(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 109195162 A
(43)申请公布日 2019.01.11

(21)申请号 201811190159.9

(22)申请日 2018.10.12

(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 魏凯敏 冯丙文 魏林锋

(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.
H04W 12/02(2009.01)
H04L 29/06(2006.01)
H04W 24/10(2009.01)
H04W 4/021(2018.01)
H04L 9/32(2006.01)

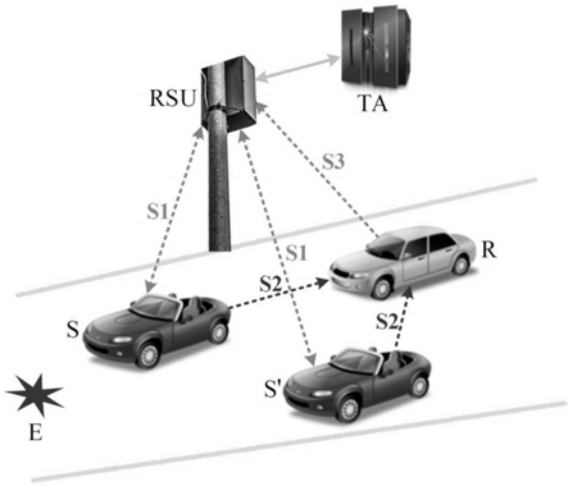
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种车联网中聚合两种信任评估的消息可靠性评估方法

(57)摘要

本发明公开了一种车联网中聚合两种信任评估的消息可靠性评估方法，其中，信任中心负责维护车辆的信任信息，车辆定期向信任中心请求自己最新的信任证书；消息发布者发送消息时附带最新的信任证书以证明自己可信赖；消息接收者收到每条消息后提取信任证书并综合考虑多个消息发布者的消息以判断其是否可靠，然后根据消息质量为每个消息发布者生成一条信任反馈，并发送至信任中心，随后信任中心更新本地存储。本发明高效聚合两种信任评估，且无需消息接收者实时请求信任中心，因而评估结果更加准确，评估速度更快，且兼容车辆短时间内无法连接到信任中心的情况，更符合车联网的高动态特性。



CN 109195162 A

1.一种车联网中聚合两种信任评估的消息可靠性评估方法，该车联网包括信任中心、若干路侧单元和节点，节点与路侧单元通过其他节点的中继进行无线通信，而路侧单元与信任中心之间采用有线通信方式，其中，信任中心负责维护节点的信任信息，每当间隔Δt时间更新各节点的信任值，对于每个节点，信任中心首先在本地存储中选出其他节点对该节点的最新的至多η条信任反馈，并据此计算该节点的最新信任值，然后用其覆盖先前存储的该节点的信任值，其特征在于，所述的评估方法如下：

步骤S1、各节点每当间隔Δt时间且进入某个路侧单元通信范围后向信任中心请求自身节点最新的信任证书，信任中心收到某节点S的请求信息后，首先验证请求信息确实来自于该节点，并在本地存储中检索该节点的最新信任值，然后为其生成信任证书，信任中心通过路侧单元将信任证书发送给该节点，并通过非对称加密方式保证其机密性，该节点收到信任证书后更新本地存储以备发送消息时使用；

步骤S2、当某事件E发生时，临近节点能够目击其发生，并作为消息发布者向后面节点广播该事件，当某节点R作为消息接收者收到报告某事件E或其对立事件-E的消息时，根据节点R与事件发生地的距离DT(R,E)和最大识别距离、最大决策距离、最大影响距离的大小关系决定节点R的判断策略；

步骤S3、当某节点R作为消息接收者与事件发生地的距离DT(R,E)小于或等于最大识别距离时，能够目击事件E的实际状态，并对先前收到的每条消息的质量进行评级，同时为每个消息发布者生成一条信任反馈，当消息接收者进入某个路侧单元通信范围后将信任反馈发送至信任中心，随后信任中心验证其签名信息并更新本地存储。

2.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，所述的信任反馈的格式为：

TF(A,S)＝(ID(A),ID(S),TR(A,S),TS(A,S),DS(A,S))，

其中，ID(A)和ID(S)分别表示反馈者A和节点S的唯一标识符，TR(A,S)表示反馈者A根据节点S先前的消息质量生成的评级分数，TS(A,S)表示TF(A,S)生成时的时间戳，DS(A,S)表示数字签名信息。

3.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，所述的步骤S2中根据节点R与事件发生地的距离DT(R,E)和最大识别距离、最大决策距离、最大影响距离的大小关系决定节点R的判断策略具体如下：

S21、当DT(R,E)大于最大影响距离时，节点R直接丢弃报告事件E或其对立事件-E的消息；

S22、当DT(R,E)介于最大决策距离和最大影响距离之间时，节点R验证所收消息中的数字签名信息并存储报告事件E或其对立事件-E的消息；

S23、当DT(R,E)介于最大识别距离和最大决策距离之间时，节点R根据收到的多条来自于不同节点的报告事件E或其对立事件-E的消息进行综合决策；

S24、当DT(R,E)小于或等于最大识别距离时，节点R能够目击事件E的实际状态，并对先前收到消息的质量进行评级。

4.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，所述的步骤S23中节点R根据收到的多条来自于不同节点的报告事件E或其对立事件-E的消息进行综合决策的过程如下：

1)若节点R对事件E的综合信任值TV(R,E)>0,则作为消息接收者的节点R信任事件E,并认为所有报告事件E的消息可靠,所有报告事件-E的消息不可靠,同时,节点R遵照报告事件E的消息采取行动;

2)若节点R对事件E的综合信任值TV(R,E)<0,则作为消息接收者的节点R信任事件-E,并认为所有报告事件-E的消息可靠,所有报告事件E的消息不可靠,同时,节点R遵照报告事件-E的消息采取行动;

3)若节点R对事件E的综合信任值TV(R,E)=0,则作为消息接收者的节点R不信任事件E和事件-E,并认为所有报告事件E和事件-E的消息不可靠,同时,节点R不采取任何行动。

5.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法,其特征在于,所述的步骤S23中,设多个消息发布者为节点S、节点S′、…,集合表示为SS(E),即SS(E)={S,S′,…},其元素个数记为|SS(E)|,对应消息为MS(S,E)、MS(S′,E)、…,报告事件E和对立事件-E分别用1和-1表示,作为消息接收者的节点R在计算事件E的综合信任值TV(R,E)时考虑以下权重:

1)消息发布者信任值权重Ws(R,S,E):由信任证书中所提取的消息发布者S的信任值TV(S)所决定,计算公式为:

Ws(R,S,E)=TV(S);

2)信任证书的时间衰减权重Wc(R,S,E):根据当前时间戳TN和信任证书中时间戳的时间差进行指数衰减,计算公式为:

$$\mathrm{Wc(R,S,E)}=e^{-\frac{TN-\mathrm{TS(TA,S)}}{\varphi}},$$

其中φ为信任衰减因子,控制Wc(R,S,E)随时间差衰减的速度;

3)消息的时间衰减权重Wm(R,S,E):根据当前时间戳TN和消息中时间戳的时间差进行指数衰减,计算公式为:

$$\mathrm{Wm(R,S,E)}=e^{-\frac{TN-\mathrm{TS(S,E)}}{\psi}},$$

其中ψ为信任衰减因子,控制Wm(R,S,E)随时间差衰减的速度。

所述的综合信任值TV(R,E)的值由以下公式导出:

$$\mathrm{TV(R,E)}=\frac{\sum_{S\in SS(E)}\pm 1*\mathrm{Ws(R,S,E)}*\mathrm{Wc(R,S,E)}*\mathrm{Wm(R,S,E)}}{|\mathrm{SS(E)}|}$$

$$=\frac{\sum_{S\in SS(E)}\pm 1*\mathrm{TV(S)}*e^{-\frac{TN-\mathrm{TS(TA,S)}}{\varphi}}*e^{-\frac{TN-\mathrm{TS(S,E)}}{\psi}}}{|\mathrm{SS(E)}|}。$$

6.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法,其特征在于,信任中心更新节点S的信任值TV(S)的过程中考虑的权重包括:

1)反馈者信任值权重Wf(A,S):由反馈者A的信任值决定,计算公式为:

Wf(A,S)=TV(A);

2)时间衰减权重Wt(A,S):根据当前时间戳TN和信任反馈中时间戳的时间差进行指数衰减,计算公式为:

$$\mathrm{Wt(A,S)} = e^{-\frac{TN-TS(A,S)}{\lambda}},$$

其中λ为信任衰减因子，控制Wt(A,S)随时间差衰减的速度；

所述的信任值TV(S)的计算公式如下：

如果关于节点S的信任反馈的总数量小于η，则信任值TV(S)被设为较小的信任初值，即：

TV(S)＝τ∈[0,1]，

否则，信任值TV(S)由以下公式导出：

$$\mathrm{TV(S)} = \frac{\sum_{A\in FS(S)} TR(A,S)*\mathrm{Wf(A,S)}*\mathrm{Wt(A,S)}}{4*\eta} = \frac{\sum_{A\in FS(S)} TR(A,S)*\mathrm{TV(A)}*e^{-\frac{TN-TS(A,S)}{\lambda}}}{4*\eta}。$$

7.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，节点S发送给信任中心的请求信息格式为：

RQ(S,TA)＝(ID(S),TS(S,TA),DS(S,TA))，

其中ID(S)表示节点S的唯一标识符，TS(S,TA)表示生成RQ(S,TA)时的时间戳，DS(S,TA)表示数字签名信息。

8.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，信任中心为节点S生成的信任证书的格式为：

TC(TA,S)＝(ID(S),TV(S),TS(TA,S),DS(TA,S))，

其中ID(S)表示节点S的唯一标识符，TV(S)为节点S的信任值，TS(TA,S)表示生成该信任证书时的时间戳，DS(TA,S)表示数字签名信息。

9.根据权利要求1所述的一种车联网中聚合两种信任评估的消息可靠性评估方法，其特征在于，所述的TR(A,S)表示反馈者A根据节点S先前的消息质量生成的评级分数，其取值为0-4之间的整数，且消息质量越高，评级分数越高。

一种车联网中聚合两种信任评估的消息可靠性评估方法

技术领域

[0001] 本发明涉及车联网安全技术领域，具体涉及一种车联网中聚合两种信任评估(即面向实体的信任评估和面向数据的信任评估)的消息可靠性评估方法。

背景技术

[0002] 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，能够提供各类信息服务、提高行车安全与效率、促进节能减排。

[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。例如，恶意车辆(“车辆”也称“节点”或“实体”)可能散布大量的虚假消息(“消息”也称“数据”或“报告”)以欺骗其他节点，进而对道路交通的安全性和可靠性造成极大的威胁。因此，每个节点需要甄别其他诚实节点和恶意节点、真实消息和虚假消息，并遵照诚实节点发布的真实消息以做出正确的决策。

[0004] 信任管理作为一种能够解决不确定性问题的理论，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检测其他恶意节点和虚假消息以避免严重后果。当前，车联网中的信任管理仍然处于初级阶段。根据评估对象，现有的信任评估方法可大致分为面向实体的信任评估和面向数据的信任评估。

[0005] Park等人[S.Park,B.Aslam,and C.C.Zou,“Long-term reputation system for vehicular networking based on vehicle’s daily commute routine,”in Proc.2011CNCC,2011,pp.436-441.]提出一个基于基础设施的长期声望模型，其中路侧单元负责监测车辆的日常行为并维护其信任信息，但该模型孤立考虑每个消息发送者的消息，完全忽略了面向数据的信任，因而其实际性能受到限制。Huang等人[Z.Huang,S.Ruj,M.A.Cavenaghi,M.Stojmenovic,and A.Nayak,“A social network approach to trust management in VANETs,”Peer Peer Netw.Appl.,vol.7,no.3,pp.229-242,Sep.2014.]从社交网络的视角提出一个新颖的信任模型，其中消息接收者同时考虑报告某事件及其对立事件的消息以综合判断其是否可靠，但该模型完全忽略了面向实体的信任，并赋予诚实车辆的消息和恶意车辆的消息以相同的权重，因而其实际性能不佳。

发明内容

[0006] 本发明的目的是为了解决现有技术中的上述缺陷，提供一种车联网中聚合两种信任评估的消息可靠性评估方法。

[0007] 本发明的目的可以通过采取如下技术方案达到：

[0008] 一种车联网中聚合两种信任评估的消息可靠性评估方法，该车联网包括信任中心、若干路侧单元和节点，节点与路侧单元通过其他节点的中继进行无线通信，而路侧单元与信任中心之间采用有线通信方式，其中，信任中心负责维护节点的信任信息，每当间隔Δt时间更新各节点的信任值，对于每个节点，信任中心首先在本地存储中选出其他节点对该

节点的最新的至多η条信任反馈，并据此计算该节点的最新信任值，然后用其覆盖先前存储的该节点的信任值，所述的评估方法如下：

[0009] 步骤S1、各节点每当间隔Δt时间且进入某个路侧单元通信范围后向信任中心请求自身节点最新的信任证书，信任中心收到某节点S的请求信息后，首先验证请求信息确实来自于该节点，并在本地存储中检索该节点的最新信任值，然后为其生成信任证书，信任中心通过路侧单元将信任证书发送给该节点，并通过非对称加密方式保证其机密性，该节点收到信任证书后更新本地存储以备发送消息时使用；

[0010] 步骤S2、当某事件E发生时，临近节点能够目击其发生，并作为消息发布者向后面节点广播该事件，当某节点R作为消息接收者收到报告某事件E或其对立事件-E的消息时，根据节点R与事件发生地的距离DT(R,E)和最大识别距离、最大决策距离、最大影响距离的大小关系决定节点R的判断策略；

[0011] 步骤S3、当某节点R作为消息接收者与事件发生地的距离DT(R,E)小于或等于最大识别距离时，能够目击事件E的实际状态，并对先前收到的每条消息的质量进行评级，同时为每个消息发布者生成一条信任反馈，当消息接收者进入某个路侧单元通信范围后将信任反馈发送至信任中心，随后信任中心验证其签名信息并更新本地存储。

[0012] 进一步地，所述的信任反馈的格式为：

[0013] TF(A,S)＝(ID(A),ID(S),TR(A,S),TS(A,S),DS(A,S))，

[0014] 其中，ID(A)和ID(S)分别表示反馈者A和节点S的唯一标识符，TR(A,S)表示反馈者A根据节点S先前的消息质量生成的评级分数，TS(A,S)表示TF(A,S)生成时的时间戳，DS(A,S)表示数字签名信息。

[0015] 进一步地，所述的步骤S2中根据节点R与事件发生地的距离DT(R,E)和最大识别距离、最大决策距离、最大影响距离的大小关系决定节点R的判断策略具体如下：

[0016] S21、当DT(R,E)大于最大影响距离时，节点R直接丢弃报告事件E或其对立事件-E的消息；

[0017] S22、当DT(R,E)介于最大决策距离和最大影响距离之间时，节点R验证所收消息中的数字签名信息并存储报告事件E或其对立事件-E的消息；

[0018] S23、当DT(R,E)介于最大识别距离和最大决策距离之间时，节点R根据收到的多条来自于不同节点的报告事件E或其对立事件-E的消息进行综合决策；

[0019] S24、当DT(R,E)小于或等于最大识别距离时，节点R能够目击事件E的实际状态，并对先前收到消息的质量进行评级。

[0020] 进一步地，所述的步骤S23中节点R根据收到的多条来自于不同节点的报告事件E或其对立事件-E的消息进行综合决策的过程如下：

[0021] 1)若节点R对事件E的综合信任值TV(R,E)>0，则作为消息接收者的节点R信任事件E，并认为所有报告事件E的消息可靠，所有报告事件-E的消息不可靠，同时，节点R遵照报告事件E的消息采取行动；

[0022] 2)若节点R对事件E的综合信任值TV(R,E)<0，则作为消息接收者的节点R信任事件-E，并认为所有报告事件-E的消息可靠，所有报告事件E的消息不可靠，同时，节点R遵照报告事件-E的消息采取行动；

[0023] 3)若节点R对事件E的综合信任值TV(R,E)＝0，则作为消息接收者的节点R不信任

事件E和事件-E，并认为所有报告事件E和事件-E的消息不可靠，同时，节点R不采取任何行动。

[0024] 进一步地，所述的步骤S23中，设多个消息发布者为节点S、节点S′、…，集合表示为SS(E)，即SS(E)＝{S,S′,…}，其元素个数记为|SS(E)|，对应消息为MS(S,E)、MS(S′,E)、…，报告事件E和对立事件-E分别用1和-1表示，作为消息接收者的节点R在计算事件E的综合信任值TV(R,E)时考虑以下权重：

[0025] 1)消息发布者信任值权重Ws(R,S,E)：由信任证书中所提取的消息发布者S的信任值TV(S)所决定，计算公式为：

[0026] Ws(R,S,E)＝TV(S)；

[0027] 2)信任证书的时间衰减权重Wc(R,S,E)：根据当前时间戳TN和信任证书中时间戳的时间差进行指数衰减，计算公式为：

[0028] $$\mathrm{Wc(R,S,E)} = e^{-\frac{TN-\mathrm{TS(TA,S)}}{\varphi}},$$

[0029] 其中φ为信任衰减因子，控制Wc(R,S,E)随时间差衰减的速度；

[0030] 3)消息的时间衰减权重Wm(R,S,E)：根据当前时间戳TN和消息中时间戳的时间差进行指数衰减，计算公式为：

[0031] $$\mathrm{Wm(R,S,E)} = e^{-\frac{TN-\mathrm{TS(S,E)}}{\psi}},$$

[0032] 其中ψ为信任衰减因子，控制Wm(R,S,E)随时间差衰减的速度。

[0033] 所述的综合信任值TV(R,E)的值由以下公式导出：

$$\mathrm{TV(R,E)} = \frac{\sum_{S\in SS(E)} \pm 1 * \mathrm{Ws(R,S,E)} * \mathrm{Wc(R,S,E)} * \mathrm{Wm(R,S,E)}}{|\mathrm{SS(E)}|}$$

[0034]

$$= \frac{\sum_{S\in SS(E)} \pm 1 * \mathrm{TV(S)} * e^{-\frac{TN-\mathrm{TS(TA,S)}}{\varphi}} * e^{-\frac{TN-\mathrm{TS(S,E)}}{\psi}}}{|\mathrm{SS(E)}|}。$$

[0035] 进一步地，信任中心更新节点S的信任值TV(S)的过程中考虑的权重包括：

[0036] 1)反馈者信任值权重Wf(A,S)：由反馈者A的信任值决定，计算公式为：

[0037] Wf(A,S)＝TV(A)；

[0038] 2)时间衰减权重Wt(A,S)：根据当前时间戳TN和信任反馈中时间戳的时间差进行指数衰减，计算公式为：

[0039] $$\mathrm{Wt(A,S)} = e^{-\frac{TN-TS(A,S)}{\lambda}},$$

[0040] 其中λ为信任衰减因子，控制Wt(A,S)随时间差衰减的速度。

[0041] 所述的信任值TV(S)的计算公式如下：

[0042] 如果关于节点S的信任反馈的总数量小于η，则信任值TV(S)被设为较小的信任初值，即：

[0043] TV(S)＝τ∈[0,1]，

[0044] 否则，信任值TV(S)由以下公式导出：

[0045] $$\mathrm{TV(S)}=\frac{\sum_{A\in FS(S)}TR(A,S)*\mathrm{Wf(A,S)}*\mathrm{Wt(A,S)}}{4*\eta}=\frac{\sum_{A\in FS(S)}TR(A,S)*\mathrm{TV(A)}*e^{-\frac{TN-TS(A,S)}{\lambda}}}{4*\eta}。$$

[0046] 进一步地，节点S发送给信任中心的请求信息格式为：

[0047] RQ(S,TA)＝(ID(S),TS(S,TA),DS(S,TA))，

[0048] 其中ID(S)表示节点S的唯一标识符，TS(S,TA)表示生成RQ(S,TA)时的时间戳，DS(S,TA)表示数字签名信息。

[0049] 进一步地，信任中心为节点S生成的信任证书的格式为：

[0050] TC(TA,S)＝(ID(S),TV(S),TS(TA,S),DS(TA,S))，

[0051] 其中ID(S)表示节点S的唯一标识符，TV(S)为节点S的信任值，TS(TA,S)表示生成该信任证书时的时间戳，DS(TA,S)表示数字签名信息。

[0052] 进一步地，所述的TR(A,S)表示反馈者A根据节点S先前的消息质量生成的评级分数，其取值为0-4之间的整数，且消息质量越高，评级分数越高。

[0053] 本发明相对于现有技术具有如下的优点及效果：

[0054] 1)本发明聚合两种信任评估，且综合考虑报告某事件或其对立事件的来自于不同消息发送者的多条消息以评估其可靠性，因而评估结果更加准确。

[0055] 2)本发明所提方案无需消息接收者实时请求信任中心，因而评估速度更快。

[0056] 3)本发明所提方案兼容车辆短时间内无法连接到信任中心的情况，更符合车联网的高动态特性。

附图说明

[0057] 图1是本发明技术方案中主要步骤示意图；

[0058] 图2是本发明技术方案中三种距离(即最大识别距离、最大决策距离和最大影响距离)示意图。

具体实施方式

[0059] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0060] 实施例

[0061] 下面结合附图1和附图2对本发明所述的技术方案进行详细说明。

[0062] 发明所述的技术方案主要包括三种元素，即信任中心(Trust Authority,TA)、路侧单元(Road-Side Unit,RSU)和车辆(即节点,Node)，其中车辆与路侧单元通过其他车辆的中继进行无线通信，而路侧单元与信任中心之间采用有线通信方式。

[0063] 信任中心负责维护节点的信任信息，每当间隔Δt时间更新各节点的信任值。

[0064] 以计算节点S的信任值TV(S)为例，信任中心首先在本地存储中选出其他节点(即反馈者，如A、B、C等)对节点S的最新的至多η条信任反馈(即TF(A,S)、TF(B,S)、TF(C,S)等)，并将对应的反馈者加入节点S的反馈者集合FS(S)，即FS(S)＝{A,B,C,…}。

[0065] 信任反馈的格式为：

[0066] TF(A,S)＝(ID(A),ID(S),TR(A,S),TS(A,S),DS(A,S))， (1)

[0067] 其中，ID(A)和ID(S)分别表示反馈者A和节点S的唯一标识符，TR(A,S)表示反馈者A根据节点S先前的消息质量生成的评级分数(即0-4之间的整数，且消息质量越高，评级分数越高)，TS(A,S)表示TF(A,S)生成时的时间戳，DS(A,S)表示数字签名信息。TF(B,S)、TF(C,S)等其他信任反馈的格式与TF(A,S)一致。

[0068] 信任值TV(S)的计算过程中考虑的权重包括：

[0069] 1)反馈者信任值权重Wf(A,S)：由反馈者A的信任值决定，计算公式为：

[0070] Wf(A,S)＝TV(A)； (2)

[0071] 2)时间衰减权重Wt(A,S)：根据当前时间戳TN和信任反馈中时间戳的时间差进行指数衰减，计算公式为：

[0072] $$\mathrm{Wt(A,S)} = e^{-\frac{TN-TS(A,S)}{\lambda}}, \qquad (3)$$

[0073] 其中λ为信任衰减因子，控制Wt(A,S)随时间差衰减的速度。

[0074] 如果关于节点S的信任反馈的总数量小于η，则信任值TV(S)被设为较小的信任初值，即：

[0075] TV(S)＝τ∈[0,1]， (4)

[0076] 否则，信任值TV(S)由以下公式导出：

[0077] $$\mathrm{TV(S)} = \frac{\sum_{A\in FS(S)} TR(A,S)*\mathrm{Wf(A,S)}*\mathrm{Wt(A,S)}}{4*\eta} = \frac{\sum_{A\in FS(S)} TR(A,S)*\mathrm{TV(A)}*e^{-\frac{TN-TS(A,S)}{\lambda}}}{4*\eta} \qquad (5)$$

[0078] 由公式(2)-(5)可得Wf(A,S)、Wt(A,S)、TV(S)的范围均为[0,1]。

[0079] 在导出TV(S)的值后，信任中心用其覆盖先前存储的节点S的信任值。

[0080] 步骤S1、各节点每当间隔Δt时间且进入某个路侧单元通信范围后向信任中心请求自己最新的信任证书(Trust Certificate,TC)。以节点S为例，它发送给信任中心的请求信息格式为：

[0081] RQ(S,TA)＝(ID(S),TS(S,TA),DS(S,TA))， (6)

[0082] 其中ID(S)表示节点S的唯一标识符，TS(S,TA)表示生成RQ(S,TA)时的时间戳，DS(S,TA)表示数字签名信息。

[0083] 信任中心收到节点S的请求信息后，首先通过DS(S,TA)验证请求信息确实来自于节点S，并在本地存储中检索节点S的最新信任值TV(S)，然后为其生成信任证书，其格式为：

[0084] TC(TA,S)＝(ID(S),TV(S),TS(TA,S),DS(TA,S))， (7)

[0085]

[0086] 其中ID(S)表示节点S的唯一标识符，表示TS(TA,S)表示生成该信任证书时的时间戳，DS(TA,S)表示数字签名信息。随后，信任中心通过路侧单元将TC(TA,S)发送给节点S，并通过非对称加密方式保证其机密性。节点S收到TC(TA,S)后更新本地存储以备发送消息时使用。

[0087] 步骤S2、当某事件E(如道路结冰)发生时，临近节点(如节点S)能够目击其发生，并向后面节点广播该事件。节点S称为目击者，也称为消息发布者，其消息的格式为：

[0088] MS(S,E)＝(ID(S),MC(S,E),TC(TA,S),TS(S,E),DS(S,E))， (8)

[0089]

[0090] 其中ID(S)表示节点S的唯一标识符,MC(S,E)表示消息内容,TC(TA,S)表示节点S的信任证书,TS(S,E)表示生成该消息时的时间戳,DS(S,E)表示数字签名信息。

[0091] 在实际中,当某事件E发生时,可能有多个节点(如节点S、节点S'等)目击其发生并向后面节点报告。这些目击节点中可能存在部分恶意节点,它们会向后面节点报告事件E的对立事件-E(如道路畅通)以欺骗其他节点。因此,当某节点评估事件E的可靠性时,应尽可能同时考虑报告事件E或其对立事件-E的来自于不同消息发送者的多条消息以提高评估可靠性。

[0092] 当某节点(即消息接收者,如节点R)收到报告某事件E或其对立事件-E的消息时,根据它与事件发生地的距离DT(R,E)决定其具体策略。

[0093] 如图2所示,在事件发生地附近共设置三种距离,即最大识别距离、最大决策距离和最大影响距离:

[0094] 1)当DT(R,E)大于最大影响距离时,节点R直接丢弃报告事件E或其对立事件-E的消息;

[0095] 2)当DT(R,E)介于最大决策距离和最大影响距离时,节点R验证所收消息中的数字签名信息并存储报告事件E或其对立事件-E的消息;

[0096] 3)当DT(R,E)介于最大识别距离和最大决策距离时,节点R根据收到的多条来自于不同节点的报告事件E或其对立事件-E的消息进行综合决策;

[0097] 4)当DT(R,E)小于或等于最大识别距离时,节点R能够目击事件E的实际状态,并对先前收到消息的质量进行评级。

[0098] 在以上情形3)中,设多个消息发布者为节点S、节点S'等,集合表示为SS(E),即SS(E)={S,S′,…},其元素个数记为|SS(E)|,对应消息为MS(S,E)、MS(S′,E)等,报告事件E和对立事件-E分别用1和-1表示。

[0099] 消息接收者R在计算事件E的综合信任值TV(R,E)时考虑以下权重:

[0100] 1)消息发布者信任值权重Ws(R,S,E):由信任证书中所提取的消息发布者的信任值所决定,计算公式为:

[0101] $Ws(R,S,E)=TV(S)$; (9)

[0102] 2)信任证书的时间衰减权重Wc(R,S,E):根据当前时间戳TN和信任证书中时间戳的时间差进行指数衰减,计算公式为:

[0103] $$Wc(R,S,E)=e^{-\frac{TN-TS(TA,S)}{\varphi}}, \quad (10)$$

[0104] 其中φ为信任衰减因子,控制Wc(R,S,E)随时间差衰减的速度;

[0105] 3)消息的时间衰减权重Wm(R,S,E):根据当前时间戳TN和消息中时间戳的时间差进行指数衰减,计算公式为:

[0106] $$Wm(R,S,E)=e^{-\frac{TN-TS(S,E)}{\psi}}, \quad (11)$$

[0107] 其中ψ为信任衰减因子,控制Wm(R,S,E)随时间差衰减的速度。

[0108] TV(R,E)的值由以下公式导出:

$$TV(R,E)=\frac{\sum_{S\in SS(E)}\pm 1*Ws(R,S,E)*Wc(R,S,E)*Wm(R,S,E)}{|SS(E)|}$$

[0109]

$$=\frac{\sum_{S\in SS(E)}\pm 1*TV(S)*e^{-\frac{TN-TS(TA,S)}{\varphi}}*e^{-\frac{TN-TS(S,E)}{\psi}}}{|SS(E)|}。\qquad(12)$$

[0110] 由公式(9)-(12)可得Ws(R,S,E)、Wc(R,S,E)、Wm(R,S,E)的范围均为[0,1]，而TV(R,E)范围为[-1,1]。

[0111] 1)若TV(R,E)>0，则节点R信任事件E，并认为所有报告事件E的消息可靠，所有报告事件-E的消息不可靠。此外，节点R遵照报告事件E的消息采取行动。

[0112] 2)若TV(R,E)<0，则节点R信任事件-E，并认为所有报告事件-E的消息可靠，所有报告事件E的消息不可靠。此外，节点R遵照报告事件-E的消息采取行动。

[0113] 3)若TV(R,E)＝0(此情况在实际中极少出现)，则节点R不信任事件E和事件-E，并认为所有报告事件E和事件-E的消息不可靠。此外，节点R不采取任何行动。

[0114] 步骤S3、当消息接收者R与事件发生地的距离小于或等于最大识别距离时，能够目击事件E的实际状态，并对先前收到的每条消息的质量进行评级，同时为每个消息发布者生成一条信任反馈，其格式如公式(1)所示。此外，当消息接收者R进入某个路侧单元通信范围后将信任反馈发送至信任中心，随后信任中心验证其签名信息并更新本地存储。

[0115] 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。

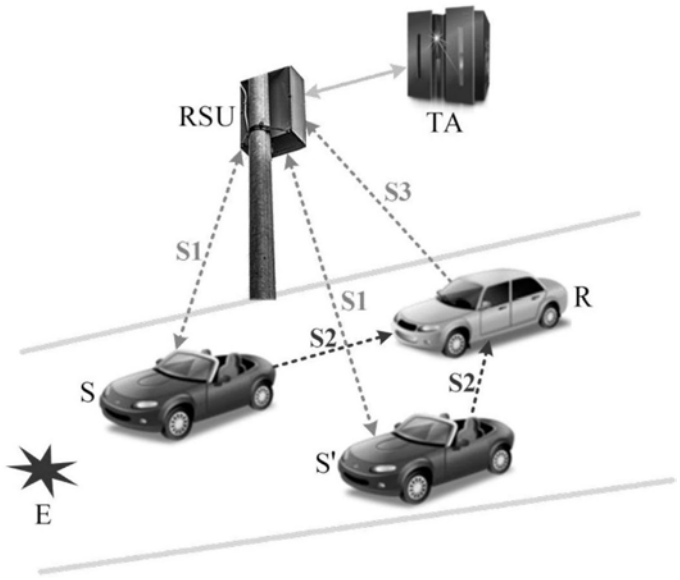


图1

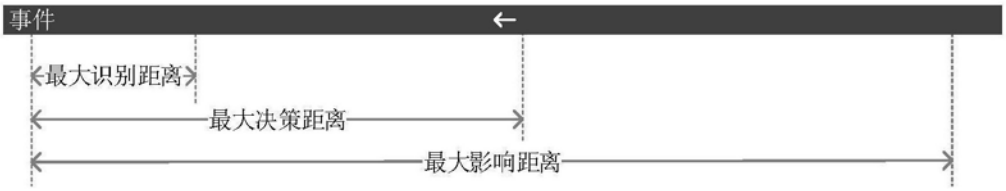


图2