DOI: 10.3979/j.issn.1673-825X.2016.06.021

Josang 信任模型的物联网感知层安全数据融合方法

魏琴芳[1],程利娜[1],付　俊[2],胡向东[3]
(1. 重庆邮电大学 通信与信息工程学院,重庆 400065; 2. 中国移动研究院,北京 100033;
3. 重庆邮电大学 自动化学院,重庆 400065)

摘　要: 物联网感知层通常涉及大量传感器节点的运用,具有节点资源有限、分布广泛、无人值守、数据冗余、攻击容易等特点,实施安全数据融合是其必然选择。为了保障物联网感知层数据融合结果的真实性与可靠性,建立了一种结合数据预处理与节点信誉度评价的安全数据融合模型,利用粗大误差理论将明显偏离正常数据(或真值)的异常数据予以识别和剔除,基于概率统计理论计算和更新节点信誉度,只允许来源于高信誉度的节点数据参与数据融合,以 Josang 信任模型形成对数据融合结果的评价。仿真实验结果表明,该模型不仅有助于确保物联网感知层数据融合结果真实性与可靠性,而且基于粗大误差的数据预处理方法可减少数据融合的计算量,降低对传感器节点资源的需求。

关键词: 物联网; 传感器节点; 数据融合; 粗大误差理论; 信誉度
中图分类号: TP393; TN915　　**文献标志码:** A　　**文章编号:** 1673-825X(2016)06-0876-07

Secure data aggregating methods by means of Josang trust models for the sensing layer of the internet of things

WEI Qinfang[1], CHENG Lina[1], FU Jun[2], HU Xiangdong[3]
(1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China; 2. Research Institute of China Mobile, Beijing 100033, P. R. China;
3. College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China)

Abstract: The sensing layer of internet of things(IoT) usually involves a large number of sensor nodes, which is characterized by limited nodes resources, wide distribution, unmanned operation, data redundancy, easy attack, etc. Carrying out secure data aggregation is thus necessary for IoT sensing layer. In order to guarantee the authenticity and reliability of the results from data aggregation of IoT sensing layer, a secure data aggregating model combining with data preprocessing and node creditability evaluation is proposed. Firstly, the abnormal data obviously deviated from normal data (or true value) are identified and eliminated by means of gross error theory. Then nodes creditability are calculated and updated by means of probability and statistics theory, and nothing but the data of nodes with high creditability is allowed to involve in data aggregation. Finally, the model gains an evaluation of the results of data aggregation by means of Josang trust model. The simulation experiment results show that the model not only helps to guarantee authenticity and reliability of data aggregation results from IoT sensing layer, but also can reduce the calculating overload of data aggregation and the demand for sensor node resources by means of data preprocessing method based on gross error theory.

Keywords: internet of things; sensor nodes; data aggregation; gross error theory; creditability

收稿日期: 2015-12-11　**修订日期:** 2016-06-02　**通讯作者:** 魏琴芳　weiqf@cqupt.edu.cn
基金项目: 国家自然科学基金(61170219); 教育部-中国移动联合研究基金(MCM20150202)
Foundation Items: The National Natural Science Foundation of China (61170219); The Joint Research Foundation of the Ministry of Education of the People's Republic of China and China Mobile (MCM20150202).

0 引　言

无线传感器网络作为物联网感知层的核心组成部分之一，主要由大量部署在监测区域内的低成本微传感器节点组成，通过无线通信方式形成一个多跳的自组织网络，可广泛应用于生态监测、健康护理、智慧交通、智能物流等众多领域，是当前研究的一个热点。然而传感器网络中节点的资源是非常有限的，这主要体现在电池能量、存储能力、处理能力以及通信带宽等方面，所以减少节点和基站间的数据传输量和通信开销、提高能效和带宽利用率显得十分必要; 且物联网感知层所采集的原始数据一般具有较大的冗余性，因此，数据融合的需求就被提出，通过数据融合技术的运用可以去除采集数据中的冗余信息以及减少网络中数据传输量，进而节省节点能量，延长网络生命周期。

物联网感知层中的大量传感器节点通常部署在无人监管的恶劣环境或安全敏感区域，使得网络中的数据融合面临着多种信息安全风险，如数据被窃听、伪造、篡改和重放等攻击，因此，安全的数据融合十分必要，相关研究得以开展[1]。

近年来，一些研究者从不同角度提出了不同的安全解决方案，其中，基于节点信誉度评价的数据融合方法得到了重视。为了量化数据融合结果的不确定性以及抵抗数据融合过程中节点被捕获等攻击，本文建立了一个改进的基于节点信誉度的安全数据融合模型(improved creditability-based data aggregation，ICBDA) ，用以解决数据融合过程中数据源的安全问题，保证数据融合结果的真实性。

1 相关工作

到目前为止，研究者对数据融合的安全实现方法进行了多种方案的探索。

SIA(secure information aggregation) 协议[2] 首先给出数据融合节点的数据融合结果，然后采用高效的抽样和交互证明来确保融合值是真实值的近似。SIA 协议还给出对多种计算函数的聚集方法，如果想要得到可靠性较高的数据值，交互次数就会相应增加，为完成数据融合所消耗的节点资源也会明显增多。

SecureDAV(secure data aggregation and verification) 协议[3] 使用密钥共享方案为簇内节点分配密钥，同时簇内节点对计算得到的簇内数据平均值进行部分签名。此方案可以验证融合数据的完整性，但是方案中只给出了计算平均值的聚集函数，公钥密码体制的应用将引入较大的计算量。

文献[4] 提出的安全数据聚合(secure data aggregation protocol，SDAP) 方法基于分而治之原理，节点的树形拓扑结构首先被动态地划分为多个类似大小的逻辑组(即子树) ，接下来的数据融合将在各个逻辑组逐跳进行，数据融合结果最终被传送到基站。基站根据这些逻辑组的融合结果集合识别可疑的数据融合逻辑组。

文献[5] 提出了一种高效安全的基于模式码的数据融合协议(efficient and secure pattern based data aggregation，ESPDA) ，该协议所进行的安全数据融合操作采用的是无任何物理意义的模式码，在数据传输过程中，中间节点不关心信息的具体内容，也就没必要对密文进行解密和再加密，这样可确保数据的机密性并避免中间节点处消息被窃听问题; 基站周期性广播密钥也有助于保障数据的新鲜性。随后，罗蔚等[6] 提出一种高效安全的数据融合协议(efficient and secure data aggregation，ESDA) ，采用模糊算法和模式码来消除传感节点所感知原始数据的冗余信息并执行相应的数据融合操作，这有助于提高数据的机密性和传感器节点的能效性。

Ganeriwal 和 Srivastava 在研究数据融合技术时，针对无线传感器网络提出了第一个基于声誉的传感器网络框架(reputation based framework sensor networks，RFSN) 信任模型[7]。该模型采用统计和决策理论，构建了一个十分有应用前景的分布式、可扩展的框架。RFSN 信任模型把计算得到的信任值作为节点参与数据融合时所提供数据的权重。

文献[8] 提出的基于分布式声誉机制的信标节点信任系统(distributed reputation based beacon trust system，DRBTS) 方案将网络中的节点分为传感节点和信标节点，信标节点的提出是本方案的一个亮点，信标节点被用于确定传感节点的位置。在该方案中，每个信标节点的主要任务是监测其邻居信标节点的行为，传感节点采用简单的多数投票机制来确定是否使用给定的信标位置信息，这样做是为了把恶意信标节点报告的虚假位置信息给过滤掉。

文献[9] 提出的加权信任评价(weighted trust evaluation，WTE) 方案是利用节点权值作为节点信誉值来进行数据融合的操作，再将实际值与数据融合结果作比较，结果不同，则说明对应的节点可疑，并用惩罚系数来降低该节点的信誉值，通过将信誉

值和融合结果不断迭代,最后筛选确定是否存在恶意节点。文献[10]提出的加权置信过滤(weighted confidence filter,WCF)算法,在WTE算法基础上进行了一定程度的改进,该算法过滤掉信誉值在平均信誉值以下的节点,只允许剩余的节点参与之后的数据融合,此方案较WTE而言,其数据融合值更接近于实际值。

上述安全方案或者增加了节点间的交互次数,或者对节点的计算与存储资源提出了过高的挑战。本文建立的ICBDA模型首先根据粗大误差判别准则识别并拒绝差值较大的节点感知数据,然后参考Josang信任模型,利用正态分布规律计算节点信誉值,信誉值高于预设阈值的节点参与数据融合,最后对数据融合结果进行评价,用评价的期望来表达对数据融合结果的可信赖程度。

2 网络模型假设

本文假设网络为层次型结构,由多个簇组成,每一个簇都由一个簇头节点和若干普通节点构成,簇头主要负责将来自普通节点的数据进行融合,并将数据融合结果通过多跳路由发送给基站。因为相比于平面型网络,层次型结构网络非常适合于大规模节点部署,具有更好的应用适应性,且引入数据融合有助于减少网络数据传输量,降低节点的数据传输能耗。

层次型结构如图1所示,SN代表普通节点,FN代表簇头节点,BS代表基站。本文中还对网络做如下假设:①基站位于网络的顶层,是传感器网络和应用网络的联接点,有强大的计算能力、足够的内存和丰富的能量,基站是完全可信的;②物联网感知层因传感器节点众多、分布密集,其采集的数据具有冗余性;③网络部署初期,所有节点都是安全可信的,且具有相同的能量、相同的储存能力、相同的处理能力,每个节点都有独立的ID标识[11]。

3 改进的安全数据融合模型

3.1 整体思路

文献[12]建立了基于信誉度的安全数据融合模型(creditability based data aggregation,CBDA),融合节点根据簇成员节点的采样数据,得到每个成员节点的信誉度,只允许有高信誉度节点的采样数据参与融合操作,计算融合结果并对其进行评价;将融合结果及其评价传给汇聚节点(即基站)用于决策利用。即使部分节点被捕获,该安全数据融合模型仍能保证融合结果的真实性,即具有较好的容错性。

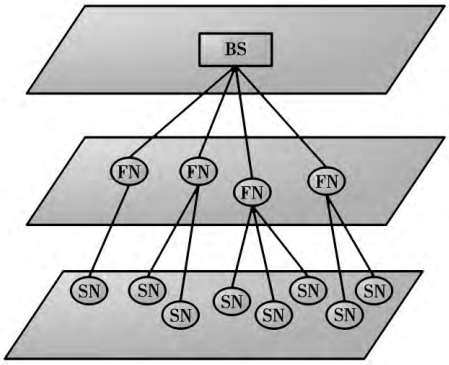

图1 层次型结构图

Fig. 1 Hierarchical structure

但该模型还存在一些明显的问题。例如,融合节点要计算所有普通成员节点的信誉值,这是对本就匮乏的网络资源的一种浪费。另外,该模型计算节点信誉值的方法,所用成员节点的历史累积信誉可能会掩饰其当前的恶意行为。

本文重点针对CBDA模型存在的问题进行了改进,改进后的基于节点信誉度的安全数据融合模型流程如图2所示。融合节点在接收成员节点发送来的感知信息之后,首先,通过误差理论识别明显偏离附近节点感知结果的数据,将其当作恶意数据或错误数据予以剔除;然后,计算和更新剩余成员节点的信誉值,确定信任节点;最后,融合节点只利用高信誉度节点的感知数据进行融合操作,对融合结果进行评价,并将融合结果和对结果的评价一起传输给汇聚节点,用来供基站完成最终的决策与数据利用。

由于物联网感知层中传感器节点具有分布密集的特点,地里位置上邻近的节点采集的数据必定存在冗余信息,基于统计和信息理论,通过检测节点所发送的感知数据来推定节点的信誉度,用来衡量每个节点可信赖的程度;根据节点信誉度的高低来决定是否采用其所采集数据进入数据融合操作,因此,每个融合结果和一个信誉度评价相关联,实现对融合结果不确定性的度量。

该方法的主要改进在于:要求簇头在计算成员节点信誉值之前,首先识别并剔除具有恶意倾向节点的数据(基于无线传感器网络的数据具有冗余性和该类节点采集的数据明显偏离附近节点的数据),不再计算其信誉值,其发送的数据不参与融合操作,这样既可以节约网络中的能量资源,又可以避免因为成员节点的历史累积信誉对其当前恶意行为

的掩饰，还可以得到较高的融合结果的评价，即对融合结果的可信赖程度越高。

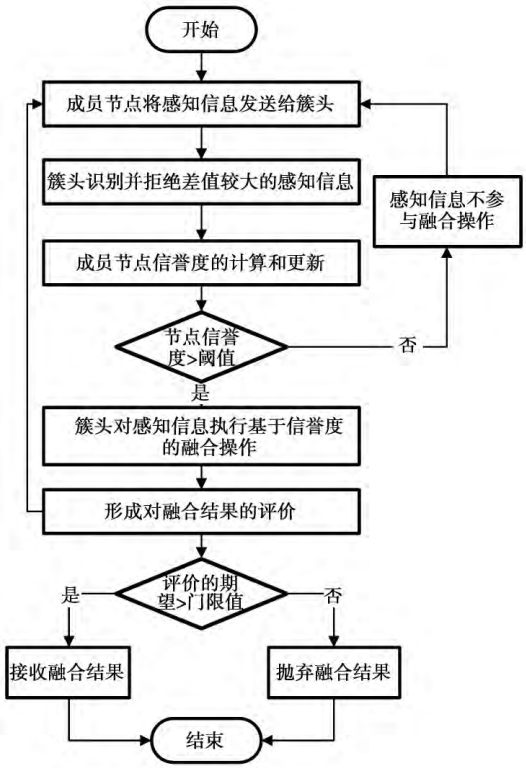

图 2　安全数据融合流程

Fig. 2　Flowchart of secure data aggregating

3.2　偏离正常感知数据的识别与剔除

物联网感知层传感器节点的主要功能是收集并返回节点所在监测区域的环境信息或被监测对象的状态数据，如被监测区域的温度、湿度等。一方面，物联网感知层中节点数量众多、地理位置上邻近节点所感知的数据具有冗余性; 另一方面，这些节点通常无法得到普遍的有人值守和维护，容易受到捕获、截听、恶意控制等攻击，出现恶意节点，从而发出偏离正常值的感知数据，即恶意节点要达到自己破坏、扰乱系统正常工作的目的，总是会发出与其邻近正常节点相差较大的错误或虚假数据，基于该数据得出的测量结果不具有真实性或新鲜性等特征，也就不具有应用价值，严重时可能导致决策错误。因此，必须发现和剔除这类含有较大差值的感知数据，从而隔离恶意节点对测量结果的影响。

要识别出偏离正常的感知数据，本文基于误差理论的知识采用粗大误差判别准则来进行识别。粗大误差判别准则主要包括 3σ 准则、罗曼诺夫斯基准则、格罗布斯准则和狄克松准则等，前 3 种粗大误差判别准则均需先求出被检验数据(即参与融合的数据) 的标准差 σ，计算过程相对复杂，对资源的需求较高，而狄克松准则用极差比的方法，得到简化而严密的结果，避免了这一点[13]。鉴于传感器节点资源受限的特点，这里选用对计算资源要求相对不高的狄克松准则。

对于测量值 $u_1, u_2, \cdots, u_n$ 的由小到大顺序统计量 $u(i)$ 的分布，当 u_i 服从正态分布时，得到最大值 $u(n)$ 的统计量表示为

$$\left.\begin{aligned} r_{10} &= \frac{u(n) - u(n-1)}{u(n) - u(1)} \\ r_{11} &= \frac{u(n) - u(n-1)}{u(n) - u(2)} \\ r_{21} &= \frac{u(n) - u(n-2)}{u(n) - u(2)} \\ r_{22} &= \frac{u(n) - u(n-2)}{u(n) - u(3)} \end{aligned}\right\} \tag{1}$$

同样地，最小值 $u(1)$ 的统计量可表示为

$$\left.\begin{aligned} r_{10} &= \frac{u(1) - u(2)}{u(1) - u(n)} \\ r_{11} &= \frac{u(1) - u(2)}{u(1) - u(n-1)} \\ r_{21} &= \frac{u(1) - u(3)}{u(1) - u(n-1)} \\ r_{22} &= \frac{u(1) - u(3)}{u(1) - u(n-2)} \end{aligned}\right\} \tag{2}$$

为了剔除粗大误差，狄克松准则认为 $n \leqslant 7$ 时，选用 r_{10} 效果好; $8 \leqslant n \leqslant 10$ 时，选用 r_{11} 效果好; $11 \leqslant n \leqslant 13$ 时，选用 r_{21} 效果好; $n \geqslant 14$ 时，选用 r_{22} 效果好。这里的 n 代表参与融合的数据个数，如以簇为单位进行融合时，n 就是簇内节点数。

选定显著度 α(其取值为 0. 01 或 0. 05 2 种情形) ，结合参与融合的数据个数 n，根据狄克松准则查表可得到对应的统计量的临界值 $r_0(n, \alpha)$，如果测量的统计值 r_{ij} 大于临界值，则认为 $u(n)$ 或 $u(1)$ 含有粗大误差。

例如，物联网感知层同一个簇内 15 个节点某一时刻感知到的环境温度(单位: ℃) 分别为 20. 42，20. 43，20. 40，20. 43，20. 42，20. 43，20. 39，20. 30，20. 40，20. 43，20. 42，20. 41，20. 39，20. 39，20. 40。先将数据由小到大进行排序，得到最小值 $u(1) = 20.30$; 最大值 $u(15) = 20.43$; 如果选用显著度 $\alpha = 0.05$，查表可知统计量的临界值 $r_0(15, 0.05) = 0.525$; 然后分别对 $u(15)$，$u(1)$ 根据(1) 式或(2) 式计算统计量 r_{22} 的值，根据计算结果可知: 对 $u(15)$ 而言，$r_{22} = 0$，小于 $r_0(15, 0.05)$，故其不含有粗大误

差,应保留;对 $u(1)$ 而言,$r_{22}=0.692$,大于 $r_0(15, 0.05)$,故其含有粗大误差,说明 20.30 ℃这个温度采集值明显偏离正常的感知温度,不被纳入数据融合范围,其对应的节点被认为是恶意节点,应从网络中予以剔除。按照同样的方法,对剩下的 14 个数据,重复上述步骤,直到所有数据中不再含有粗大误差,所有可能的恶意节点被剔除。

3.3 节点信誉度的计算和更新

无线传感器网络中包含的传感器节点成千上万个,它们在各自的分布区域内独立地感测外界环境;一般情况下,这些传感器节点所感知的数据遵循正态分布规律,而被捕获后的正常节点或恶意节点发出的数据将会明显偏离正态分布(否则达不到破坏系统的目的),因此,可参考 Josang 信任模型[14],利用正态分布规律计算节点的信誉度值。理想情况下,正态随机变量的取值在距离中心值 $[-\sigma, +\sigma]$ 的概率为 0.68(即伯努利分布),当存在恶意节点经常报告伪造数据时,实际概率分布就会与此概率不一致。以理想情况下的节点概率为标准,理想节点概率分布和实际节点概率分布的差异用距离来表征,这个距离能够代表节点信誉值。距离越小,节点的信誉度越高,反之亦然。

令某节点输出数据频率在距离中心值一倍标准差范围内的概率为 p_i,则在此范围外的概率为 $1-p_i$,那么它的偏离程度可表示为

$$D_i = \left|(1-p_i)\,\mathrm{lb}\frac{1-p_i}{0.32} + p_i\mathrm{lb}\frac{p_i}{0.68}\right| \tag{3}$$

本文定义对应节点的信誉值为

$$T_i = \mathrm{e}^{-\sqrt{D_i}} - kD_i \tag{4}$$

(4)式中,k 是惩罚因子。前半部分是一个指数运算,能够使得接近理想概率的节点得到比远离理想概率的节点高得多的信誉值,并能够反映一个节点的历史累积行为;后半部分是一个惩罚措施。惩罚因子的引入有助于对节点信誉值计算和更新时达到慢增快减的效果,便于快速发现和识别恶意节点,这对物联网感知层的应用是十分有利的。随着迭代次数的增加,节点的信誉值不断累积更新,如果节点的当前信誉值低于系统预设的阈值 T_0 时,系统自动将其判定为恶意节点,其提供的数据不再被采用。

ICBDA 模型中节点的信誉值可以分为累积信誉值和当前信誉值,累积信誉值是对节点过去感知数据的信赖程度的评定,它可以反映一个节点的历史累积行为,当前信誉值则是指节点当前时刻采样数据的信誉度,它具有实时性。该模型在数据融合中采用的是节点的当前信誉值,在节点当前信誉值的计算和更新时参考了节点的累积信誉值。

3.4 数据融合

ICBDA 模型利用高信誉值节点输出值进行加权数据融合,加权融合方法如图 3 所示,T 和 u 分别代表节点的信誉值和感知数据。

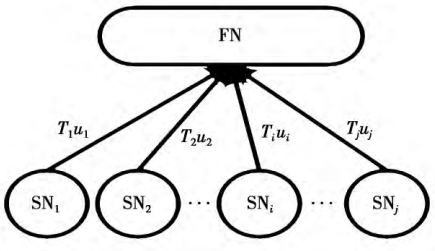

图 3 加权融合示意图

Fig. 3 Schematic of weighted aggregating

融合节点根据各个普通节点的信誉值和感知数据,按(5)式计算加权融合结果

$$U = \frac{\sum_{i=0}^{n} T_i \cdot u_i}{\sum_{i=0}^{n} T_i}, T_i > Th \tag{5}$$

(5)式中:U 是融合结果;Th 是高信誉度阈值;u_i 是第 i 个节点采集的数据;n 是参与数据融合的节点个数。只有节点信誉值高于 Th 的节点数据才能参与加权数据融合,融合过程中使用的权值即为节点的信誉值 T_i。这里只允许信誉值高于阈值的节点数据参与融合,既隔离了恶意节点数据对融合结果的影响,又减少了数据融合的计算量。

3.5 融合结果的评价

针对数据融合结果以及数据流中的不确定因素的处理问题,本文采用 Josang 信任模型,该模型通过一个被称为评价的信任来度量对于某种声明的可信赖程度[12]。

定义 评价 $W=(b,d,u,a)$,其中,a,b,d,u 分别表示对融合结果 U 的相对系数、信任度、不信任度和不确定度,它们应满足 $b+d+u=1$,$a\in[0,1]$。

评价的期望概率可表述为

$$E(W) = b + u \times a \tag{6}$$

即期望概率取决于信任度和不确定度的综合结果,a 的作用是决定不确定度对评价期望概率的贡献程度。

针对物联网感知层的安全数据融合结果的可信

赖程度，我们基于 Josang 信任模型借助“评价”来衡量，信任模型是基于节点数据的统计理解实现对节点的信任评价，即度量源于感知数据的统计特征，普通节点的累积信誉和实时行为数据被融合节点不断地进行分析来更新其信誉度。在得出节点的信誉值和融合结果后，融合节点就能够形成对融合结果的评价，对应着融合结果的可信任程度。

数据融合结果评价的期望与节点的当前信誉值和累积信誉值是密切相关的，通过(6)式可以知道评价的期望概率取决于节点的信任度和不确定度，即节点信誉值的大小，节点信誉值包括节点累积信誉值和当前信誉值。ICBDA 模型在计算节点当前信誉值时加入了一个惩罚措施，这有助于节点信誉值计算和更新时达到慢增快减的效果，可避免成员节点的历史累积信誉掩饰其当前的恶意行为，因此，可以得到较高的数据融合结果评价的期望。

4　实验仿真与模型评估

假设物联网感知层的传感器节点网络已通过分簇算法形成了若干个簇，每个簇有一个簇头节点和若干个成员节点，每个节点的感知数据遵循正态分布规律。采用 MATLAB 仿真平台对 ICBDA 模型进行评估。

仿真参数主要包括实验迭代轮数 R，网络中恶意节点比率 P，信誉惩罚因子 k，数据融合信任阈值门限 Th 和簇内节点个数 n，本文仿真实验中它们的取值分别为 30，0.02，0.06，0.5 和 30; 30 个簇内节点中，假设前 3 个节点为恶意节点。

4.1　节点信誉值比较

簇内节点信誉值是安全数据融合模型的一个重要指标，是影响数据融合结果可靠性、可信度和融合效率的一个主要因素。

ICBDA 模型和 CBDA 模型的节点信誉值比较如图 4 所示。由图 4 可见，2 种模型的前 3 个节点的信誉值都明显低于其余节点的信誉值，这是因为仿真实验设定前 3 个节点被假设为恶意节点。另外，ICBDA 模型相比于 CBDA 模型，其恶意节点信誉值更低，而正常节点的信誉值明显更高，这是因为 ICBDA 模型在计算成员节点信誉值之前，通过狄克松准则识别出包含粗大误差感知数据的节点，其感知的数据并不参与数据融合，这可增加节点输出数据落在距离一倍标准差范围内的概率，从而有助于提高正常节点的信誉值; 而 CBDA 模型并没有这样的机制，即使出现包含粗大误差的感知数据仍要参与数据融合操作。

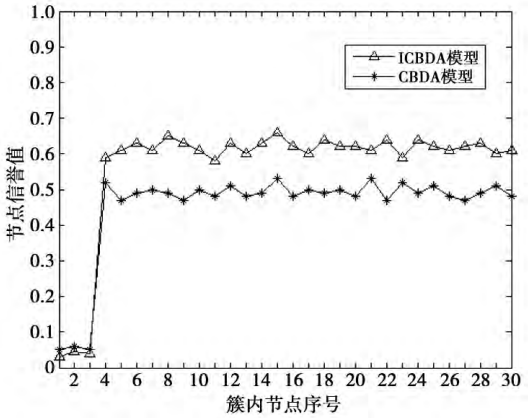

图 4　节点信誉值对比

Fig. 4　Comparison of node creditability

4.2　数据融合结果及其评价的比较

数据融合值是评判数据融合结果准确性的一个重要依据。

理想情况、ICBDA 模型和 CBDA 模型的数据融合值对比如图 5 所示。其中，理想情况数据融合值表示簇内没有恶意节点存在的情况下得到的数据融合结果，即无干扰的真实结果。由图 5 可见，ICBDA 模型的数据融合值和真实值比较接近，而 CBDA 模型的数据融合值偏离真实值的程度更大，这是因为 ICBDA 模型对参与融合的数据进行了严格的筛选，提高了参与数据融合的真实感知数据的比例，从而改善了数据融合结果的准确性。

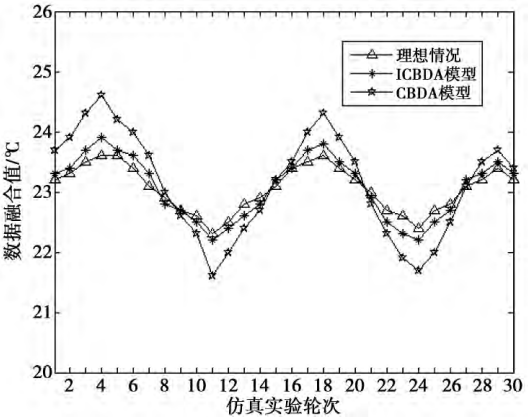

图 5　数据融合值对比

Fig. 5　Comparison of data aggregating value

融合结果的评价和评价的期望有助于进一步衡量数据融合结果的可信赖程度。

ICBDA 模型和 CBDA 模型的数据融合结果评价期望值对比如图 6 所示。由图 6 可见，ICBDA 模型的期望值普遍高于 CBDA 模型，这是因为 ICBDA

模型在计算节点信誉值时引入一个惩罚措施,这可避免成员节点的历史累计信誉掩饰其当前的恶意行为,从而提高了对数据融合结果评价的期望。即ICBDA模型的数据融合结果更值得信赖。

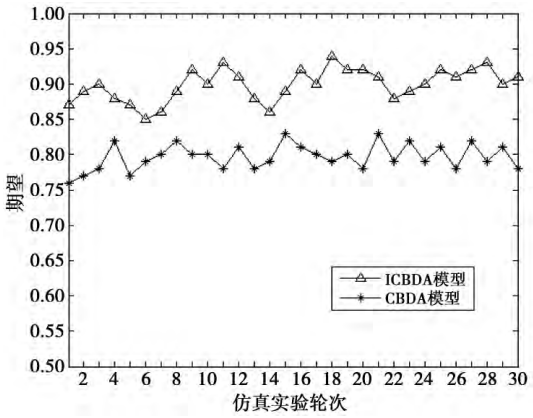

图6 数据融合结果评价期望值对比

Fig. 6 Comparison of estimate expectation for data aggregating results

4.3 模型的效率优势和适应性

改进的ICBDA模型摒弃了CBDA模型中融合节点需要计算所有普通成员节点信誉值的做法,而是首先基于误差理论,选用对计算资源要求不高的狄克松判别准则来识别并剔除恶意节点,不再计算其信誉值,也不接受其数据参与融合操作,从而减少计算量,大大提高数据的处理效率;同时,这种方法对资源严格受限的物联网感知层是友好的,具有良好的适应性。

5 结 论

作为"互联网+"的典型代表,物联网在互联网基础上进行了感知层的拓展,由此引出了感知层的数据融合及其安全问题。本文以提升物联网感知层数据融合结果的安全性为目标,结合网络中节点资源有限的突出特点,运用粗大误差理论、概率统计理论和Josang信任模型建立了一个改进的结合数据预处理与节点信誉度评价的安全数据融合模型—ICBDA,该模型首先基于粗大误差理论将明显偏离正常数据(或真值)的异常数据予以识别和剔除;然后,基于概率统计理论计算和更新节点信誉度,只允许高信誉度的节点数据参与数据融合操作;最后,基于Josang信任模型得到对数据融合结果的评价。该模型本质上是将对节点的信誉度评价转化成节点感知数据的统计处理,以物联网感知层传感器节点所感知信息的统计特征为度量标准,基于分析计算节点的累积信誉和实时行为特征得出其信誉度,并滤除低信誉值节点的数据,从而实现既降低恶意节点对融合结果的影响,又减少数据融合操作对系统资源的需求。仿真实验结果验证了所建立的ICBDA模型在节点信誉、融合结果和融合性能等方面的改进,有助于提升物联网感知层数据融合的安全性。

参考文献:

[1] 胡向东,魏琴芳,向敏,等. 物联网安全[M]. 北京:科学出版社,2012:115-120.
HU Xiangdong, WEI Qinfang, XIANG Min, et al. The Internet of things security [M]. Beijing: Science Press, 2012:115-120.

[2] PRZYDATEK B, SONG D, PERR IG A. Sia: secure information aggregation in sensor networks [C]//ACM. Proceedings of the 1st ACM International Conference on Embedded Networked Sensor Systems. New York: ACM, 2003: 255-265.

[3] MAHIMKAR A, RAPPAPORT T S. SecureDAV: a secure data aggregation and verification protocol for sensor networks [C]//IEEE. IEEE Global Telecom-munications Conference, 2004. New York: IEEE, 2004: 2175-2179.

[4] YANG YI, WANG Xinran, ZHU Sencun, et al. SDAP: a secure hop-by-Hop data aggregation protocol for sensor networks [C]//Proc of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing, Florence, Italy. New York: ACM, 2006, 356-367.

[5] CAM H, OZDEMIR S, SANLI H O. ESPDA: energy efficient and secure pattern based data aggregation for wireless sensor networks [C]// IEEE. Proceedings of the 2nd IEEE Conference on Sensors. New York: IEEE Society Press, 2003: 732-736.

[6] 罗蔚,胡向东. 无线传感器网络中一种高效的安全数据融合协议[J]. 重庆邮电大学学报:自然科学版, 2009, 21(1): 110-114.
LUO Wei, HU Xiangdong. An efficient security data fusion protocol in wireless sensor network [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2009, 21(1): 110-114.

[7] GANERIWAL S, BALZANO L K, SRIVASTAVA M. Reputation based framework for high integrity sensor networks [J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37.

[8] SRINIVASAN A, TEITELBAUM J, WU J. DRBTS: distributed reputation based beacon trust system [C]// IEEE. Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, USA. New York: IEEE, 2006: 277-283.

(下转第891页)

[J]. 通信学报,2006, 27(12): 6-9
WANG Qinglong, YANG Bo, HAN Zhen, et al. Collusion-free public-key traitor tracing scheme [J]. Journal on Communications, 2006, 27(12): 6-9.

[10] 王云,芦殿军,张秉儒. 基于身份的公钥叛逆者追踪方案 [J]. 青海师范大学学报: 自然科学版,2012(1): 31-35.
WANG Yun, LU Dian jun, Zhang bing ru. A traitor tracing scheme based on bilinear map [J]. Journal of Qinghai Normal University: Natural Science, 2012(1): 31-35.

[11] 张学军. 新的面向多服务的叛逆者追踪方案 [J]. 电子科技大学学报, 2008, 37(3): 404-407.
ZHANG Xuejun. A new multi-services oriented traitor tracing scheme [J]. Journal of University of Electrical Science and Technology of China, 2008, 37(3): 404-407.

[12] 王青龙,徐丽. 两个叛逆者追踪方案的安全性分析 [J]. 计算机工程与科学. 2013, 35(6): 78-81.
WANG Qinglong, XU Li. Security analysis of two traitor tracing schemes [J]. Computer Engineering and Science, 2013, 35(6): 78-81.

[13] 王青龙,韩臻,杨波. 基于双线性映射的叛逆者追踪方案 [J]. 计算机研究与发展,2009,46(3): 384-389.
WANG Qinglong, HAN Zhen, YANG Bo. A traitor tracing scheme based on bilinear map [J]. Journal of Computer Research and Development, 2009, 46(3): 384-389.

[14] 王晓明,姚国祥,廖志委. 一个叛逆者追踪方案分析和改进 [J]. 计算机研究与发展,2013,50(10): 2092-2099.
WANG Xiaoming, YAO Guoxiang, LIAO Zhiwei, Cryptanalysis and Modification of a Traitor Tracing Scheme [J]. Journal of Computer Research and Development, 2013, 50(10): 2092-2099.

[15] KAWAHARA Y, TAKAGI T, OKAMOTO E. Efficient implementation of Tate Pairing on a Mobile Phone Using Java [C] // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2007: 396-405.

作者简介:

康桂花(1962-),女,浙江东阳人,副教授,主要研究方向为信息安全、网络协议和计算机应用。E-mail: 841936744@qq.com。

(编辑: 张　诚)

(上接第 882 页)

[9] ATAKLI I, HU H, CHEN Y. Malicious node detection in wireless sensor networks using weighted trust evaluation [C] //ACM. Hassan Rajaei. Spring Simulation Multiconference. Ottawa, Canada: ACM Press, 2008: 836-843.

[10] HU Xiangdong, YU Pengqin, WEI Qinfang. Securing sensor networks based on optimization of weighted confidence [J]. China Communications, 2012(8): 122-128.

[11] 崔慧,潘巨龙,闫丹丹. 无线传感器网络中基于安全数据融合的恶意节检测 [J]. 传感技术学报,2014,27(5): 664-669.
CUI Hui, PAN Julong, YAN Dandan. Based on security data fusion of malicious node detection in wireless sensor network [J]. Journal of Sensing Technology, 2014, 27(5): 664-669.

[12] HU Xiangdong, WEI Qinfang, TANG Hui. Model and simulation of creditability-based data aggregation for the internet of tings [J]. Chinese Journal of Scientific Instrument, 2010, 31(11): 2636-2640.

[13] 费业泰. 误差理论与数据处理 [M]. 北京: 机械工业出版社,2007: 43-49.
FEI Yetai. The error theory and data processing [M]. Beijing: China Machine Press, 2007: 43-49.

[14] JOSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for online service provision [J]. Decision Support Systems, 2007, 43(2): 618-644.

作者简介:

魏琴芳(1971-),女,云南曲靖人,重庆邮电大学高级工程师,主要研究方向为无线通信与编码等。E-mail: weiqf@cqupt.edu.cn。

程利娜(1988-),女,河南濮阳人,重庆邮电大学硕士研究生,主要研究方向为无线通信与物联网技术等。E-mail: 641041551@qq.com。

(编辑: 王敏琦)