得网络系统的风险可控,从而大大提高了系统的安全性。



CN 107231363 B

1.一种分布式认证方法,其特征在于包括:

两节点要进行交易,不仅要通过双向身份认证即确定节点真伪,还要通过双向权限认证即确定节点对对方的信任度;

节点把交易对方的信任度转化为可以交易的有效信息量,通过权限认证进行风险控制;

信任度由直接信任度和间接信任度构成,直接信任度由历史交易评价决定,间接信任度则由担保节点的担保信任度决定;

交易结束后,交易节点根据交易服务情况对交易对方节点和担保节点给出评价,并更新各节点的信任度信息;

所述直接信任度由历史交易评价决定,具体包括:

每个节点在本地保存每次交易的评价信息;

其中,评价信息的结构为(ID,fRankT,fScore,sRankT,sScore),

ID代表交易的统一标识符,用它可以找到任意一次交易;fRankT和fScore分别代表交易后第一次评价的时间以及给出的评价分数;sRankT和sScore分别代表追加评论的时间及给出的评价分数;

其中,直接信任度的计算方式如下:

$$D_t = \sum_{i=1}^{k} (W_i * R_i)$$

其中,Dt代表直接信任度;R_i是交易后根据交易对方综合表现而给出的评价;W_i是各次交易评价所占的权重,随着i的增大而变小;i代表从当前时间往回数的第i次交易,每次的交易评价按照评价时间进行排序,若有sRankT则以sRankT为准。

2.根据权利要求1所述的分布式认证方法,其特征在于,所述身份认证具体包括:

每个节点有一个名字,并把名字和自身的公钥组成身份标识;

服务消费者把资源申请请求和身份标识用私钥进行数字签名,并把资源申请请求、身份标识以及数字签名一起发送给服务提供者;

服务提供者收到消息后对数字签名进行解密认证,然后把认证结果及自身的身份标识用私钥进行数字签名,并把数字签名、认证结果及身份标识返回给服务消费者;

服务消费者收到服务提供者返回的消息后对数字签名进行解密认证;

任一方的身份未通过验证都会使交易中断。

3.根据权利要求1所述的分布式认证方法,其特征在于,所述权限认证具体包括:

节点计算交易对方当前的信任度,若信任度小于阈值,则拒绝本次交易;否则,把交易对方的信任度转化为本次交易的有效信息量;

其中,信任度T与有效信息量I的对应关系为:

I=W*T

W为有效信息量和信任度的比例实数,不同节点的W能不一样。

4.根据权利要求3所述的分布式认证方法,其特征在于,通过改变有效信息量和信任度的比例实数W来进行风险控制。

5.根据权利要求1所述的分布式认证方法,其特征在于,所述信任度由直接信任度和间

接信任度构成具体包括：

信任度计算公式为：

$T=a*D_t+b*R_t$

其中，直接信任度Dt的权重a比间接信任度R_t权重b大，并且a随着历史交易次数k的增大而增大，b随着历史交易次数的增大而减小。

6.根据权利要求1所述的分布式认证方法，其特征在于，所述间接信任度由担保节点的担保信任度计算得到具体包括：

每个节点在本地保存所有交易过的节点的直接信任度，并按直接信任度从高到低对所有节点进行排序；

节点向直接信任度排在前n的n个邻居节点发送担保请求信息，n与节点交易过的节点的数量有关，有上限阈值n_{th}，即若交易过的节点数量大于n_{th}，则$n=n_{th}$，否则n为交易过的节点的数量；

邻居节点收到担保请求信息后根据自身对被担保节点的直接信任度决定是否做担保，若确认做担保则把被担保节点的直接信任度返回，返回的直接信任度之后称为担保信任度；

节点把反馈回来的担保信任度进行筛选，并把选中的担保信任度的节点加入担保列表E，

间接信任度由担保信任度确定，计算公式为：

$$\mathrm{Rt}=\sum_{m\in E}U_m*\mathrm{Dt}_{ms}\ ,\quad \mathrm{Um}=\frac{\mathrm{Dt}_{cm}}{\sum_{m\in E}\mathrm{Dt}_{cm}}$$

其中，m代表担保列表E中节点，c代表担保申请节点，s代表被c计算信任度的节点，Dt_{cm}代表担保申请节点c对担保节点m的直接信任度，Dt_{ms}代表担保节点m对被计算信任度的节点s的直接信任度，U_m代表节点m的担保信任度在间接信任度Rt中所占的比重。

7.根据权利要求1所述的分布式认证方法，其特征在于，所述交易结束后，交易节点根据交易服务情况对交易对方节点和担保节点给出评价，并更新各节点的信任度信息，具体包括：

交易结束后，交易节点根据交易服务情况对交易对方节点和担保节点给出评价；

并把评价信息加入本地保存的评价信息列表；

更新各节点的直接信任度；

评价后若发现评价有误可随时更新评价信息。

8.一种用于实现权利要求1～7任一项所述认证方法的分布式认证模型，其特征在于包括：

身份认证模块，用于接收资源申请或身份认证消息、验证申请者的身份信息、把节点的身份标识和数字签名发送给申请者；

担保模块，用于向邻居节点发送担保请求信息，并把反馈回来的担保信任度进行筛选，将选中的担保信任度的节点加入担保列表E；

信任度计算模块，用于从担保列表E中取出担保信任度来计算间接信任度，再结合间接信任度和本地保存的直接信任度计算节点的信任度；

有效信息量授权模块，用于把信任度转化为有效信息量，进行权限控制，控制当次交易

最多能进行交易的有效信息量；

担保节点奖罚模块，根据交易情况对担保节点做出相应的奖罚。

一种分布式认证方法与认证模型

技术领域

[0001] 本发明涉及网络安全领域,尤其涉及一种分布式认证方法与模型。

背景技术

[0002] 网络认证技术是最重要的网络安全技术之一。认证技术主要包括信息认证与信息认证两个方面的内容,其中信息认证用于保证信息的完整性与不可否认性(不可否认性是指用户事后不能否认自己的行为)身份认证则用于鉴别用户身份,限制非法用户访问网路资源。常用的身份认证技术主要分为集中式认证方法和分布式认证方法。

[0003] 常用的PKI认证体系就是集中式认证体系,该体系采用层次化的信任模型,在模型的顶层只有一个根节点,用作认证服务器,因而其原理、设计、管理都比较简单。然而,随着用户的节点的不断增多,单一认证服务器越来越难以承受不断加大的认证压力;此外,由于该根节点是PKI认证体系的核心,一旦由于硬件故障、通信中断、恶意攻击等因素导致CA某个节点无法访问,就会导致相对应的认证功能完全失效,整个PKI面临瘫痪。也就是说,集中式认证中,认证中心容易成为技术瓶颈。

[0004] 分布式认证方法的核心思想将原来单一认证服务器的私钥SK根据门限秘密共享的分成n个子密钥,并把n个子密钥分别发给n个证书服务节点,这n个证书节点共享签发证书的能力。节点获取证书只需n个节点中的任意t个节点签名证书,组合起来就形成了一份由私钥SK签名的完整证书。这种分布式认证方案的安全性由门限t的大小决定,t取值越大系统越安全,相应的系统的实现也会越复杂。虽然这种分布式认证方法能克服单点失效的问题;但是也存在服务节点分布不均匀以及节点认证工作中的通信开销大且成功率不高的问题。

发明内容

[0005] 本发明所要解决的技术问题是提供一种分布式认证方法,阻止有害信息的扩散,保护网络的安全。

[0006] 本发明涉及到的相关概念包括:

[0007] 定义1.节点,计算机网络是由一系列的终端节点构成的,他们之间互为平等关系,他们既可以是服务提供者也可以是服务消费者;在某次交易中作为服务提供者的节点在另一次交易中可能是服务消费者,反之亦然。

[0008] 定义2.评价信息,是指交易完成后,服务消费者根据服务提供者提供服务的质量和真实性等综合给出的评价,同时也是服务消费者计算服务提供者的直接信任度的基础和依据。

[0009] 定义3.直接信任度,是服务消费者根据与服务提供者的历史交易评价计算出来的,是服务消费者判断服务提供者是否可靠的重要依据。

[0010] 定义4.间接信任度,是服务消费者根据邻居节点对服务提供者的直接信任度计算出来的,是服务消费者根据其他节点提供的信息推测服务提供者是否可靠的依据之一,在

自身与服务提供者的历史交易经验足够丰富的情况下不需要计算间接信任度。

[0011] 定义5.信任度，由直接信任度和间接信任度计算得到，代表某节点的可信程度，决定了某次交易能提供或获得的有效信息量。

[0012] 定义6.有效信息量，表示网络资源对用户的信息价值。如果是垃圾信息、浏览者没有兴趣的信息，那么有效信息量为零；若是浏览者有兴趣并且含有新知识，那么能吸收的新知识就是有效信息量。

[0013] 本发明提供的一种分布式认证方法，其包括：

[0014] 两节点要进行交易，不仅要通过双向身份认证即确定节点真伪，还要通过双向权限认证即确定节点对对方的信任度；

[0015] 节点把交易对方的信任度转化为可以交易的有效信息量，通过权限认证进行风险控制；

[0016] 信任度由直接信任度和间接信任度构成，直接信任度由历史交易评价决定，间接信任度则由担保节点的担保信任度决定；

[0017] 交易结束后，交易节点根据交易服务情况对交易对方节点和担保节点给出评价，并更新各节点的信任度信息。

[0018] 进一步地，所述身份认证具体包括：

[0019] 每个节点有一个名字，并把名字和自身的公钥组成身份标识；

[0020] 服务消费者把资源申请请求和身份标识用私钥进行数字签名，并把资源申请请求、身份标识以及数字签名一起发送给服务提供者；

[0021] 服务提供者收到消息后对数字签名进行解密认证，然后把认证结果及自身的身份标识用私钥进行数字签名，并把数字签名、认证结果及身份标识返回给服务消费者；

[0022] 服务消费者收到服务提供者返回的消息后对数字签名进行解密认证；

[0023] 任一方的身份未通过验证都会使交易中断。

[0024] 进一步地，所述权限认证具体包括：

[0025] 节点计算交易对方当前的信任度，若信任度小于阈值，则拒绝本次交易；否则，把交易对方的信任度转化为本次交易的有效信息量；

[0026] 其中，信任度T与有效信息量I的对应关系为：

[0027] $I=W*T$

[0028] W为有效信息量和信任度的比例实数，不同节点的W能不一样。

[0029] 进一步地，通过改变有效信息量和信任度的比例实数W来进行风险控制。

[0030] 进一步地，所述信任度由直接信任度和间接信任度构成具体包括：

[0031] 信任度计算公式为：

[0032] $T=a*D_t+b*R_t$

[0033] 其中，直接信任度Dt的权重a比间接信任度Rt权重b大，并且a随着历史交易次数 k 的增大而增大，b随着历史交易次数的增大而减小。

[0034] 进一步地，所述直接信任度由历史交易评价决定，具体包括：

[0035] 每个节点在本地保存每次交易的评价信息；

[0036] 其中，评价信息的结构为(ID,fRankT,fScore,sRankT,sScore)，

[0037] ID代表交易的统一标识符，用它可以找到任意一次交易；fRankT和fScore分别代

表交易后第一次评价的时间以及给出的评价分数;sRankT和sScore分别代表追加评论的时间及给出的评价分数;

[0038] 其中,直接信任度的计算方式如下:

[0039] $$D_t = \sum_{i=1}^{k} (W_i * R_i)$$

[0040] 其中,Dt代表直接信任度;R_i是交易后根据交易对方综合表现而给出的评价;W_i是各次交易评价所占的权重,随着i的增大而变小;i代表从当前时间往回数的第i次交易,每次的交易评价按照评价时间进行排序,若有sRankT则以sRankT为准。

[0041] 进一步地,所述间接信任度由担保节点的担保信任度计算得到具体包括:

[0042] 每个节点在本地保存所有交易过的节点的直接信任度,并按直接信任度从高到低对所有节点进行排序;

[0043] 节点向直接信任度排在前n的n个邻居节点发送担保请求信息(n与节点交易过的节点的数量有关,有上限阈值n_{th}。即,若交易过的节点数量大于n_{th},则$n=n_{th}$,否则n为交易过的节点的数量);

[0044] 邻居节点收到担保请求信息后根据自身对被担保节点的直接信任度决定是否做担保,若确认做担保则把被担保节点的直接信任度返回,返回的直接信任度之后称为担保信任度;

[0045] 节点把反馈回来的担保信任度进行筛选,并把选中的担保信任度的节点加入担保列表 E,

[0046] 间接信任度由担保信任度确定,计算公式为:

[0047] $R_t = \sum_{m \in F} U_m * Dt_{ms}$, $U_m = \frac{Dt_{cm}}{\sum_{m \in E} Dt_{cm}}$

[0048] 其中,m代表担保列表E中节点,c代表担保申请节点,s代表被c计算信任度的节点,Dt_{cm}代表担保申请节点c对担保节点m的直接信任度,Dt_{ms}代表担保节点m对被计算信任度的节点s的直接信任度,U_m代表节点m的担保信任度在间接信任度Rt中所占的比重。

[0049] 进一步地,所述交易结束后,交易节点根据交易服务情况对交易对方节点和担保节点给出评价,并更新各节点的信任度信息,具体包括:

[0050] 交易结束后,交易节点根据交易服务情况对交易对方节点和担保节点给出评价;

[0051] 并把评价信息加入本地保存的评价信息列表;

[0052] 更新各节点的直接信任度;

[0053] 评价后若发现评价有误可随时更新评价信息。

[0054] 本发明还提供一种分布式认证模型,所述分布式认证模型包括:

[0055] 身份认证模块,用于接收资源申请或身份认证消息、验证申请者的身份信息、把节点的身份标识和数字签名发送给申请者;

[0056] 担保模块,用于向邻居节点发送担保请求信息,并把反馈回来的担保信任度进行筛选,将选中的担保信任度的节点加入担保列表E;

[0057] 信任度计算模块,用于从担保列表E中取出担保信任度来计算间接信任度,再结合间接信任度和本地保存的直接信任度计算节点的信任度;

[0058] 有效信息量授权模块,用于把信任度转化为有效信息量,进行权限控制,控制当次

交易最多能进行交易的有效信息量；

[0059] 担保节点奖罚模块，根据交易情况对担保节点做出相应的奖罚。

[0060] 本发明与现有技术相比，有以下的优点：

[0061] 本发明中交易双方不仅要通过双向身份认证，还要通过双向权限认证，增强了认证的可靠性。现有技术一般是计算信任度后满足条件就进行交易并给予同样的权限，不满足条件就拒绝交易；这样的话阈值的选择就成为效益的关键。而本发明在得到信任度后与一个阈值做比较，若满足条件就将信任度转化为可交易的有效信息量，也就是加入了权限认证，对权限进行了细化；使得可以交易的信息量根据信任度进行动态调整；还可以通过调整信任度与有效信息量的比例来进行风险控制，从而能更有效地阻止不良信息的传播。

附图说明

[0062] 图1为本发明实施例所述的分布式认证模型的组成模块图；

[0063] 图2为本发明实施例所述的分布式认证方法的结构图；

[0064] 图3为本发明实施例所述的分布式认证方法的直接信任度示意图；

[0065] 图4为本发明实施例所述的分布式认证方法的担保列表示意图；

[0066] 图5为本发明实施例所述的分布式认证方法的历史评价信息示意图；

[0067] 图6为本发明实施例所述的分布式认证方法的信任度与有效信息量转化图。

具体实施方式

[0068] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明的实施方式进一步地详细描述。

[0069] 如图1，本发明实施例提供了一种分布式认证模型，包括身份认证模块101、担保模块 102、信任度计算模块103、有效信息量授权模块104、担保节点奖罚模块105。

[0070] 其中，身份认证模块101，用于接收所述资源申请或身份认证消息、验证申请者的身份信息、把节点的身份标识和数字签名发送给申请者；

[0071] 担保模块102，用于向邻居节点发送担保请求信息，并把反馈回来的担保信任度进行筛选，将选中的担保信任度的节点加入担保列表E；

[0072] 信任度计算模块103，用于从担保列表E中取出担保信任度来计算间接信任度，再结合间接信任度和本地保存的直接信任度计算节点的信任度；

[0073] 有效信息量授权模块104，用于把信任度转化为有效信息量，进行权限控制，控制当次最多能进行交易的有效信息量；

[0074] 担保节点奖罚模块105，用于根据交易情况对担保节点做出相应的奖罚。

[0075] 本发明提供了一种分布式认证方法，其中交易的两节点需要进行双向的身份认证和双向的权限认证。但是，由于身份认证和权限认证在任何一个节点都是同样的步骤，下面仅结合附图和实施例对单向的身份认证和权限认证进行进一步说明。如图2，具体包括以下步骤：

[0076] 步骤201：身份认证阶段。

[0077] 服务消费者C对服务提供者S对进行身份认证，具体是对S的数字签名进行验证，若验证通过就继续以下步骤，否则直接拒绝交易。

[0078] 若通过身份认证,也可在此处协商好之后进行加密通信的密钥。

[0079] 步骤202:担保节点查找阶段。

[0080] 身份认证通过后,服务消费者C开始计算服务提供者S的信任度,也就需要得到邻居节点提供的担保信任度。

[0081] 因此,服务消费者C向本地存储的直接信任度排在前n的n个邻居节点发出担保请求;

[0082] 邻居节点收到担保请求信息后根据自身对被担保节点的直接信任度决定是否做担保,若确认做担保则把对被担保节点的直接信任度(若有返回则之后称为担保信任度)返回;

[0083] 节点把反馈回来的担保信任度进行筛选,并把选中的担保信任度的节点加入担保列表E。

[0084] 如图3,图中所示为C本地保存的节点的直接信任度信息列表,各节点信息按照直接信任度的从高到低顺序进行排序,节点C向前n(本实例此处n=7)个邻居节点发送担保申请消息;邻居节点接收到担保申请后,若同意做担保则返回对节点S的直接信任度,若不做担保或没有和S的交易经验则返回0;最终收到的担保信任度如图4所示。

[0085] 如图4,图中所示为节点C接收到的邻居节点提供的担保信任度,其中C2和C6提供的信息和Dtcs相差过大,故把它们筛选掉;不采用它们作为担保节点,这样可以预防一定的诋毁或合谋攻击。

[0086] 步骤203:间接信任度计算阶段。

[0087] 根据担保列表E中节点提供的担保信任度和本地存储空间存储的对担保节点的直接信任度计算间接信任度。

[0088] 根据间接信任度的计算公式:

[0089] $R_t=\sum_{m\in E}U_m*Dt_{ms}$,$U_m=\frac{Dt_{cm}}{\sum_{m\in E}Dt_{cm}}$,计算得到C对S的间接信任度Rtcs=0.623。

[0090] 步骤204:直接信任度计算阶段。

[0091] 从本地存储空间中取出C对S的直接信任度,其中直接信任度由历史交易评价计算得到。

[0092] 如图5,图中所示为服务消费者C本地保存的与服务提供者S的历史交易评价,其中有一笔交易有两个评价,第二个评价为交易过后发现刚第一次评价有误而追加的评价,计算的时候按追加的评价进行计算,根据直接信任度的计算公式$D_t=\sum_{i=1}^{k}(W_i*R_i)$,可以算得C对S的直接信任度Dtcs=0.62。

[0093] 步骤205:信任度计算阶段。

[0094] 计算信任度。由信任度计算公式$T=a*D_t+b*R_t$,可以算得(此处a=0.7,b=0.3):Tcs=0.6209;

[0095] 服务提供者根据相同的步骤即可计算出对服务消费者C的信任度Tsc,这里假设Tsc=0.7。

[0096] 步骤206:权限控制即有效信息量转化阶段。

[0097] 把信任度转化为有效信息量,即对节点S的行为进行授权,给予S提供资源的权限。

[0098] 在本实施例中假设阈值Th=0.3,由步骤205得到Tcs=0.6209和Tsc=0.7,都大于

0.3,所以交易继续;并分别把信任度转化为有效信息量。

[0099] 其中,信任度T与信息量I的对应关系为:

[0100] I＝W*T;

[0101] 服务提供者和服务消费者计算得到的信任度和相应的转化后的信息量如图6所示。

[0102] 现有的分布式认证方法,在计算出所有服务提供者的信任度后,在做选择时,往往只是单纯的取信任度最高的服务提供者作为交易对象,它们没有考虑到在阈值之上的信任度的高低的差别。比如说,某次交易服务消费者计算出的服务提供者的信任度分别为0.5和0.6,然后就选择了信任度为0.6的服务提供者进行交易。但是在另外一次交易中服务提供者的信任度分别为0.9和0.8,这次是选择了信任度为0.9的服务提供者进行交易。在两次交易中服务提供者的信任度实际上相差比较大,但是在交易中却没有体现出这种差别。为此,本发明实施例提出了把信任度转化为有效信息量的方法,来解决信任度高低不同权限一样的问题,从而更有效地阻止有害信息的扩散,保护网络的安全。

[0103] 步骤207:节点间交易控制阶段。

[0104] 服务提供者和服务消费者计算得到的较小的有效信息量决定了本次交易的有效信息量。

[0105] 由步骤206可知,本次交易所能传输的有效信息量为Ic＝0.6209W,如图6所示。Wc和 Ws分别为服务消费者和服务提供者的信任度和信息量的转化实数,可能相等也可能不相等,在本发明实施例中假设两者相等,都为W。

[0106] 步骤208:更新评价信息阶段。

[0107] 交易结束后,Ci根据交易服务情况对Sj给出一个评价信息、对担保列表E中担保节点做出相应的奖罚并更新各节点的直接信任度。

[0108] 为了说明本发明的内容及实施方法,上述内容给出了一个具体实施例。在实施例中引入细节的目的不是限制权利要求书的范围,而是帮助理解本发明所述方法。本领域的技术人员应理解:在不脱离本发明及其所附权利要求书的精神和范围内,对实施例步骤得各种修改、变化或替换都是可能的。因此,本发明不应局限于实施例及所附图所公开的内容。

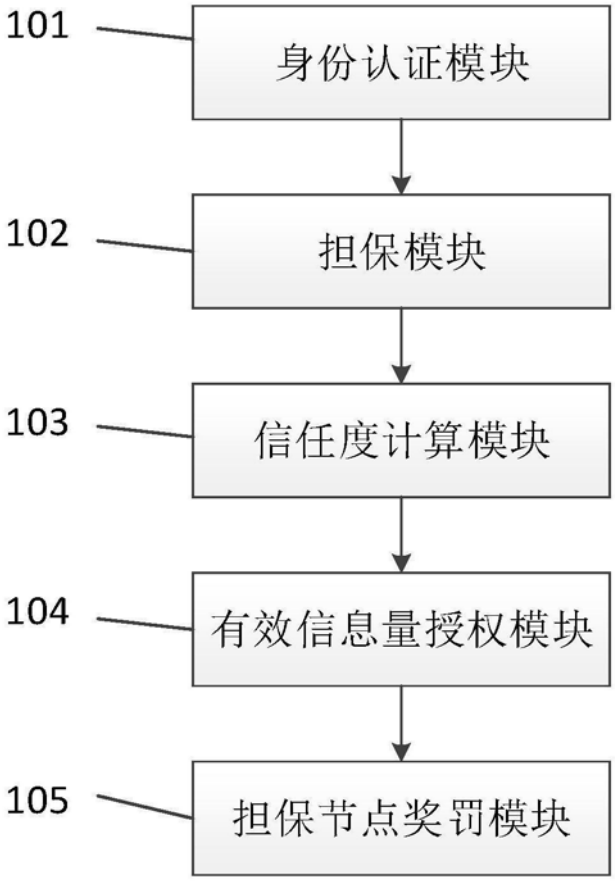

101
身份认证模块
102
担保模块
103
信任度计算模块
104
有效信息量授权模块
105
担保节点奖罚模块

图1

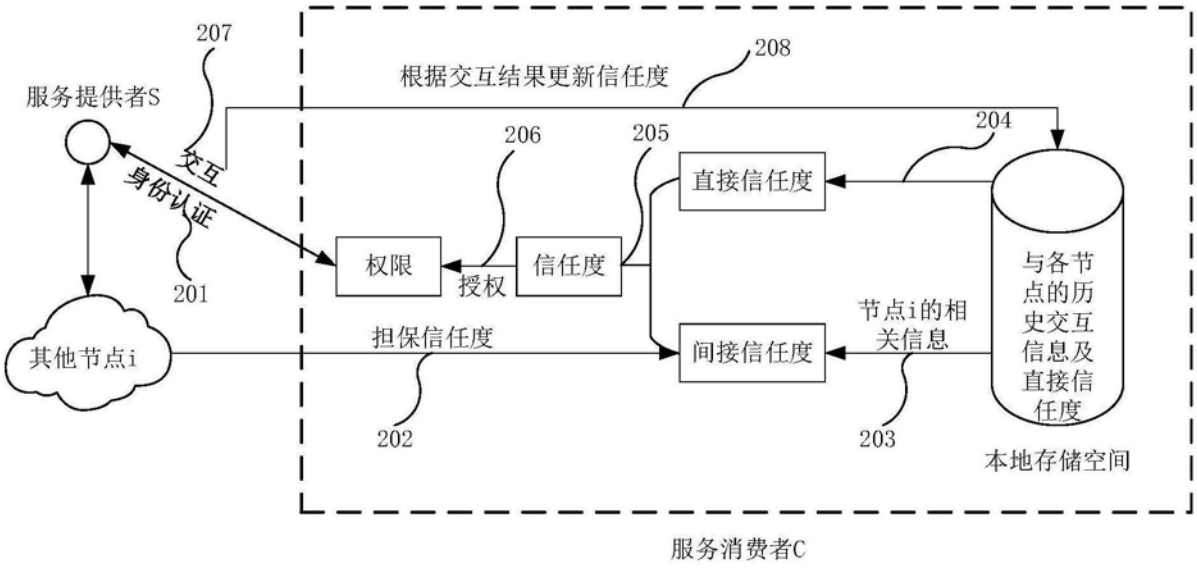

207
服务提供者S
根据交互结果更新信任度
208
204
206
205
交互
身份认证
直接信任度
权限
授权
信任度
201
与各节点的历史交互信息及直接信任度
节点i的相关信息
其他节点i
担保信任度
间接信任度
202
203
本地存储空间
服务消费者C

图2

C本地保存的节点的直接信任度信息列表		
Num	ID	Dt
1	C1	0.9
2	C2	0.85
3	C3	0.82
4	C4	0.8
5	C5	0.8
6	C6	0.78
7	C7	0.76
...	...	...
	S	0.62
...	...	...

图3

担保列表E		
ID	Dt_{cis}	是否采用
C1	0.63	是
C2	0.23	否
C3	0.65	是
C4	0.55	是
C5	0.68	是
C6	0	否
C7	0.60	是
Rt = 0.623		

图4

C本地保存的节点S的评价信息表			
fRankT	fScore	sRankT	sScore
17/3/8	0.6	0	0
17/3/7	0.7	0	0
17/3/6	0.65	0	0
17/3/5	0.6	0	0
17/3/4	0.66	0	0
17/3/3	0.56	0	0
17/2/8	0.3	17/3/3	0.6
17/3/2	0.55	0	0
17/3/1	0.58	0	0
...	...	...	...
C对S的直接信任度 Dtcs = 0.62			

图5

信任值T	有效信息量I	最终可交易的最大信息量
Tcs=0.6209	Ic=0.6209W	Ic
Tsc=0.7	Is=0.7W	

图6