文章编号:0253-2778(2017)4-0297-07

基于感知源信任评价的物联网数据可靠保障模型

陈振国[1,2],田立勤[2],林 闯[3]

(1.东北大学计算机科学与工程学院,辽宁沈阳 110819;
2.华北科技学院计算机学院,北京 101601;3.清华大学计算机系,北京 100084)

摘要:为了解决物联网大数据源头的可靠问题,给出一种基于感知源信任评价的物联网数据可靠保障的模型.模型首先构建感知层评测单元,每个评测单元均包括工作节点、伴生节点和判决节点三种类别.感知同种指标的工作节点之间可互相作为对方信任值计算的依据;伴生节点和判决节点均用于对工作节点的状态进行监测,伴生节点用于对工作节点的数据进行定期的验证,从而确定工作节点的状态;判决节点则是当工作节点出现疑似异常,无法最终确定时,被动启用以作为最终的判断结果.通过以上三种节点的数据收集和验证给出了一种用于节点可靠度计算、调整的方法,以此获得每个工作节点的信任值.然后在给定阈值的情况下,构建信任列表,剔除不可信的感知节点,只传输和处理可信节点所感知的数据.同时为了保证感知节点的初始可靠,引入接入认证机制.从理论分析和仿真的结果看,该模型具有节点感知数据可靠、灵活可扩展等特点,能够有效提高物联网大数据源头的可靠性.

关键词:物联网;大数据;信任评价;数据可靠;节点筛选

中图分类号:TP393 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2017.04.003

引用格式:陈振国,田立勤,林闯. 基于感知源信任评价的物联网数据可靠保障模型[J]. 中国科学技术大学学报,2017,47(4):297-303,335.

CHEN Zhenguo, TIAN Liqin, LIN Chuang. Data reliable assurance model of Internet of Things based on the trust evaluation of perceived source[J]. Journal of University of Science and Technology of China, 2017,47(4):297-303,335.

Data reliable assurance model of Internet of Things based on the trust evaluation of perceived source

CHEN Zhenguo[1,2], TIAN Liqin[2], LIN Chuang[3]

(1. *School of Computer Science and Engineering, Northeastern University, Shenyang* 110819, *China*;
2. *North China Institute of Science and Technology, Beijing* 101601, *China*;
3. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: In order to solve the source reliability problem of Big Data in the Internet of Things, a data reliable assurance model of Internet of Things based on the trust evaluation of perceived source was constructed with the evaluation unit, and each evaluation unit includes three categories, including the work node, the companion node and the decision node. The working nodes which are aware of the same kind of

收稿日期:2016-08-28;修回日期:2016-12-08

基金项目:国家自然科学基金(61472137),青海省农业科技成果转化与推广计划(2012-N-525),河北省科技计划(15210703),国家安全监管总局安全生产重大事故防治关键技术科技项目(zhishu-031-2013AQ),中央高校基本科研业务费资助项目(3142014125,3142015022,3142013098)资助.

作者简介:陈振国,男,1976年生,博士生/副教授.研究方向:网络安全、物联网. E-mail: zhenguo_chen@126.com

通讯作者:田立勤,博士/教授. E-mail: tianliqin@tsinghua.org.cn

index can be used as the basis for calculating the value of each other's trust. The companion nodes and decision nodes are used to monitor the status of the working nodes. The companion nodes are used to verify the data of the working nodes regularly, so as to determine the status of the working nodes. The decision node is used when the working node is suspected to be abnormal so as to give the final result. Through the data collection and validation of the above three kinds of nodes, a method for calculating and adjusting the reliability of nodes was presented, which was used to obtain the trust value of each working node. Then, according to the given threshold value, the trust list was constructed, and the non-trusted nodes removed, and only the data perceived by the trusted node gets transmited and processed. At the same time, in order to ensure the initial reliability of the sensor node, the access authentication mechanism is introduced. From the results of theoretical analysis and simulation, the model has the characteristics of reliable node sensing data and flexible expansion, and can effectively improve the reliability of the data source of the Internet of Things.

Key words: Internet of Things; Big Data; trust evaluation ; Data reliability; node selection

0 引言

随着云计算、物联网等技术的发展,在信息技术应用中所产生的数据规模越来越大.大数据来源形式多样,可以是人们在(移动)互联网活动中所产生的各种信息,也可以是各类计算机信息系统所产生的数据,还可以是各种感知设备所感知或采集的数据.每一种来源都存在复杂的数据产生、传输环境,并且大数据在存储过程中也面临各种风险,这些都有可能导致大数据的无效,因此保障数据本身的可靠、可信、可用至关重要.

物联网感知所获得的数据量庞大,是大数据的一种典型来源.由于物联网具有低功耗、密集部署、无人值守等特点使得其安全性更难以保证.无例外通常会部署在长时间无人值守的环境中工作,部署区域的节点会大量暴露在攻击者的范围之内,这给网络的安全带来很大隐患.在这种环境下,节点很容易遭受物理攻击,被攻击者俘获,提取节点中的私密信息,加以改造节点,发起各种攻击,从而导致源头数据的无效.另外很多感知节点是一种微型的嵌入式设备,其硬件资源相当有限,受到计算和存储等限制,也使得传统的安全策略不能高效地发挥作用,因此如何保证所感知数据的可靠是我们必须面对和解决的物联网关键技术之一,本文针对物联网感知中感知节点数据的统计研究了节点可靠性评价与筛选机制,给出了一种从源头对感知数据可靠性进行保证的模型.

1 相关研究

物联网通过对区域内的对象进行信息采集和协同处理,将信息传送给观察者,而在此过程中如何有效的保障数据的可靠、可信则是需要重点研究和解决的问题.由于物联网极易受到诸如被动窃听、主动入侵、信息假冒、信息阻塞等多种形式的攻击,无法保证感知的数据正确可靠.为了提高物联网的安全、可信和可靠性,研究者进行了多方面的研究,并给出了一些有效的方法,如从能量监测、节点行为、分级管理等角度通过设计面向感知设备和人的信任评价方法,实现对数据收集源头的控制[2-5];文献[6]研究如何从传感网获取数据,使得物理世界能够被准确近似,从而获取高精度数据,提高数据的可用性.具体的处理方式则是通过研究数据之间的关系或者通过特定的算法,实现异常数据的发现、纠正或剔除异常数据,如文献[7]发现数据源之间的数据复制关系能够帮助系统更好地选取高质量的数据源、改善集成数据的可用性.针对静态数据,则提出了基于贝叶斯分析的方法,判定数据源之间的复制关系,并基于复制关系提出了高质量数据获取与整合的方法,提高了获取与整合后数据的可用性.文献[8]则基于Web大数据发现、抽取、识别、融合等方法,提出Web跨源数据不一致分类方法和一致性约束机制,建立了Web跨源数据的不一致分类方法和分类模型,为保证大数据的有效性提供了一种方法.张安珍等采用数据依赖理论中的条件函数依赖,给出了一种不一致数据检测与修复算法[9].金连等针对数据中存在大量缺失值的问题,给出了一种基于概率推

理的填充分类属性的算法，用以完善数据的有效性[10]．文献[11]为了提高 RFID 系统中数据的质量，提出了一种基于有限状态机的 RFID 流数据过滤与清理方法．文献[12]结合数据分析技术构建信任模型，给出了一种雾霾感知源的信任评价方法，从而从源头对数据的有效性进行保障．文献[13]根据网络负载状况设计了一种基于单位基准时隙的自适应机制，设置尽量小的退避等待时间，提高信息广播的实时性，在保证算法实时性的基础上最大限度地提高可靠性．文献[14]则结合物联网大面积部署的特点，对拓扑结构的可靠性进行了设计．文献[15]在保证成员节点证人机密性的基础上，通过绑定证人与组密钥更新计算，限制了非成员节点对新密钥的计算能力，提高了抵抗伪造、重放和共谋等恶意攻击的能力．

通过分析可以看出，对感知源信任评价的研究，已有一些可用的成果，但其研究思路大多集中在以行为信息作为评价的基础，而物联网中感知源的主要作用就是感知数据，而使用其所感知的数据进行评价的研究成果不多．对数据的可靠性保障的研究也主要集中在传输、存储过程中或者利用数据自身信息进行保障，而通过对数据源头可靠保障的研究，则更多地集中在接入认证等传统的方法，本文则从感知数据出发，给出了一种感知源信任评价的模型，从而通过该模型可保障数据源头的可靠性．

2　感知源信任评价模型

本文的信任模型将物联网的感知层节点分为感知节点、中继节点和协调器节点．感知节点用于实现某个数据指标的感知，并采用短程通信技术发送给中继节点，不负责其他节点的数据转发；中继节点不负责数据的感知，用于完成数据的融合和转发任务，同时各感知节点的信任调整和计算也是由中继节点完成的．协调器节点则负责建立网络和数据的远程转发或直接转交给网关，一般应用的基本结构如图 1 所示，图中的传输方式可采用不同形式．

由于仅进行感知源的信任评价分析，保障数据在源头、传输中的可靠性，需要使用已有的安全策略进行一定的保障，因此假定中继节点和协调器节点均是可靠的．

2.1　感知评测单元

在感知源信任评价中，以评测单元为单位，为了降低各感知节点的能耗，由评测单元中的中继节点完成对各感知节点的信任值的调整和计算．为了提高信任的有效性，将评测单元中的感知节点分为三类，分别是工作节点、伴生节点和判决节点．下面就相关概念给出定义．

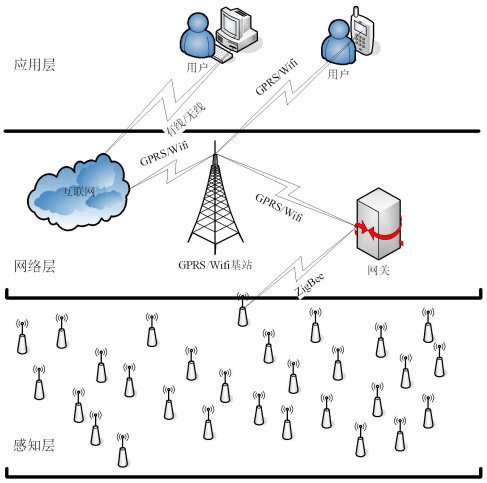

图 1　物联网应用的基本结构

Fig.1　Fundamental structure of Internet of Things

定义 2.1　评测单元：评测单元是信任评价执行的基本单位，一般定义为隶属于同一个中继节点并具有相同监测任务的所有感知节点的集合．

定义 2.2　工作节点：是指工作在正常频率下，用于实现信息感知的节点；

定义 2.3　伴生节点：是和工作节点在一个评测单元内，以远低于正常频率进行感知数据的节点，用于对工作节点的数据进行验证；

定义 2.4　判决节点：是和工作节点、伴生节点在同一个评测单元内，以被动方式启用的感知数据的节点，用于对工作节点和伴生节点感知到的数据是否明显不一致进行判决；

工作节点和伴生节点的数据差值要求在一定的阈值范围内，阈值可人为设定，伴生节点的感知频率远低于工作节点，具体取值在考虑工作节点的信任度的基础上通过优化得到，当信任度高时（大于设定的阈值）降低伴生节点的感知频率，若较低（小于设定的阈值）则增加伴生节点的感知频率，最大不能超过工作节点的感知频率．判决节点是被动启用的，它没有固定的感知频率，当工作节点的信任度高于设定的阈值，而出现工作节点和伴生节点的差值超过设定阈值的次数达到设定的上限时，由中继节点通知判决节点启动进行数据感知，依据感知的数据对工作节点的数据进行终极判断．

2.2 信任评价模型

本模型利用物联网中感知节点冗余、密集部署，同一个评测单元中对相同指标进行监测的工作节点具有近似的感知值的特点，可实现工作节点自身、工作节点之间的信任评价，同时结合伴生、判决节点给出的监督信任评价，再结合历史信任值进行加权运算，最后得到感知节点的综合信任值，最后根据设定的阈值和信任值的结果进行信任列表的更新，信任评价及信任列表更新的整体结构如图 2 所示.

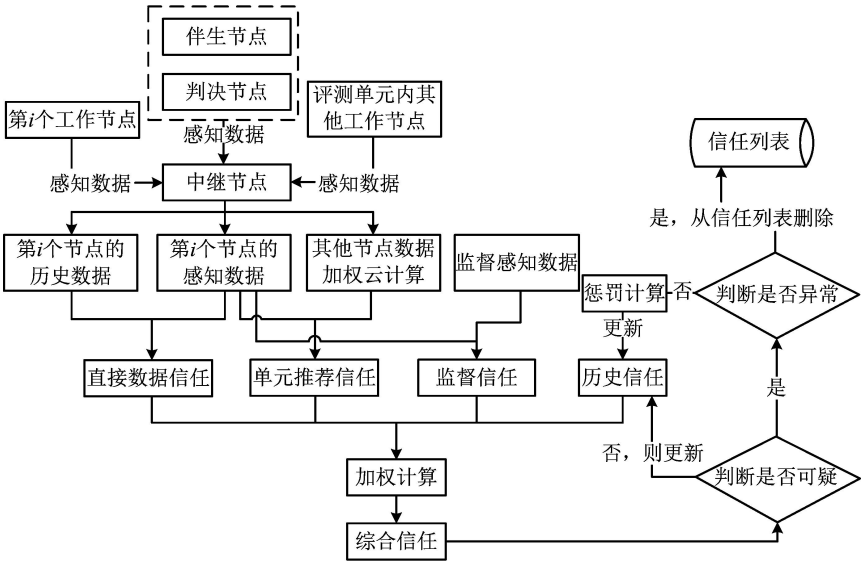

图 2 信任评价模型的结构图

Fig.2 The structure of the trust evaluation model

2.2.1 直接信任的计算

假定工作节点所感知的数据是连续且不具有突变的特点，中继节点保存其所辖的每个感知节点的上一次历史数据.直接信任反映了工作节点的是否可信的状态，通过实时感知数据和该节点的历史数据的计算，可以得到直接信任的值.设第 i 个工作节点的实时感知数据记作 ${}^{w}\mathrm{Data}_i$，该节点的历史数据记作 ${}^{h}\mathrm{Data}_i$，直接信任记作 ${}^{dt}T_i$，则直接信任可根据下式计算得到.

$$ {}^{dt}T_i = \lfloor \mathrm{Max} \times ((|{}^{w}\mathrm{Data}_i - {}^{h}\mathrm{Data}_i| - {}^{dt}K) > {}^{dt}K \ ? \ 0 : (|{}^{w}\mathrm{Data}_i - {}^{h}\mathrm{Data}_i| - {}^{dt}K)/{}^{dt}K) \rfloor \quad (1) $$

式中，Max 表示初始和最大直接信任值，是一个常数，可根据经验或由专家设定. ${}^{dt}K$ 是一个阈值，表示实时感知数据和历史数据之差的上限.

2.2.2 单元推荐信任的计算

监测单元是隶属于同一中继节点并具有相同监测任务的所有感知节点的集合.第 i 个工作节点的单元推荐信任通过该节点的实时感知数据和监测单元内其他工作节点的实时监测数据的均值计算得到.设定在监测区域内共有 N 个工作节点，第 i 个节点的单元推荐信任记作 ${}^{urt}T_i$.单元推荐信任的初始和最大记作 Max，和直接信任的最大相同.第 i 个节点外的其他 $N-1$ 个工作节点的实时感知数据的均值记作 ${}^{urt}\mathrm{Aver}_i$.第 i 个节点的实时感知数据和其他工作节点的实时感知数据的均值的差值上限记作 ${}^{urt}K$，则单元推荐信任可由下式计算得到.

$$ {}^{urt}\mathrm{Aver}_i = \sum_{j=1}^{N-1} {}^{w}\mathrm{Data}_j/(N-1) $$

$$ \mathrm{dif}_i^{urt} = \begin{cases} 1, & {}^{urt}\mathrm{Aver}_i = 0 \\ |{}^{w}\mathrm{Data}_i - {}^{urt}\mathrm{Aver}_i| - {}^{urt}K > {}^{urt}K \ ? \ 0 : |{}^{w}\mathrm{Data}_i - {}^{urt}\mathrm{Aver}_i| - {}^{urt}K, & {}^{urt}\mathrm{Aver}_i \neq 0 \end{cases} $$

$$ {}^{urt}T_i = \lfloor \mathrm{Max} \times (\mathrm{dif}_i^{urt}/{}^{urt}K) \rfloor \quad (2) $$

说明：在均值计算过程中，会对参与计算的工作节点的综合信任度进行判断，若不在信任列表中，则

不参与均值的计算.

2.2.3　监督信任的计算

监督信任根据伴生节点和判决节点的工作情况进行计算.第 i 个节点的监督信任记作 ${}^{st}T_i$.设伴生节点的实时感知数据记作 ${}^{c}\mathrm{Data}$,判决节点的实时感知数据记作 ${}^{d}\mathrm{Data}$,若节点处于休眠的状态,其数据取值为 0.第 i 个节点的实时感知数据与伴生节点的实时感知数据的差值上限记作 ${}^{wc}K$,与判决节点的实时感知数据的差值上限记作 ${}^{wd}K$.则监督信任可根据下式进行计算.

$$\mathrm{dif}_i^{wc}=\begin{cases}1, {}^{c}\mathrm{Data}=0\\ \left|\left|{}^{w}\mathrm{Data}_i-{}^{c}\mathrm{Data}\right|-{}^{wc}K\right|>{}^{wc}K\ ?\ 0:\left|\left|{}^{w}\mathrm{Data}_i-{}^{c}\mathrm{Data}\right|-{}^{wc}K\right|, {}^{c}\mathrm{Data}\neq 0\end{cases}$$

$$\mathrm{dif}_i^{wd}=\begin{cases}1, {}^{d}\mathrm{Data}=0\\ \left|\left|{}^{w}\mathrm{Data}_i-{}^{d}\mathrm{Data}\right|-{}^{wd}K\right|>{}^{wd}K\ ?\ 0:\left|\left|{}^{w}\mathrm{Data}_i-{}^{d}\mathrm{Data}\right|-{}^{wd}K\right|, {}^{d}\mathrm{Data}\neq 0\end{cases}$$

$$ {}^{st}T_i=\lfloor \mathrm{Max}\times \mathrm{dif}_i^{wc}/{}^{wc}K\times \mathrm{dif}_i^{wd}/{}^{wd}K \rfloor \tag{3}$$

式中,Max 同上.

2.2.4　综合信任的计算

综合信任通过直接信任、单元推荐信任、监督信任和历史信任加权平均计算得到.其中第 i 个工作节点的历史信任自作 ${}^{h}T_i$,其初始值取信任的最大值,即 Max .综合信任记作 T_i ,则综合信任可由下式计算得到.

$$T_i=\lceil \alpha\times {}^{dt}T_i+\beta\times {}^{urt}T_i+\gamma\times {}^{st}T_i+\lambda\times {}^{h}T_i \rceil \tag{4}$$

式中,$\alpha,\beta,\gamma,\lambda$ 是权重因子,由经验获得或专家指定,其取值满足如下条件 $0<\alpha,\beta,\gamma,\lambda<1$,且 $\alpha+\beta+\gamma+\lambda=1$.

2.2.5　历史信任的计算

本文引入了节点接入认证机制,因此历史信任的初始值设为最大信任,即 Max. 表示初始对工作节点是完全信任的.为了或的更好的评价效果,我们设定了两个不可信的级别,分别是疑似和异常,疑似门限记作 $\mathrm{Th}_{\mathrm{susp}}$,异常门限记作 $\mathrm{Th}_{\mathrm{abn}}$.则历史信任的更新计算可由下式得到.

$${}^{h}T_i=\begin{cases}T_i, T_i<\mathrm{Th}_{\mathrm{susp}}\\ T_i-\left|T_i-\mathrm{Th}_{\mathrm{susp}}\right|, \mathrm{Th}_{\mathrm{susp}}<T_i<\mathrm{Th}_{\mathrm{abn}}\\ T_i-\tau\times\left|T_i-\mathrm{Th}_{\mathrm{abn}}\right|, T_i\geqslant \mathrm{Th}_{\mathrm{abn}}\end{cases} \tag{5}$$

式中,τ ($\tau\geqslant 1$) 是惩罚因子,用以调整惩罚力度.

2.3　信任列表更新

每个评测单元维护一个信任列表,初始信任列表中包含所有的工作节点,然后根据综合信任值和异常门限 $\mathrm{Th}_{\mathrm{abn}}$ 的关系实现信任列表的更新.综合信任 T_i 大于或等于 $\mathrm{Th}_{\mathrm{abn}}$ 时,则将第 i 个节点从信任列表中剔除.

3　仿真实验及分析

由于算法是以监测单元为单位执行评价过程,因此算法具有良好的扩展性,只需要在微型的物联网环境中验证其有效性,则可以很容易扩展到更大规模的网络中去.为了验证算法的有效性,本文搭建了一个由 10 个感知节点、1 个中继节点和 1 个协调器节点构成的微型物联网,感知节点的功能是完成室内温度的感知,然后在中继节点上实现算法的功能和性能的验证.

在 10 个感知节点中,为了验证在工作节点个数不同情况下,对单元推荐信任度的影响,我们在组网过程中逐步增加工作节点的个数.

此外,算法中用到了比较多的常量或阈值,我们结合实践经验和算法运行中的结果综合给出了赋值结果,如表 1 所示.

工作节点的感知频率设定为 2 秒,伴生节点的感知频率设定为 10 秒.

对于表 1 中的各常量和阈值,首先结合实验环境由经验设定,然后根据仿真的结果,不断调整对结果影响比较大的节点数值以适合环境的要求.表 1 中所列,除 Max 和 N 对结果基本无影响外,其他的常量或阈值,若设置的过大或过小都会对结果有较大的影响,因此在仿真过程中,为了确定相对合理的取值,需要有一个根据仿真结果不断调整的过程.

表 1 信任评价模型常量取值表

Tab.1 The constant value in the trust evaluation model

符号名	最终取值	单位	说明	来源
Max	100	-	信任度的最大值	设定
${}^{dt}K$	0.1	摄氏度	工作节点实时数据和其上次历史数据的差值上限	经验值并根据实验结果作了一些调整
N	1-8	个	工作节点的个数	实际取值
${}^{urt}K$	0.3	摄氏度	被评价的工作节点实时数据和其工作节点的均值的差值上限	经验值并根据实验结果作了一些调整
${}^{wc}K$	0.3	摄氏度	被评价的工作节点实时数据和伴生节点的实时数据的差值上限	经验值并根据实验结果作了一些调整
${}^{wd}K$	0.3	摄氏度	被评价的工作节点实时数据和判决节点的实时数据的差值上限	经验值并根据实验结果作了一些调整
$\alpha,\beta,\gamma,\lambda$	0.2,0.3,0.2,0.3	-	加权因子	根据实验结果调整得到
$\mathrm{Th}_{\mathrm{susp}}$	80	-	疑似门限	经验值并根据实验结果作了一些调整
$\mathrm{Th}_{\mathrm{abn}}$	65	-	异常门限	经验值并根据实验结果作了一些调整
τ	1	-	惩罚因子	经验值并根据实验结果作了一些调整

由图 3 可知,在工作节点未出现异常的情况下,历史信任和综合信任是相对稳定的,由于我们在此对 ${}^{dt}K$ 选择较小,因此直接信任的波动较大,但其对综合信任和历史信任的影响并不显著.单元推荐信任取值在正常情况下也相对稳定,监督信任由于和工作节点的感知频率不同,因此其信任值大多处于最大的状态.

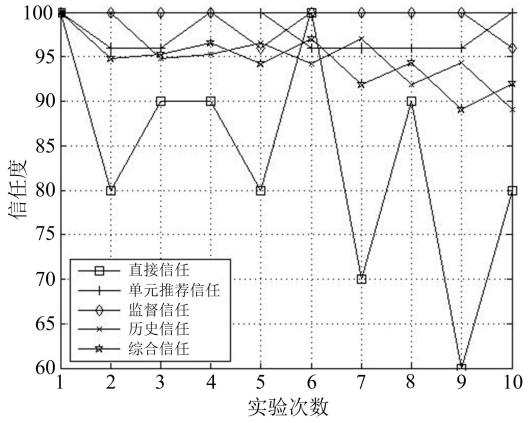

图 3 正常工作节点各信任值的变化趋势

Fig.3 The change of the trust value of normal working node

图 4 展示了当被评价节点出现异常,所感知的数据出现明显偏离正确值的情况下的各信任值的变化趋势.从图中可以看出,当异常出现时,直接信任和单元推荐信任直接归 0,综合信任和历史信任也急剧降低,已经低于异常门限,此时应将该节点从信任列表中剔除,其不再参与对其他节点的信任评价,中继节点在进行数据融合时也会跳过该节点的数据.由此可知,本模型能有效发现和规避异常数据的影响.若感知节点的异常状态一直持续,可以看到,直接信任会恢复到正常状态,但单元推荐信任和监督信任则仍然处于零值,因此综合信任和历史信任仍然会低于异常门限,从而会继续将该节点排除在信任列表之外.从图 4 中还可以看出,当该节点恢复正常后,其直接信任和单元推荐信任均立即恢复到正常状态,而综合信任和历史信任则需要逐步恢复,慢慢恢复到门限之上,这也体现了信任值的易失难得的特点.

图 5 展示了,在进行综合信任计算时,各加权因子的不同取值对综合信任取值的影响.为了保证信任的连续性特点,本文设定,历史信任所占比重必须

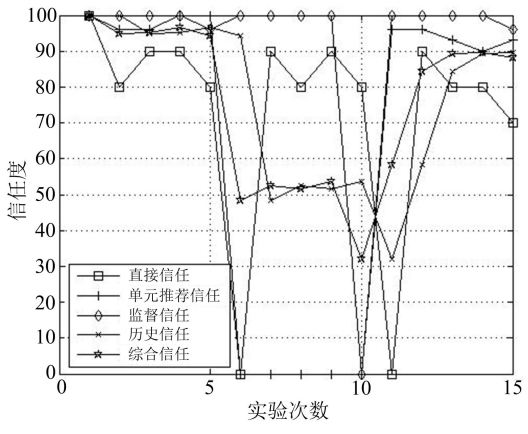

图 4　节点出现异常时各信任值的变化趋势

Fig.4　The change of the trust value of abnormal node

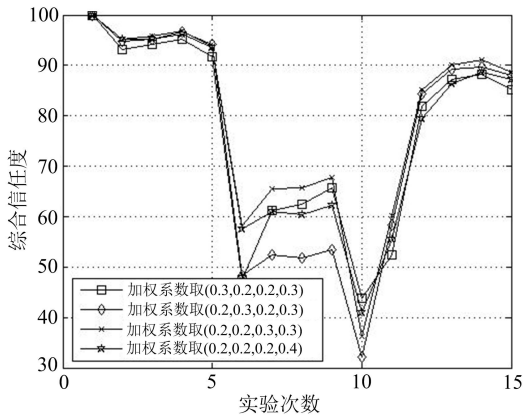

图 5　不同加权因子下综合信任的变化趋势

Fig.5　The change of the comprehensive trust with different weighting factors

不小于其他项所占比例，因此在仿真中，历史信任的加权系数 λ 最小的取值是 0.3.我们给出了 4 种组合方式，由图 5 可以看出，4 种组合都可以对节点的异常进行检测.当出现异常时，综合信任的变化趋势有一定的差别，通过比较可以看出，表 1 中给出的取值是相对合理的一种，在异常出现时，能在综合信任上有比较急剧的体现.没有异常时又可以较好地保持历史的惯性，保持综合信任的稳定.

本文模型具有相对较低地能耗.对感知节点而言，并没有额外增加通信开销，因此不影响其能耗，这一点优于使用行为信息进行评价的算法.在中继节点所进行的运算都是简单的基本运算，因此所需要增加的额外资源也比较有限.

4　结论

本文结合物联网应用场景的特点，给出了一种从源头保障数据可靠，且自适应、灵活可扩展的感知源信任评价模型.模型提出了评测单元的概念，将感知节点分为工作节点、伴生节点和判决节点，在充分利用具有相同功能任务的各感知节点自身及感知节点之间数据相近性的特点，给出了直接信任和单元推荐信任的计算方法，并通过引入伴生和判决两类节点给出了监督信任的计算，使得信任评价的结果更准确，最后再结合历史信任，通过加权平均计算获得每个工作节点的综合信任，然后再以此为基础，实现了一种简单的信任列表的更新算法.从仿真结果看，本文算法能有效地评价感知节点的状态，且易于扩展，对保障物联网大数据源头的可靠性提供了一种新的思路.

参考文献(References)

[1] International Telecommunication Union. Internet reports 2005: The Internet of Things [R]. 7ed, Geneva: ITU, 2005.

[2] 范存群，王尚广，孙其博，等.基于能量监测的传感器信任评估方法研究[J]. 电子学报, 2013, 41(4): 646-651.
FAN Cunqun, WANG Shangguang, SUN Qibo, et al. A trust evaluation method of sensors based on energy monitoring[J]. Acta Electronica Sinica, 2013, 41(4): 646-651.

[3] HE D J, CHEN C, CHAN S, et al. A distributed trust evaluation model and its application scenarios for medical Sensor networks [J]. IEEE Transaction on Information Technology in Biomedicine, 2012, 16(6): 1164-1175.

[4] SICARI S, RIZZARDI A, GRIECO L A, et al. Security, privacy and trust in Internet of Things: The road ahead [J]. Computer Networks, 2015, 76: 146-164.

[5] ZHANG B, HUANG Z H, XIANG Y. A novel multiple-level trust management framework for wireless sensor networks [J]. Computer Networks, 2014, 72: 45-61.

[6] CHENG S Y, LI J Z, CAI Z P. $O(\varepsilon)$-approximation to physical world by sensor networks[C]// Proceedings of IEEE INFOCOM'13. Piscataway, USA: IEEE Press, 2013: 3084-3092.

[7] DONG X L, BERTI-EQUILLE L, SRIVASTAVA D. Truth discovery and copying detection in a dynamic world [J]. Proceedings of the VLDB Endowment, 2009, 2(1): 562-573.

(下转第 335 页)

momentum of research projects [J]. Knowledge Discovery and Data Mining, 2011, 6635(2):532-543.

[10] DU Y, HE Y, TIAN Y, et al. Microblog bursty topic detection based on user relationship[C]// Proceedings of the 6th IEEE Joint International Information Technology and Artificial Intelligence Conference. Chongqing, China: IEEE Press, 2011, 1: 260-263.

[11] **王征，王林森，赵磊. 基于信息密度的微博突发话题检测模型研究[J]. 情报理论与实践**，2016，39(3)：125-129.

[12] **申国伟，杨武，王巍，等. 面向大规模微博消息流的突发话题检测[J]. 计算机研究与发展**，2015，52(2)：512-521.
SHEN Guowei, YANG Wu, WANG Wei, et al. Burst topic detection oriented large-scale microblogs streams [J]. Journal of Computer Research and Development, 2015, 52(2): 512-521.

[13] **贺敏，徐杰，杜攀，等. 基于时间序列分析的微博突发话题检测方法[J]. 通信学报**，2016，37(3)：48-54.
HE Min, XU Jie, DU Pan, et al. Bursty topic detection method for microblog based on time series analysis[J]. Journal on Communications, 2016, 37(3): 48-54.

[14] **郭踯秀，吕学强，李卓. 基于突发词聚类的微博突发事件检测方法[J]. 计算机应用**，2014，34(2)：486-490，505.
GUO Yixiu, LYN Xueqiang, LI Zhuo. Bursty topics detection approach on Chinese microblog based on burst words clustering [J]. Journal of Computer Applications, 2014, 34(2): 486-490, 505.

[15] **徐志明，李栋，刘挺，等. 微博用户的相似性度量及其应用[J]. 计算机学报**，2014，37(1)：207-218.
XU Zhiming, LI Dong, LIU Ting, et al. Measuring similarity between microblog users and its application [J]. Chinese Journal of Computers, 2014, 37(1): 207-218.

[16] **毛佳昕，刘奕群，张敏，等. 基于用户行为的微博用户社会影响力分析[J]. 计算机学报**，2014，37(4)：791-800.
MAO Jiaxin, LIU Yiqun ZHANG Min, et al. Social influence analysis for micro-blog user based on user behavior[J]. Chinese Journal of Computers, 2014, 37(4): 791-800.

[17] **陈克寒，韩盼盼，吴健. 基于用户聚类的异构社交网络推荐算法[J]. 计算机学报**，2013，36(2)：349-359.
CHEN Kehan, HAN Panpan, WU Jian. User clustering based social network recommendation [J]. Chinese Journal of Computers, 2013, 36(2): 349-359.

(**上接第** 303 **页**)

[8] **余伟，李石君，杨莎，等.** Web **大数据环境下的不一致跨源数据发现[J]. 计算机研究与发展**，2015，52(2)：295-308.
YU Wei, LI Shijun, YANG Sha, et al. Automatically discovering of inconsistency among cross-source Data based on Web big Data [J]. Journal of Computer Research and Development, 2015, 52(2): 295-308.

[9] **张安珍，门雪莹，王宏志，等. 大数据上基于** Hadoop **的不一致数据检测与修复算法[J]. 计算机科学与探索**，2015，9(9)：1044-1055.

[10] **金连，王宏志，黄沈滨，等. 基于** Map-Reduce **的大数据缺失值填充算法[J]. 计算机研究与发展**，2013，50：312-321.

[11] **罗元剑，姜建国，王思叶，等. 基于有限状态机的** RFID **流数据过滤与清理技术[J]. 软件学报**，2014，25(8)：1713-1728.
LUO Yuanjian, JIANG Jianguo, WANG Siye, et al. Filtering and cleaning for RFID streaming *Data* technology based on finite state machine[J]. Journal of Software, 2014, 25(8): 1713-1728.

[12] **陈振国，田立勤. 信任模型在雾霾感知源评价中的应用[J]. 计算机应用**，2016，36(2)：472-477.
CHEN Zhenguo, TIAN Liqin. Application of trust model in evaluation of haze perception source [J]. Journal of Computer Applications, 2016, 36(2): 472-477.

[13] **罗涛，李俊涛，刘瑞娜，等.** VANET **中安全信息的快速可靠广播路由算法[J]. 计算机学报**，2015，38(3)：663-672.
LUO Tao, LI Juntao, LIU Ruina, et al. A fast and reliable broadcast routing algorithm for safety related information in VANET [J]. Chinese Journal of Computers, 2015, 38(3): 663-672.

[14] **田立勤，林闯，张琪，等. 物联网监测拓扑可靠性设计与优化分析[J]. 软件学报**，2014，25(8)：1625-1639.
TIAN Liqin, LIN Chuang, ZHANG Qi, et al. Topology reliability design and optimization analysis of IoT-based monitoring[J]. Journal of Software, 2014, 25(8): 1625-1639.

[15] **钟晓睿，马春光. 基于动态累加器的异构传感网认证组密钥管理方案[J]. 通信学报**，2014，35(3)：124-134.
ZHONG Xiaorui, MA Chunguang. Dynamic accumulators-based authenticated group key management scheme for heterogeneous wireless sensor network [J]. Journal on Communications, 2014, 35(3): 124-134.