行为证据不全对无线传感器网络信任评估的影响与性质分析

田立勤[1,2] 林 闯[2]

(华北科技学院计算机系 北京 101601)[1] (清华大学计算机科学与技术系 北京 100084)[2]

摘 要 在无线传感器网络中单独基于节点身份认证的静态安全控制不能满足动态的安全需要,必须结合节点动态的行为可信确认才能更好地提供安全保障,因此基于行为可信的研究已经成为业界研究无线传感器网络的热点。在节点行为信任评估中,行为证据是行为评估的根本依据,但由于节点的行为是随机的,不确定的,因此能否获得证据也是随机的,不确定的,这就造成了节点行为证据不全、每次交往的行为价值不相等的现象,但目前在无线传感器网络的行为信任评估中很少考虑这个非常重要的现象。分析了节点交往中行为证据不全对信任评估带来的重要影响,论述了节点交往中证据不全与节点行为价值的关系,给出了不足填充法和权重扩展法等针对不同价值交往的节点信任评估策略。最后通过两个定理和两个性质证明了方法对节点行为信任评估的作用和性质,这为提高节点行为信任的价值可信度奠定了量化基础。

关键词 无线传感器网路,节点行为证据,节点行为价值,节点行为信任

中图法分类号 TP393 **文献标识码** A

Influence and Analysis of the Incomplete Behavior Evidence on Trust Evaluation in WSNs

TIAN Li-qin[1,2] LIN Chuang[2]

(Department of Computer Science and and Technology, North China Institute of Science and Technology, Beijing 101601, China)[1]

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[2]

Abstract In wireless sensor networks, single static identity-based node authentication can't meet the dynamic security needs. In order to provide better security we must combine dynamic behaviour-based node trust with static identity-based node authentication. In node behavior trust evaluation, behavior evidence is the fundamental basis of behavior evaluation. Because the node's behavior is random, uncertain, which causes behavior evidence was not complete and behavior value is not equal in each interaction, but as far as we know, this very important phenomenon in behavior trust evaluation is rarely considerd. This paper analyzed incomplete behavior evidence obtained in node interaction brings about a significant impact on trust evaluation and discussed the relationship between incomplete behavior evidence and behavior value, gave a kind of behavior trust evaluation strategy for different values interaction such as Less-Filling and Weight-Extension. Finally, we used two theorems and two properties to prove strategy's effect and property in behavior trust evaluation. Paper lays the quantity foundation in enhancing value-trust reliability of node behavior trust.

Keywords Wireless sensor network, Node behavior evidence, Node behavior value, Node behavior trust

1 引言

在无线传感器网络这种新型网络应用中,单独的基于节点身份认证的静态安全控制不能满足动态的安全需要,必须结合动态的行为可信确认才能更好地提供安全保障[1-4]。如,在无线传感器网络中,由于节点被敌方捕获,节点的身份可能被暴露并伪造合法的身份,但这时被捕获的恶意的节点的行为已经是不可信的了。因此,对节点行为进行可信确认是无线传感器网络应用的需求,是对身份认证和内容认证的重要补充。在行为可信认证中,行为证据是行为可信认证的基础[5],分析节点行为证据的特性和行为的价值对提高节点行为可信评估的可信性具有重要意义。本文分析了节点交往中行为证据不全对信任评估带来的重要影响,论述了节点不同交往中证据不全与节点行为价值的关系,给出了不足填充法和权重扩展法等针对不同价值交往的节点信任评估策略。最后通过两个定理和两个性质证明了方法对节点行为信任评估的作用和性质,这为提高节点行为信任的价值可信度奠定了量化基础。

2 节点行为证据的分类

定义1(节点行为证据) 节点行为证据是指在节点交往过程中施信节点(主体)可直接根据软硬件检测获得的用来定

到稿日期:2009-11-24 返修日期:2010-01-20 本文受国家重点基础研究发展规划(973计划)项目(No. 2010CB328105),国家自然科学基金项目(No. 60872055,60673187,60803123),中国博士后科学基金(No. 20090460320),河北省自然科学基金与发展指导项目(No. F2010001745,No. 07213570),国家安全监管总局安全生产重大事故防治关键技术重点科技项目(No. 10-120)资助。

田立勤(1970—),男,博士后,教授,硕士生导师,主要研究方向为计算机网络、无线传感器网络和可信网络,E-mail:tianliqin@tsinghua.org.cn;
林 闯(1948—),男,博士,教授,博士生导师,主要研究方向为系统性能评价、网络安全、随机Petri网、逻辑推理模型等。

量评估待测求信节点(客体)行为信任的基础数值,它具有客观性,本身不具有信任的主观特性,本文用 et 表示。我们很容易找到常见的证据,例如节点回应比例,节点的剩余能量值、节点回应时间、报文丢失率、位置变化次数等[6]。施信节点搜集到的节点行为证据不仅量大而且比较杂,因此要想很好地利用它们来研究具有针对性的问题,必须对它们进行分类。

定义 2(节点行为信任属性) 节点行为信任属性是与某一类应用服务相关的所有行为证据的有机组合。例如,安全行为属性是与安全有关的所有行为证据的有机组合。目前我们将证据分成 3 种最常见的行为信任属性,即,安全行为属性、可靠性行为属性和性能行为属性。由于评估的原理和方法是一致的,因此可以在研究中根据需要进行扩展。根据获得的证据值落在不同的取值范围,我们可以把证据分为 7 个信任等级:完全信任、信任、比较信任、可信任、不确定信任(陌生信任)、预警信任和不信任。

3 基于行为证据的节点行为信任评估的模型与计算方法

3.1 基于行为证据的节点行为信任评估模型

本文采用层次组合模型来计算基于行为证据的节点行为信任。由定义 1 可知,求信节点行为证据是指可用软硬件直接测量获得的数据,它具有客观性和确定性等特性,但信任最初是从社会学衍生出来的,具有主观性、笼统性等特性[7],这种社会学科的信任不利于对节点行为信任进行量化评估。层次组合模型的步骤是:先根据实际应用需求和功能特性将整体的节点行为信任进行逐层分解,将综合的、笼统的节点行为信任分解为若干行为信任属性,再将行为信任属性继续细化为可用软硬件直接测量的行为信任证据,这样可以有效解决节点行为信任的笼统性和不确定性问题。

3.2 基于行为证据的节点行为信任的量化评估

由定义 2 知,节点行为信任属性是某一类相关的具有一定应用背景的所有行为证据的有机组合。例如,安全行为属性是与安全有关的所有行为证据的有机组合。我们用矩阵的方法求节点的行为信任属性,设 n 表示节点行为信任包含信任属性的项数,p 表示所有信任属性中包含信任证据项数的最大值,没有达到最大值 p 的可以让对应的权值为 0,$et_{ij}\in[0,1]$表示第 i 个信任属性的第 j 个证据,$ew_{ij}\in[0,1]$表示第 i 个信任属性的第 j 个信任证据的权值,即有:

证据矩阵 $E=\begin{bmatrix} et_{11} & \cdots & et_{1f} & \cdots & et_{1p} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ et_{i1} & \cdots & et_{if} & \cdots & et_{ip} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ et_{n1} & \cdots & et_{nf} & \cdots & et_{np} \end{bmatrix}$,权值矩阵 $WE=$

$\begin{bmatrix} ew_{11} & \cdots & ew_{1f} & \cdots & ew_{1p} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ ew_{i1} & \cdots & ew_{if} & \cdots & ew_{ip} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ ew_{n1} & \cdots & ew_{nf} & \cdots & ew_{np} \end{bmatrix}$,这里的权值 ew_{ij} 为 0 的可能性有:属性的证据项数没有达到最大值 p 或者施信节点对相应的证据不感兴趣。计算信任属性的公式为:

$$E*WE^T \tag{1}$$

结果只取主对角线值或只计算主对角线的值就可得到各个信任属性值。

有了信任属性值,就可以计算信任了,设节点行为信任的属性向量 A 为 $\begin{bmatrix} a_1 \\ \cdots \\ a_i \\ \cdots \\ a_n \end{bmatrix}$,信任属性的权值向量 $WA=\begin{bmatrix} wa_1 \\ \cdots \\ wa_i \\ \cdots \\ wa_n \end{bmatrix}$,则节点行为信任的计算公式为:

$$tru=A*WA^T=\sum_{i=1}^{n}a_i wa_i \tag{2}$$

4 行为证据获得的不完全性与行为的价值分析

定义 3(节点行为证据获得的不完全性) 节点行为证据获得的不完全性是指如果施信节点不能全部获得它所希望的全部证据就称为证据获得不完全。

在节点交往的过程中,由于节点的行为是随机的,不确定的,因此获得证据也是随机的,不确定的。执行了某些行为,与这些行为的相关证据就可以获得,不执行某些行为,相关的证据就不能获得[8]。在实际的无线传感器网络的应用中,会出现施信节点对求信节点证据获得不全的情况,这对信任评估带来重大影响,理由包括:首先当节点行为证据不全时,如果只按实际已经获得的证据及原有的权重进行计算行为信任,那么权重的和不再等于 1,计算的结果必定是错误的;其次,即使我们把权重扩充到 1,如果证据较少,那么本次的信任评估不能代表本次节点行为信任真实的评估结果,失真比较严重;第三,如果只按已经获得的低价值证据进行信任评估,那么恶意节点可能用"低价值"的节点交往换取高信任的欺骗行为,即,虽然每次节点行为信任的评估结果很高,但它这个高信任不能说明关键高价值的行为是否可信。因此对节点行为信任的评估需要考虑每次节点交往的重要性,即价值,但如何表示交往的价值是问题的关键所在。因为证据的权重代表各个证据的重要程度,那么节点每次交往实际获得的 $m1$ 个证据权重和 $ew_1+ew_2+\cdots+ew_{m1}$ 在数量上就代表节点该次交往的价值,本文用 v_i 表示。注意:证据的权重是通过两两比较获得的,一般情况下只有在同一个信任属性范围内才具有可比性,因此讨论交往价值是在同一个信任属性范围内的。

定义 4(节点行为价值) 节点行为价值是指求信节点每次与施信节点交往后实际获得的证据所对应的权重和,它体现该节点当次交往的重要性和价值,即 $v_i=ew_1+ew_2+\cdots+ew_{m1}$。

当所有证据都能得到时,各个证据所对应的权重总和等于 1,这时该节点的交往价值达到最大。如果不能全部获得,则该信任各个证据的权重和在[0,1]之间。设两个价值参数 $V_{\min},V_{\max}\in[0,1]$,它们分别代表行为信任评估所要求的权重的最小和与最大和,这两个参数在实际评估中可根据实际应用和评估的粒度进行配置。

下面定义在行为证据获得不完全的情况下的微价值交往、中等价值交往、高价值交往和全价值交往行为。

定义 5(微价值交往) 当 $0\leqslant v_i<V_{\min}$ 时称该节点的交往是微价值交往。

定义 6(中等价值交往) 当 $0\leqslant V_{\min}<v_i<V_{\max}<1$ 时称

该节点的交往是中等价值交往。

定义 7（高价值交往） 当 $1>v_i>V_{max}$ 时称该节点的交往是高价值交往。

定义 8（全价值交往） 当 $v_i=1$ 时称该节点的交往是全价值交往，设这时全部证据个数为 N。

5 不同价值交往的节点行为信任评估方法

当节点的交往是全价值交往，即 $v_i=1$ 时，信任评估的效果是最理想的[9]，这时按式(1)和式(2)直接计算节点的行为信任即可。当节点的交往是微价值交往时，由于施信节点实际获得的证据所对应的权重和 v_i 小于行为信任评估所需要的最小权重和 V_{min}，因此该次交往对于施信节点来说没有什么评估的价值，此次交往的信任评估作废，即此次交往不参与实际评估。

5.1 中等价值交往的节点行为信任评估方法——不足填充法

5.1.1 中等价值交往时的行为信任属性评估分析

当节点的交往是中等价值交往时，该次交往具有评估的价值，因此不能作废，作废就损失了一次评估机会，因为评估的可信性是与评估次数和规模有关的[10]，因此不能随意放弃。但由于信任证据缺项比较多，直接按比例扩充权重，会犯以偏代全的错误，信任的真实性和可信性会大大降低。

我们采取的策略是不足填充法，填充替代的策略有好几种：第一种是用陌生节点的缺省信任证据代替未获得的证据，这个证据通常是信任等级比较小的证据，对于可信节点来说这种替换降低了实际信任值，对于不可信节点来说这种替换增加了实际信任值；第二种策略是用以往全部节点对应的证据平均值代替，这种代替方法的替代数据比较粗糙，不够精细和准确；第三种替代策略是用该节点以往对应的证据均值代替，这种代替方法的替代数据比较准确和合理，但缺点是：(1)当以往节点交往的次数比较少时，假设低于 N_{min} 次的交往规定为比较少的交往，这时替代值的准确度就有可能很差，同样会出现以偏代全的情况，给恶意节点留下信任欺骗的空隙；(2)当以往节点的行为证据时间比较久远的时候，证据的信任价值在节点行为可信评估中已经衰减，不能准确反映节点的最近行为的真实性；(3)当以往节点行为的证据波动较大时，其平均值不能代表该节点的真实行为。

5.1.2 中等价值交往的行为信任属性评估策略

从上面的分析我们可以看到，三种策略中的每一种都有其弊端，本文采用的策略是对前面三种策略的综合与折中。我们以第三种较为合理的替代方法为基础，对其三个缺陷进行改进，以达到防止以偏代全和恶意节点欺骗的目的。基本思路是：解决由于节点在过去有效时间范围内交往次数比较少而导致的代替误差较大问题。

为了对节点中等价值交往进行信任评估，我们建立一个存放第 i 个历史证据 et_i 的二维表：每个历史记录包括以往的证据 et_i 及其获得证据的时间 t_i 两个字段，即证据为 $et_{i1}, et_{i2}, \cdots et_{im}, \cdots$，时间为 $t_{i1}, t_{i2}, \cdots t_{im}, \cdots$，并设证据对应的权重为 w_i，记录是按时间从远到近排序的，即 $t_{i1}<t_{i2}<\cdots<t_{im}$。另设一个近期有效时间跨距 $T0$，定期检查证据表，对这个表做如下两种操作：

(1)追加操作：新获得的证据追加到这个表尾；

(2)删除：删除包括两种，第一种是从第一个记录 et_{i1} 开始循环检查证据 et_{ij} 的 $|t_{im}-t_{ij}|$ 是否大于 $T0$，即证据记录时间是否超过 $T0$ 有效时间跨距，如果是，则将 et_{ij} 从这个表中删除，保证记录的时间有效性；第二种是当记录个数超过表最大的记录限制个数 N_{min} 时，删除时间最远的记录，保证策略的可扩展性，我们看到这两种操作不破坏表的记录排序顺序。经过上述增删后，表中的剩余记录数设为 n，并计算剩余记录的证据值的平均值 $\overline{et_k}=\sum_{k=1}^{n} et_k/n$。

前面的增删策略保证了基于价值的信任评估的时间有效性和可扩展性。在用以往的该节点的证据均值替换前，还要考虑节点在以往有效时间内的证据值是否稳定，如果稳定就可以用以往的节点的证据均值替换，否则因为较大的偏差而影响信任评估的可信性就不能替换，这里我们用方差来判断表中的证据的稳定性，设方差最小要求为 L，计算方差的公式为：

$$\sigma_n=\frac{1}{n}((et_{i1}-\overline{et_k})^2+(et_{i2}-\overline{et_k})^2+\cdots+(et_{in}-\overline{et_k})^2) \tag{3}$$

因此是否用自己以往的相应的证据均值替换与三个因素有关，即有效时间、交往次数和以往证据的方差。当节点以往实际交往次数 $n<N_{min}$ 但 $\sigma_n>L$ 时，则不能用自己以往的均值 $\overline{et_k}$ 替换，而用较低证据值的陌生节点的信任值 D 替换；当节点以往实际交往次数 $n<N_{min}$ 但 $\sigma_n\leqslant L$ 时，先用 n 次该节点以往的信任证据值进行求和，余下不足的用 $N_{min}-n$ 次陌生信任证据值 D 填充，然后将二者求和，最后除以最低要求次数 N_{min}，用式(4)计算 et_{mid}：

$$et_{mid}=\frac{(N_{min}-n)*D+\sum_{k=1}^{n} et_k}{N_{min}} \tag{4}$$

当节点以往实际交往次数 $n\geqslant N_{min}$ 时，如果 $\sigma_n>L$，则仍用 D 替换，否则用自己以往的相应的证据均值替换，即：

$$et_{mid}=\frac{\sum_{k=1}^{n} et_k}{n} \tag{5}$$

综合上面内容，对于中等价值的交往，未获得证据 et_i 的最终替代可用式(6)进行概括：

$$et_i=\begin{cases} D & \sigma_n>L \\ \sum_{k=1}^{n} et_k/n & n\geqslant N_{min}\ \ \sigma_n\leqslant L \\ ((N_{min}-n)*D+\sum_{k=1}^{n} et_k)/N_{min} & n<N_{min}\ \ \sigma_n\leqslant L \end{cases} \tag{6}$$

从上面的公式可以看到，在中等价值交往中，开始替换值的有效率随着交往的次数 n 的增加而增加，当次数大于最低次数要求 N_{min} 时，由 $\sum_{k=1}^{n} et_k/n$ 知，替换值的有效率与交往的次数 n 成正比例，达到最高。随后，当 $n>N_{max}$ 时，为了算法扩展性，一些有效的记录从表中被删除了。

在中等价值交往中，采用不足填充法求节点信任时，本次获得的证据值保持不变，未获得的证据用式(6)计算填充，各个证据的权重保持不变，就可以用式(1)和式(2)求节点行为信任。

5.2 高价值交往时的节点行为信任评估方法——权重扩展法

当节点的交往是高价值但不是全价值交往时，未获得的证据的价值较小，因此可以忽略，即只按已经获得的证据计算本次行为的信任即可，未获得的证据可以不再填充。

但这时如果仍然继续按照式(1)和式(2)计算节点的行为信任，则结果会出现错误，因为已获得证据对应的权重和不再等于1，其信任值最大也不会大于已获得证据对应权重的和 w_i，因此需要进行必要的处理，使得实际获得的行为证据所对应的权重之和最大可以扩充到1。

本文采取的措施是按原有权重的比例扩充现有的权重来保证 $w_i=1$。设原有的证据分别是 $ew_1, ew_2, \cdots, ew_N$，获得证据对应的权重分别是 $ew_1', ew_2', \cdots, ew_{m1}'$，其中 N 是该属性所包含的所有证据的个数，$m1$ 是该次交往实际获得的证据个数，通常 $m1<N$，扩充方法用下面的赋值语句：

$$ew_i'=\frac{ew_i'}{ew_1'+ew_2'+\cdots+ew_{m1}'} \tag{7}$$

在高价值交往中，用权重扩展法求节点信任时，证据值保持不变，就可以用式(1)和式(2)求节点行为信任。

5.3 基于不同价值交往的节点信任评估

不同的价值交往具有不同的行为信任评估策略，其评估流程图如图1所示。

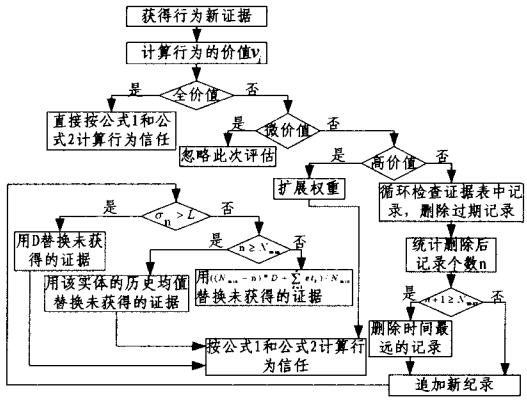

图1 不同的价值交往的信任评估策略

设第 i 个信任属性原来全部的证据为 N 个，其证据的权重分别是 $ew_1, ew_2, \cdots, ew_N$，获得证据个数为 $m2$ 个，其对应的权重分别是 $ew_1, ew_2, \cdots, ew_{m2}$，扩展后的权重为 ew_1'，$ew_2', \cdots, ew_{m2}'$；则基于不同价值交往的信任属性 a 评估方法为式(8)，有了信任属性值就可以根据式(2)求节点行为的信任值。

$$a=\begin{cases} no & w_i<W_1 \\ \sum_{i=1}^{m_2} ew_i et_i+\sum_{j=1}^{N-m_2} ew_j \overline{et} & W_1<w_i<W_2 \\ \sum_{i=1}^{m2} ew_i' et_i & w_i>W_2 \\ \sum_{i=1}^{N} ew_i et_i & w_i=1 \end{cases} \tag{8}$$

6 算法的改进，效果性质分析

6.1 算法的效果性质分析

在节点的行为信任评估中考虑交往价值可以提高信任评估的可信性，主要原因包括：(1)摒弃了没有多大交往价值的行为信任评估，增加了每次评估的有效性；(2)对于高价值的交往修正了评价中最高信任不能为1的缺陷；(3)对于那些中等价值的交往，给出了针对不同情况下对未获得证据的合理的替换策略，并具有对信任评估有利的性质(见后面的性质和定理)。

性质1 在高价值交往中，权重扩展法对已获得证据的权重是按原有权重的大小比例扩展的，且扩展后的权重和等于1。

证明：由权重扩充法的式(7)知，扩展后的各个权重的分母是相同的，而分子是权重本身，因此这些权重是按比例扩大的。同时有：

$$\frac{ew_1'}{ew_1'+ew_2'+\cdots+ew_{m1}'}+\frac{ew_2'}{ew_1'+ew_2'+\cdots+ew_{m1}'}+\cdots$$
$$\frac{ew_m'}{ew_1'+ew_2'+\cdots+ew_{m1}'}=1$$

性质2 在中等价值交往时，对于未获得的节点行为证据，在有效时间 $T0$ 内，当以往该节点证据值的方差 $\sigma_n \leqslant L$，且记录个数大于 $N_{\min}$ 时，本次未获得的证据替换的有效率最高，等于该节点以往证据均值。

证明：当全部用节点自己的以往证据值替换未获得的证据值时，证据替换值的有效率是最高的。从前面的论述可以看到：只有节点以往的证据值稳定，量大和时间有效，这时用节点本身的过去均值替换未获得证据的值，其信任评估结果才具有可信性，因此当符合这些条件时，才能用节点自己的以往值替换，其他的需要用较低的陌生信任值 D 替换，即符合这三个条件时证据替换的有效率最高，等于该节点以往的证据均值，即 $\sum_{k=1}^{n} et_k/n$。

定理1 在高价值交往中，如果获得的证据值都相等，则不论获得的证据是什么，证据个数是否相等，只要交往的价值相等，则行为信任的评估值一定相等。

证明：设在两次不同的高价值交往中，第 i 次交往获得的证据为 $et_{i1}, et_{i2}, \cdots, et_{in}$，第 j 次交往获得的证据为 $et_{j1}, et_{j2}, \cdots, et_{jm}$，由假设条件知，这些的证据值相等，设为 et，并且有 $ew_{i1}+ew_{i2}+\cdots+ew_{in}=ew_{j1}+ew_{j2}+\cdots+ew_{jm}$，则根据高价值交往的计算信任的权重扩充法，第 i 次节点交往获得 n 个证据的信任属性为：

$$\frac{ew_{i1}}{\sum_{k=1}^{n} ew_{ik}} et+\frac{ew_{i2}}{\sum_{k=1}^{n} ew_{ik}} et+\cdots\frac{ew_{in}}{\sum_{k=1}^{n} ew_{ik}} et=\frac{\sum_{k=1}^{n} ew_{ik}}{\sum_{k=1}^{n} ew_{ik}} et=et$$，第 j 次节点交往获得 m 个证据的信任属性为：

$$\frac{ew_{j1}}{\sum_{k=1}^{m} ew_{jk}} et+\frac{ew_{j2}}{\sum_{k=1}^{m} ew_{jk}} et+\cdots\frac{ew_{jm}}{\sum_{k=1}^{m} ew_{jk}} et=\frac{\sum_{k=1}^{m} ew_{jk}}{\sum_{k=1}^{m} ew_{jk}} et=et$$，因此二者相等。因为两次行为信任属性相等，则根据式(2)，最终的信任也必然相等。

本定理说明在等值的高价值交往中，如果两次获得的证据都相等，则信任值必然相等，而与具体的证据和证据个数无关。这说明了在节点交往中行为价值的重要性。

6.2 算法的进一步改进

在前面的算法中，当历史记录大于记录限制个数 $N_{\max}$ 时，为了保证信任评估的可扩展性，直接删除时间最远的记录，但这是以减小历史证据均值的可靠性为代价的。下面我们对此进行改进，不是直接删除过期记录，而是将过期的记录

(下转第67页)

参 考 文 献

[1] 崔莉,鞠海玲,苗勇,等. 传感器网络研究进展[J]. 计算机研究与发展,2005,42(1):163-174

[2] Ye Z, Abouzeid A, Ai J. Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks[C]// Proceedings of the IEEE Conference on Computer Communications (INFOCOM). May 2007

[3] Gao J, Guibas L, Hershberger J, et al. Sparse Data Aggregation in Sensor Networks[C]// Information Processing in Sensor Networks(IPSN). April 2007

[4] Subramanian S, Shakkottai S, Gupta P. On Optimal Geographic Routing in Networks with Holes and Non-Uniform Traffic[C]// Proceedings of the IEEE Conference on Computer Communications(INFOCOM). May 2007

[5] Shah R C, Rabaey J M. Energy Aware Routing for Low Energy Ad Hoc Sensor Networks[C]// Proceeding of IEEE Wireless Communication and Networking Conference (WCNC2002). March 2002

[6] Subramanian S, Shakkottai S, Gupta P. On Optimal Geographic Routing in Networks with Holes and Non-Uniform Traffic[C]// Proceedings of the IEEE Conference on Computer Communications(INFOCOM). May 2007

[7] Tian He J. A Stankovica Chenyang Lub Tarek Abdelzaher. SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks[C]// IEEE 23rd International Conference on Distributed Computing Systems(ICDCS'03). May 2003

[8] Willig A. Recent and Emerging Topics in Wireless Industrial Communications: A Selection[J]. IEEE Transactions on Industrial Informatics, 2008, 4(2): 102-124

[9] Zhang Yan, Luo Jujun, Hu Honglin. Wireless Mesh Networking: Architectures, Protocols and Standards[M]. Boca Ration: Auerbach publications Taylor & Francis Group LLC, 2007: 8-13

[10] Rappaport T S. Indoor radio communications for factories of the future[J]. IEEE Communications Magazine, 1989, 27(5): 15-24

[11] Kumar R, Wolenetz M, Agarwalla B, et al. DFuse: A Framework for Distributed Data Fusion[C]// Proc. 1st ACM Conference on Embedded Networked Sensor Systems(SenSys'03). Los Angeles, CA, Novermber 2003: 114-125

(上接第 41 页)

累加起来,将累加的结果按一定的比例参与历史记录的均值计算中,这样可以提高证据的合理性和有效率,且不影响算法的可扩展性。

初始累加证据可以取最低信任临界值 D,每一个证据的累加都是在原累加证据的基础上进行的,根据当前要删除的证据 et_{new} 来累加原有的累加证据 et_{old},如果被删除的证据大于原有的累加证据,则证据增加,否则减少。浮动值的大小是以被删除获得的证据值与原有累加证据的差为基数来计算的,证据累加的计算方法见式(9):

$$\begin{cases} et_{old}+et_{old}*(et_{new}-et_{old})*\beta^{(et_{new}-D+1/n)} & et_{new}\geqslant D \\ et_{old}+et_{old}*(et_{new}-et_{old})*\beta^{(et_{new}-D)} & et_{new}<D \end{cases} \tag{9}$$

式中,$0<\beta<1$ 是主观的信任调节因子,$\beta^{(et_{new}-D+1/n)}$,$\beta^{(et_{new}-D)}$ 分别称为证据信任累加控制部分和证据非信任累加控制部分,n 是节点过期被删除的证据总个数。

此证据累加公式具有如下性质,我们用一个定理来描述。

定理 2 在被删除证据增长幅度相同的情况下,被删除证据在陌生者证据之上的证据累加幅度一定小于被删除证据在陌生者证据值之下的证据累加幅度。

证明:设在信任临界值之上的被删除证据为 et^a_{new},在信任临界值之下的被删除证据为 et^b_{new},由已知得 $|(et^a_{new}-et_{old})|=|(et^b_{new}-et_{old})|$,并且有 $et^a_{new}>the0>et^b_{new}$,则 et^a_{new} 和 et^b_{new} 证据累加增长幅度之比为 $et_{old}*(et^a_{new}-et_{old})*\beta^{(et^a_{new}-D+1/n)}$ 和 $et_{old}*(et^b_{new}-et_{old})*\beta^{(et^b_{new}-D)}$ 之比,由于 $|(et^a_{new}-et_{old})|=|(et^b_{new}-et_{old})|$,因此 $|\beta^{(et^a_{new}-D+1/n)}|/\beta^{(et^b_{new}-D)}$ 这是两个指数函数之比,由于 $0<\beta<1$,$et^a_{new}>D>et^b_{new}$,因此 $|\beta^{(et^a_{new}-D+1/n)}|<1$ 而 $\beta^{(et^b_{new}-D)}>1$,故:$|\beta^{(et^a_{new}-D+1/n)}|/|\beta^{(et^b_{new}-D)}|<1$。

本定理说明,在被删除证据幅度增长相同的情况下,如果新证据在信任范围内,则累加速度慢,体现"日久见人心"的信任积累原则,如果在不信任范围内,则信任下降速度加快,体现对不信任行为的惩罚力度。

结束语 本文针对目前在无线传感器网络的节点行为信任评估中很少考虑节点行为价值的现象,从节点行为证据这个根本依据出发,论述了证据不全、行为价值不相等的问题,提出了针对不同价值交往的节点信任评估方法,重点论述了不足填充法和权重扩展法。最后通过两个定理和两个性质证明了方法对节点行为信任评估的有效性。

参 考 文 献

[1] Zhan Guoxing, Shi Weisong, Deng Julia. a resilient trust model for WSNs[C]//Proceedings of the 7th International Conference on Embedded Networked Sensor Systems. Berkeley, California, USA, Novembe, 2009: 411-412

[2] Zhang Mingwu, Yang Bo, Qi Yu. Using Trust Metric to Detect Malicious Behaviors in WSNs[C]//Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Qingdao, China, 2007: 104-108

[3] Lin Chuang, Wang Yuanzhuo, Tian Liqin. Development of Trusted Network and Chanllenges It Faces[J]. ZTE Communications, 2008, 6(1): 13-17

[4] Tian Liqin, Lin Chuang, Ji Tieguo. Kind of quantitative evaluation of user behaviour trust using AHP[J]. Journal of Computational Information Systems, 2007, 3(4): 1329-1334

[5] Lin Chuang, Pen Xuehai. Research on Trustworthy Networks [J]. Chinese Journal of Computers, 2005, 28(5): 751-758

[6] He Xin, Gui Xisolin. A Heider-Theory Based Reputation Framework for WSN[C]// 2008 10th IEEE International Conference on High Performance Computing and Communications. 2008: 635-640

[7] Tian Liqin, Lin Chuang, Sun Jinxia. A kind of prediction method of user behaviour for future trustworthy network[C]// 2006 International Conference on Communication Technology. 2006: 199-202

[8] Tian Liqin, Lin Chuang, Ji Tieguo. Quantitative Analysis of Trust Evidence in Internet[C]// 2006 10th International Conference on Communication Technology Proceedings. 2006: 194-198

[9] LinChuang, TianLi-qin, WangYuan-zhuo. ResearchonUserBehavior Trust in Trustworthy Network[J]. Journal of Computer Research and Development. 2008, 45(12): 2033-2043

[10] Zhu, Cheng. A secure data fusion algorithm based on behavior trust in wireless sensor networks[C]// International Conference on Wireless Communications, Networking and Mobile Computing. 2008: 191-194