(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109347852 A
(43)申请公布日 2019.02.15

(21)申请号 201811315880.6

(22)申请日 2018.11.07

(71)申请人 暨南大学
地址 510632 广东省广州市天河区黄埔大道西601号

(72)发明人 刘志全 翁健 马建峰 李盈 兰奕明 魏凯敏 冯丙文

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 陈燕娴

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/24(2006.01)
H04L 9/32(2006.01)

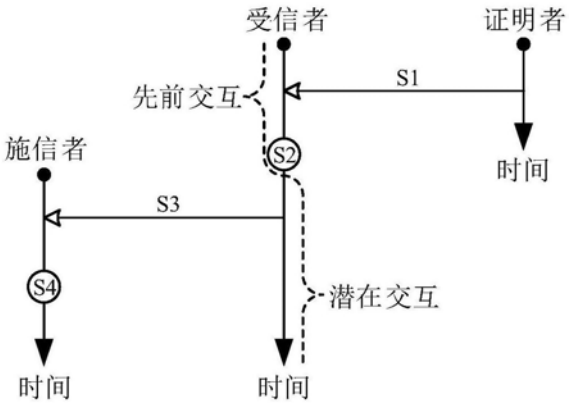
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种轻量级的车联网信任评估方法

(57)摘要

本发明公开了一种轻量级的车联网信任评估方法，具体包括步骤：S1、在节点先前交互结束时，交互双方均根据交互体验为对方生成一条包含自身数字签名的信任证明并发送给对方；S2、交互双方收到新的信任证明后验证其签名信息，并更新本地存储以保存对自身最有利的至多η条信任证明，其中$\eta \in Z^+$为系统参数；S3、在潜在交互开始时，潜在交互双方均将本地存储的信任证明发送给对方以证明自身可信赖；S4、潜在交互双方通过数字签名信息验证信任证明的真实性并据此导出对方的信任值和决定是否同意与之交互，当且仅当双方都同意时进行交互。本发明不依赖信任中心和路侧单元，更符合车联网的大规模、分布式特性。



CN 109347852 A

1.一种轻量级的车联网信任评估方法,其特征在于,具体包括如下步骤:

S1、在节点先前交互结束时,交互双方均根据交互体验为对方生成一条包含自身数字签名的信任证明并发送给对方;

S2、交互双方收到新的信任证明后验证其签名信息,并更新本地存储以保存对自身最有利的至多η条信任证明,其中$\eta\in Z_+$为系统参数;

S3、在潜在交互开始时,潜在交互双方均将本地存储的信任证明发送给对方以证明自身可信赖;

S4、潜在交互双方通过数字签名信息验证信任证明的真实性并据此导出对方的信任值和决定是否同意与之交互,当且仅当双方都同意时进行交互。

2.根据权利要求1所述的轻量级的车联网信任评估方法,其特征在于,所述的步骤S1中,信任证明具体格式为:

TC(B,A)=(ID(B),ID(A),RT(B,A),WG(B),TS(B,A),DS(B,A))

其中B和A表示节点,B为证明者,A为受信者;ID(B)和ID(A)分别表示证明者B和受信者A的唯一标识符;RT(B,A)表示评估值向量,具体格式为:

RT(B,A)=(RT(B,A,1),RT(B,A,2),...,RT(B,A,n))

其中n表示信任方面的个数,RT(B,A,i)(i∈[1,n])表示证明者B对受信者A的第i个信任方面的评估值;WG(B)表示权重值向量,具体格式为:

WG(B)=(WG(B,1),WG(B,2),...,WG(B,n))

其中WG(B,i)(i∈[1,n])表示证明者B对第i个信任方面的兴趣偏好水平;TS(B,A)表示TC(B,A)生成时的时间戳;DS(B,A)表示数字签名信息。

3.根据权利要求2所述的轻量级的车联网信任评估方法,其特征在于,所述RT(B,A,i)表示为语言变量,包括“非常好”、“好”、“一般”、“差”和“非常差”;所述WG(B,i)表示为语言变量,包括“非常高”、“高”、“中”、“低”和“非常低”。

4.根据权利要求1所述的轻量级的车联网信任评估方法,其特征在于,所述的步骤S2中,受信者A收到证明者B为自身生成的信任证明TC(B,A)后,首先验证其签名信息DS(B,A),然后判断本地已存储信任证明的数量NM(A)与η的大小关系:若NM(A)<η,则受信者A直接存储TC(B,A);若NM(A)=η,则受信者A计算每条信任证明对应的加权评估值,并据此选出对自身最有利的η条信任证明进行存储,同时删除其他信任证明,受信者A考虑的信任证明包括TC(B,A)和本地已存储的η条信任证明。

5.根据权利要求1所述的轻量级的车联网信任评估方法,其特征在于,所述步骤S2中,由TC(B,A)计算加权评估值的具体步骤为:

S2.1、将TC(B,A)中的RT(B,A,i)转换为模糊评估RF(B,A,i)和清晰评估RC(B,A,i),其中RF(B,A,i)的具体格式为:

RF(B,A,i)=(RF(B,A,i,1),RF(B,A,i,2),RF(B,A,i,3),RF(B,A,i,4))

其中0≤RF(B,A,i,1)≤RF(B,A,i,2)≤RF(B,A,i,3)≤RF(B,A,i,4)≤100;RC(B,A,i)为RF(B,A,i)的符号距离,具体可由以下公式导出:

$$RC(B,A,i)=d\big(RF(B,A,i)\big)=\frac{\sum_{k=1}^{4}RF(B,A,i,k)}{4};$$

S2.2、将TC(B,A)中WG(B,i)转换为模糊权重WF(B,i)和清晰权重WC(B,i),其中WF(B,i)

的具体格式为：

WF(B,i)＝(WF(B,i,1),WF(B,i,2),WF(B,i,3),WF(B,i,4))

其中0≤WF(B,i,1)≤WF(B,i,2)≤WF(B,i,3)≤WF(B,i,4)≤10;WC(B,i)可由以下公式导出：

$$WC(B,i)=\frac{d(WF(B,i))}{\sum_{j=1}^{n} d(WF(B,j))}=\frac{\sum_{k=1}^{4} WF(B,i,k)}{\sum_{j=1}^{n}\sum_{k=1}^{4} WF(B,j,k)};$$

S2.3、TC(B,A)对应的模糊评估值SF(B,A)可计算为：

$$SF(B,A)=(\sum_{i=1}^{n}(RF(B,A,i,1)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,2)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,3)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,4)*WC(B,i)))$$

TC(B,A)对应的清晰评估值SC(B,A)可计算为：

$$SC(B,A)=\frac{d(SF(B,A))}{100}=\frac{\sum_{k=1}^{4}\sum_{i=1}^{n}(RF(B,A,i,k)*WC(B,i))}{100};$$

S2.4、受信者A在选择最有利信任证明时仅考虑时间衰减权重WT(B,A)，其计算公式为：

$$WT(B,A)=\begin{cases}0, & \text{if } TN-TS(B,A)>\omega\\ e^{-\frac{TN-TS(B,A)}{\theta}}, & \text{otherwise}\end{cases}$$

其中，TN表示当前时间戳;TS(B,A)为TC(B,A)中所含时间戳;ω表示时间窗口大小;θ为时间衰减因子，控制WT(B,A)随时间差衰减的速度；

S2.5、TC(B,A)对应的加权评估值SW(B,A)可计算为：

SW(B,A)＝SC(B,A)*WT(B,A)。

6.根据权利要求1所述的轻量级的车联网信任评估方法，其特征在于，所述的步骤S3中，信任证明集合的具体格式为：

TCs(A)＝{TC(B^1,A),TC(B^2,A),...,TC($B^{NM(A)}$,A)}

其中NM(A)≤η。

7.根据权利要求1所述的轻量级的车联网信任评估方法，其特征在于，所述的步骤S4具体为：

S4.1、在潜在交互开始时，作为施信者的节点C收到作为受信者的节点A的信任证明集合TCs(A)后，首先提取出其中的信任证明，即TC(B^1,A)、TC(B^2,A)、...、TC($B^{NM(A)}$,A)，若NM(A)<η，则施信者C对受信者A的信任值TV(C,A)被设为常数τ∈[0,1)；否则，施信者C通过每条信任证明中的数字签名信息验证其真实性，然后导出每条信任证明对应的加权评估值并计算TV(C,A)；同理，可得出施信者A对受信者C的信任值TV(A,C)；

S4.2、当且仅当TV(C,A)≥TH(C)且TV(A,C)≥TH(A)时，节点A与节点C进行交互，其中TH(C),TH(A)∈[0,1]分别为节点C、节点A的信任门限。

8.根据权利要求1所述的轻量级的车联网信任评估方法，其特征在于，所述的步骤S4中，施信者C除考虑时间衰减权重WT(B,A)外，还考虑兴趣偏好相似度权重WS(C,B)，该权重

由施信者C与证明者B的兴趣偏好向量的加权欧式距离DS(C,B)导出,具体计算公式为:

$$DS(C,B)=\sqrt{\frac{\sum_{i=1}^{n}((WC(C,i)-WC(B,i))^2*WC(C,i))}{\sum_{i=1}^{n}WC(C,i)}}$$

WS(C,B)＝1-DS(C,B)。

9.根据权利要求8所述的轻量级的车联网信任评估方法,其特征在于,所述的步骤S4中,TC(B,A)对应的加权评估值ST(C,B,A)可计算为:

ST(C,B,A)＝SC(B,A)*WT(B,A)*WS(C,B)

同理,施信者C能够导出TC(B^1,A)、TC(B^2,A)、...、TC(B^η,A)对应的加权评估值,并计算对受信者A的信任值TV(C,A),具体计算公式为:

$$TV(C,A)=\frac{\sum_{j=1}^{\eta}ST(C,B^j,A)}{\eta}。$$

一种轻量级的车联网信任评估方法

技术领域

[0001] 本发明涉及车联网安全技术领域，具体涉及一种轻量级的车联网信任评估方法。

背景技术

[0002] 当前，交通事故、道路拥堵和环境污染已成为全球城市所面临的关键问题，而车联网作为物联网在汽车行业的主要应用和智能交通系统的核心组成部分，在城市道路交通方面发挥着至关重要的作用。车联网被认为是物联网中最具市场潜力的分支之一，现已被列为国家“十二五”、“十三五”规划纲要的重大研究项目。

[0003] 然而，由于大规模、开放式、分布式、稀疏和高动态等特性，车联网对于恶意行为和攻击是脆弱的，安全性和可靠性已逐渐成为制约车联网进一步发展的瓶颈，并关系到车联网能否应用于真实的道路环境中。现有方案大都采用数字签名和密码学技术，无法评估节点(即车辆)的可靠性和消息的质量。

[0004] 信任管理在车联网中扮演至关重要的角色，它使得每个节点能够预先评估其他节点和消息的信任值，以避免恶意节点和不实消息引起的严重后果。当前，车联网中的信任管理仍然处于初级阶段，仅少量的信任评估方案被提出。基于体系结构，现有方案能够被粗略地划分为两类，即基于基础设施的方案和自组织方案。

[0005] Li等人[X.Li,J.Liu,X.Li,and W.Sun,"RGTE:A reputation-based global trust establishment in VANETs,"In Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems,2013,pp.210-214.]为车联网提出一个基于声望的全局信任建立方案RGTE，其中声望管理中心负责收集所有合法节点的信任信息并计算其声望分数。该模型假设声望管理中心完全可信并实时在线，需要较高的维护成本，并存在单点失效、时延大等固有缺陷。Wei等人[Z.Wei,F.R.Yu,and A.Boukerche,"Trust based security enhancements for vehicular ad hoc networks,"In Proceedings of the 4th International Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications,2014,pp.103-109.]综合考虑基于历史交互的直接信任和基于信任推荐的间接信任，并为车联网提出一种分布式信任评估方法，其中直接信任由贝叶斯公式导出，而间接信任由D-S证据理论导出。该模型需要施信者收集关于受信者的信任推荐信息，通常会导致较大的时间、带宽消耗。

发明内容

[0006] 本发明的目的在于克服现有技术的缺点与不足，提供一种轻量级的车联网信任评估方法，此方法不依赖信任中心和路侧单元，更符合车联网的大规模、分布式特性。

[0007] 本发明的目的通过以下的技术方案实现：一种轻量级的车联网信任评估方法，具体包括如下步骤：

[0008] S1、在节点先前交互结束时，交互双方均根据交互体验为对方生成一条包含自身

数字签名的信任证明并发送给对方；

[0009] S2、交互双方收到新的信任证明后验证其签名信息，并更新本地存储以保存对自身最有利的至多η条信任证明，其中$\eta \in Z_+$为系统参数；

[0010] S3、在潜在交互开始时，潜在交互双方均将本地存储的信任证明发送给对方以证明自身可信赖；

[0011] S4、潜在交互双方通过数字签名信息验证信任证明的真实性并据此导出对方的信任值和决定是否同意与之交互，当且仅当双方都同意时进行交互。

[0012] 优选的，所述的步骤S1中，信任证明具体格式为：

[0013] TC(B,A)＝(ID(B),ID(A),RT(B,A),WG(B),TS(B,A),DS(B,A))

[0014] 其中B和A表示节点，B为证明者，A为受信者；ID(B)和ID(A)分别表示证明者B和受信者A的唯一标识符；RT(B,A)表示评估值向量，具体格式为：

[0015] RT(B,A)＝(RT(B,A,1),RT(B,A,2),...,RT(B,A,n))

[0016] 其中n表示信任方面的个数，RT(B,A,i)(i∈[1,n])表示证明者B对受信者A的第i个信任方面的评估值；WG(B)表示权重值向量，具体格式为：

[0017] WG(B)＝(WG(B,1),WG(B,2),...,WG(B,n))

[0018] 其中WG(B,i)(i∈[1,n])表示证明者B对第i个信任方面的兴趣偏好水平；TS(B,A)表示TC(B,A)生成时的时间戳；DS(B,A)表示数字签名信息。

[0019] 更进一步的，所述RT(B,A,i)表示为语言变量，包括“非常好”、“好”、“一般”、“差”和“非常差”；所述WG(B,i)表示为语言变量，包括“非常高”、“高”、“中”、“低”和“非常低”。

[0020] 优选的，所述的步骤S2中，受信者A收到证明者B为自身生成的信任证明TC(B,A)后，首先验证其签名信息DS(B,A)，然后判断本地已存储信任证明的数量NM(A)与η的大小关系：若NM(A)＜η，则受信者A直接存储TC(B,A)；若NM(A)＝η，则受信者A计算每条信任证明对应的加权评估值，并据此选出对自身最有利的η条信任证明进行存储，同时删除其他信任证明，受信者A考虑的信任证明包括TC(B,A)和本地已存储的η条信任证明。

[0021] 优选的，所述步骤S2中，由TC(B,A)计算加权评估值的具体步骤为：

[0022] S2.1、将TC(B,A)中的RT(B,A,i)转换为模糊评估RF(B,A,i)和清晰评估RC(B,A,i)，其中RF(B,A,i)的具体格式为：

[0023] RF(B,A,i)＝(RF(B,A,i,1),RF(B,A,i,2),RF(B,A,i,3),RF(B,A,i,4))

[0024] 其中0≤RF(B,A,i,1)≤RF(B,A,i,2)≤RF(B,A,i,3)≤RF(B,A,i,4)≤100；RC(B,A,i)为RF(B,A,i)的符号距离，具体可由以下公式导出：

[0025] $$RC(B,A,i) = d\big(RF(B,A,i)\big) = \frac{\sum_{k=1}^{4} RF(B,A,i,k)}{4};$$

[0026] S2.2、将TC(B,A)中WG(B,i)转换为模糊权重WF(B,i)和清晰权重WC(B,i)，其中WF(B,i)的具体格式为：

[0027] WF(B,i)＝(WF(B,i,1),WF(B,i,2),WF(B,i,3),WF(B,i,4))

[0028] 其中0≤WF(B,i,1)≤WF(B,i,2)≤WF(B,i,3)≤WF(B,i,4)≤10；WC(B,i)可由以下公式导出：

[0029] $$WC(B,i) = \frac{d(WF(B,i))}{\sum_{j=1}^{n} d(WF(B,j))} = \frac{\sum_{k=1}^{4} WF(B,i,k)}{\sum_{j=1}^{n}\sum_{k=1}^{4} WF(B,j,k)};$$

[0030] S2.3、TC(B,A)对应的模糊评估值SF(B,A)可计算为：

[0031]

$$SF(B,A)=(\sum_{i=1}^{n}(RF(B,A,i,1)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,2)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,3)*WC(B,i)),\sum_{i=1}^{n}(RF(B,A,i,4)*WC(B,i)))$$

[0032] TC(B,A)对应的清晰评估值SC(B,A)可计算为：

[0033] $$SC(B,A)=\frac{d(SF(B,A))}{100}=\frac{\sum_{k=1}^{4}\sum_{i=1}^{n}(RF(B,A,i,k)*WC(B,i))}{100};$$

[0034] S2.4、受信者A在选择最有利信任证明时仅考虑时间衰减权重WT(B,A)，其计算公式为：

[0035] $$WT(B,A)=\begin{cases}0, & \text{if } TN-TS(B,A)>\omega\\ e^{-\frac{TN-TS(B,A)}{\theta}}, & \text{otherwise}\end{cases}$$

[0036] 其中，TN表示当前时间戳；TS(B,A)为TC(B,A)中所含时间戳；ω表示时间窗口大小；θ为时间衰减因子，控制WT(B,A)随时间差衰减的速度；

[0037] S2.5、TC(B,A)对应的加权评估值SW(B,A)可计算为：

[0038] SW(B,A)＝SC(B,A)*WT(B,A)。

[0039] 优选的，所述的步骤S3中，信任证明集合的具体格式为：

[0040] $TCs(A)=\{TC(B^{1},A),TC(B^{2},A),\ldots,TC(B^{NM(A)},A)\}$

[0041] 其中$NM(A)\leqslant\eta$。

[0042] 优选的，所述的步骤S4具体步骤为：

[0043] S4.1、在潜在交互开始时，作为施信者的节点C收到作为受信者的节点A的信任证明集合TCs(A)后，首先提取出其中的信任证明，即$TC(B^{1},A)$、$TC(B^{2},A)$、…、$TC(B^{NM(A)},A)$，若$NM(A)<\eta$，则施信者C对受信者A的信任值TV(C,A)被设为常数$\tau\in[0,1)$；否则，施信者C通过每条信任证明中的数字签名信息验证其真实性，然后导出每条信任证明对应的加权评估值并计算TV(C,A)；同理，可得出施信者A对受信者C的信任值TV(A,C)；

[0044] S4.2、当且仅当TV(C,A)≥TH(C)且TV(A,C)≥TH(A)时，节点A与节点C进行交互，其中TH(C)，TH(A)∈[0,1]分别为节点C、节点A的信任门限。

[0045] 优选的，所述的步骤S4中，施信者C除考虑时间衰减权重WT(B,A)外，还考虑兴趣偏好相似度权重WS(C,B)，该权重由施信者C与证明者B的兴趣偏好向量的加权欧式距离DS(C,B)导出，具体计算公式为：

[0046] $$DS(C,B)=\sqrt{\frac{\sum_{i=1}^{n}((WC(C,i)-WC(B,i))^{2}*WC(C,i))}{\sum_{i=1}^{n}WC(C,i)}}$$

[0047] WS(C,B)＝1-DS(C,B)。

[0048] 更进一步地，所述的步骤S4中，TC(B,A)对应的加权评估值ST(C,B,A)可计算为：

[0049] ST(C,B,A)＝SC(B,A)*WT(B,A)*WS(C,B)

[0050] 同理，施信者C能够导出TC(B^1,A)、TC(B^2,A)、…、TC(B^η,A)对应的加权评估值，并计算对受信者A的信任值TV(C,A)，具体计算公式为：

[0051] $$TV(C,A)=\frac{\sum_{j=1}^{\eta} ST(C,B^j,A)}{\eta}。$$

[0052] 本发明与现有技术相比，具有如下优点和有益效果：

[0053] 1、本发明采用完全自组织方式，施信者、受信者、证明者等三种角色在不同评估阶段进行转换，不依赖于信任中心和路侧单元，因而更适应大规模、分布式的车联网环境。

[0054] 2、本发明由受信者自行存储和提供信任信息，而无需施信者收集，因而能够大幅减少时间、带宽消耗，实现快速、轻量级信任评估。

附图说明

[0055] 图1是本发明轻量级的车联网信任评估方法实施例的主要步骤示意图。

[0056] 图2是本发明轻量级的车联网信任评估方法实施例的简单实例。

具体实施方式

[0057] 为了更好地理解本发明的技术方案，下面结合附图详细描述本发明提供的实施例，但本发明的实施方式不限于此。

[0058] 实施例

[0059] 如图1-2所示，本实施例不含信任中心和路侧单元，而仅由大量普通节点(即车辆)组成，其间通过无线自组网方式进行通信。每个节点的角色为施信者、受信者或证明者之一，且会在不同评估阶段进行转换。

[0060] 步骤S1、节点A、B先前交互结束时，作为证明者的B为作为受信者的A根据交互体验生成一条信任证明TC(B,A)，具体格式为：

[0061] TC(B,A)＝(ID(B),ID(A),RT(B,A),WG(B),TS(B,A),DS(B,A)) (1)

[0062] 其中ID(B)和ID(A)分别表示证明者B和受信者A的唯一标识符；RT(B,A)表示评估值向量，具体格式为：

[0063] RT(B,A)＝(RT(B,A,1),RT(B,A,2),...,RT(B,A,n)) (2)

[0064] 其中n表示信任方面的个数，RT(B,A,i)(i∈[1,n])表示证明者B对受信者A的第i个信任方面的评估值，其值被表示为语言变量，如“非常好”、“好”、“一般”、“差”、“非常差”等；WG(B)表示权重值向量，具体格式为：

[0065] WG(B)＝(WG(B,1),WG(B,2),...,WG(B,n)) (3)

[0066] 其中WG(B,i)(i∈[1,n])表示证明者B对第i个信任方面的兴趣偏好水平，其值也被表示为语言变量，如“非常高”、“高”、“中”、“低”、“非常低”等；TS(B,A)表示TC(B,A)生成时的时间戳；DS(B,A)表示数字签名信息。

[0067] 同理，作为受信者的B为作为证明者的A生成TC(B,A)后将其发送给证明者A。类似地，证明者A也为受信者B生成信任证明TC(A,B)并将其发送给受信者B。

[0068] 步骤S2、受信者A收到证明者B为自身生成的信任证明TC(B,A)后，首先验证其签名

信息DS(B,A)，然后判断本地已存储信任证明的数量NM(A)与η的大小关系，其中$\eta \in Z^+$为系统参数：若NM(A)＜η，则受信者A直接存储TC(B,A)；若NM(A)＝η，则受信者A计算每条信任证明对应的加权评估值，并据此选出对自身最有利的η条信任证明进行存储，同时删除其他信任证明，受信者A计算的信任证明包括TC(B,A)和本地已存储的η条信任证明。

[0069] 以计算TC(B,A)对应的加权评估值为例：TC(B,A)中RT(B,A,i)可由现有的模糊简单加性权重系统[S.Y.Chou,Y.H.Chang,and C.Y.Shen,"A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes,"European Journal of Operational Research,2008,vol.189,no.1,pp.132-145.]转换为模糊评估RF(B,A,i)和清晰评估RC(B,A,i)，其中RF(B,A,i)的具体计算步骤为：

[0070] RF(B,A,i)＝(RF(B,A,i,1),RF(B,A,i,2),RF(B,A,i,3),RF(B,A,i,4)) (4)

[0071] 其中，0≤RF(B,A,i,1)≤RF(B,A,i,2)≤RF(B,A,i,3)≤RF(B,A,i,4)≤100；RC(B,A,i)为RF(B,A,i)的符号距离，具体可由以下公式导出：

[0072] $$RC(B,A,i) = d\big(RF(B,A,i)\big) = \frac{\sum_{k=1}^{4} RF(B,A,i,k)}{4} \quad (5)$$

[0073] 类似地，WG(B,i)可转换为模糊权重WF(B,i)和清晰权重WC(B,i)，其中WF(B,i)的具体格式为：

[0074] WF(B,i)＝(WF(B,i,1),WF(B,i,2),WF(B,i,3),WF(B,i,4)) (6)

[0075] 其中0≤WF(B,i,1)≤WF(B,i,2)≤WF(B,i,3)≤WF(B,i,4)≤10；WC(B,i)可由以下公式导出：

[0076] $$WC(B,i) = \frac{d(WF(B,i))}{\sum_{j=1}^{n} d(WF(B,j))} = \frac{\sum_{k=1}^{4} WF(B,i,k)}{\sum_{j=1}^{n}\sum_{k=1}^{4} WF(B,j,k)} \quad (7)$$

[0077] 其中，j,k均为求和的临时变量。

[0078] 随后，TC(B,A)对应的模糊评估值SF(B,A)可计算为：

[0079]

$$SF(B,A) = \left(\sum_{i=1}^{n}(RF(B,A,i,1)*WC(B,i)), \sum_{i=1}^{n}(RF(B,A,i,2)*WC(B,i)), \sum_{i=1}^{n}(RF(B,A,i,3)*WC(B,i)), \sum_{i=1}^{n}(RF(B,A,i,4)*WC(B,i))\right) \quad (8)$$

[0080] TC(B,A)对应的清晰评估值SC(B,A)可计算为：

[0081] $$SC(B,A) = \frac{d\big(SF(B,A)\big)}{100} = \frac{\sum_{k=1}^{4}\sum_{i=1}^{n}(RF(B,A,i,k)*WC(B,i))}{100} \quad (9)$$

[0082] 受信者A在选择最有利信任证明时仅考虑时间衰减权重WT(B,A)，其计算公式为：

[0083] $$WT(B,A) = \begin{cases} 0, & \text{if } TN - TS(B,A) > \omega \\ e^{-\frac{TN-TS(B,A)}{\theta}}, & \text{otherwise} \end{cases} \quad (10)$$

[0084] 其中TN表示当前时间戳；TS(B,A)为TC(B,A)中所含时间戳；ω表示时间窗口大小；θ为时间衰减因子，控制WT(B,A)随时间差衰减的速度。

[0085] 因此，TC(B,A)对应的加权评估值SW(B,A)可计算为：

[0086] SW(B,A)＝SC(B,A)*WT(B,A) (11)

[0087] 由公式(4)-(10)可推得RC(B,A,i)的范围为[0,100]，而WC(B,i)、WT(B,A)、SC(B,A)、SW(B,A)的范围为[0,1]。

[0088] 同理，受信者A分别计算本地已存储的η条信任证明对应的加权评估值$SW(B^1,A)$、$SW(B^2,A)$、…、$SW(B^\eta,A)$，然后从SW(B,A)、$SW(B^1,A)$、…、$SW(B^\eta,A)$中选出η个较大值并存储对应的信任证明，同时删除其他信任证明。

[0089] 步骤S3、在潜在交互开始时，受信者A欲与作为施信者的节点C进行交互，受信者A首先取出本地存储的信任证明，其集合记为TCs(A)，即：

[0090] $TCs(A)=\{TC(B^1,A),TC(B^2,A),...,TC(B^{NM(A)},A)\}$ (12)

[0091] 其中NM(A)≤η。随后，受信者A将TCs(A)发送给施信者C以证明自身可信赖。

[0092] 同理，作为受信者的节点C将TCs(C)发送给作为施信者的节点A以证明自己可信赖。

[0093] 步骤S4、施信者C收到受信者A的信任证明集合TCs(A)后，首先通过数字签名信息验证信任证明的真实性，提取出其中的信任证明，即$TC(B^1,A)$、$TC(B^2,A)$、…、$TC(B^{NM(A)},A)$，若NM(A)＜η，则施信者C对受信者A的信任值TV(C,A)被设为较小的常数τ∈[0,1)；否则，施信者C通过每条信任证明中的数字签名信息验证其真实性，然后导出每条信任证明对应的加权评估值并计算TV(C,A)。

[0094] 以施信者C导出TC(B,A)对应的加权评估值ST(C,B,A)为例：施信者C除考虑时间衰减权重WT(B,A)(即公式(10))外，还考虑兴趣偏好相似度权重WS(C,B)，该权重由施信者C与证明者B的兴趣偏好向量的加权欧式距离DS(C,B)导出，具体计算公式为：

[0095] $$DS(C,B)=\sqrt{\frac{\sum_{i=1}^{n}((WC(C,i)-WC(B,i))^2*WC(C,i))}{\sum_{i=1}^{n}WC(C,i)}} \quad (13)$$

[0096] WS(C,B)＝1-DS(C,B) (14)

[0097] 因此，TC(B,A)对应的加权评估值ST(C,B,A)可计算为：

[0098] ST(C,B,A)＝SC(B,A)*WT(B,A)*WS(C,B) (15)

[0099] 根据公式(13)-(15)所述方法，施信者C能够导出$TC(B^1,A)$、$TC(B^2,A)$、…、$TC(B^\eta,A)$对应的加权评估值，并计算对受信者A的信任值TV(C,A)，具体公式为：

[0100] $$TV(C,A)=\frac{\sum_{j=1}^{\eta}ST(C,B^j,A)}{\eta} \quad (16)$$

[0101] 由公式(13)-(16)可推得WS(C,B)、ST(C,B,A)、TV(C,A)的范围均为[0,1]。

[0102] 若TV(C,A)≥TH(C)(其中TH(C)∈[0,1]为节点C的信任门限)，则施信者C同意与受信者A交互，反之亦然。

[0103] 同理，作为施信者的节点A也能够根据作为受信者的节点C提供的信任证明集合TCs(C)导出对受信者C的信任值TV(A,C)，并根据与自身信任门限TH(A)的大小关系决定是否同意与受信者C交互。

[0104] 当且仅当TV(C,A)≥TH(C)且TV(A,C)≥TH(A)时，节点A与节点C进行交互。

[0105] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，

均应为等效的置换方式,都包含在本发明的保护范围之内。

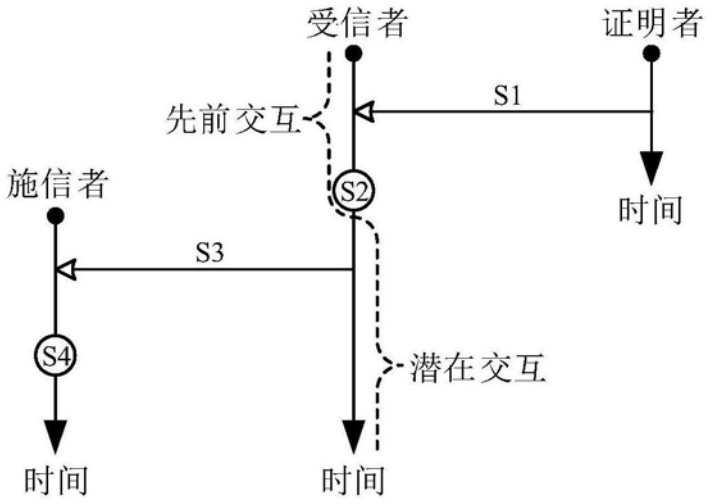

受信者
证明者
S1
先前交互
施信者
S2
时间
S3
S4
潜在交互
时间
时间

图1

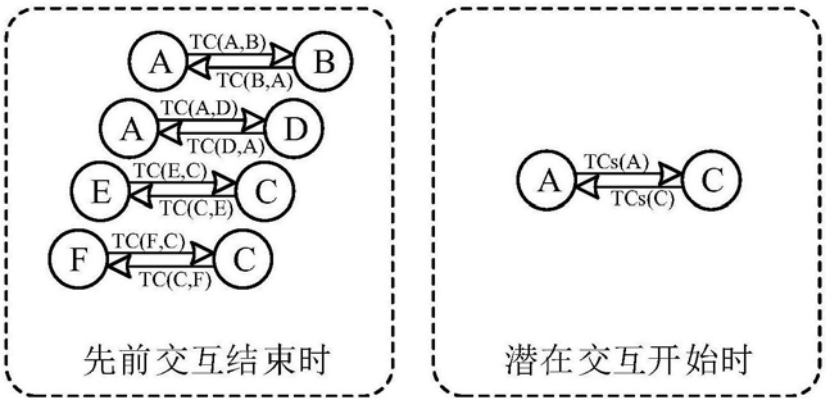

A
TC(A,B)
TC(B,A)
B
A
TC(A,D)
TC(D,A)
D
E
TC(E,C)
TC(C,E)
C
F
TC(F,C)
TC(C,F)
C
先前交互结束时
A
TCs(A)
TCs(C)
C
潜在交互开始时

图2