DOI:10.19329/j.cnki.1673-2928.2015.02.009

基于数据和能量可信的物联网信任模型

朱 程

(蚌埠学院 计算机科学与技术系,安徽 蚌埠 233030)

摘 要:正在掀起第三次信息技术革命的物联网具有巨大的应用前景,其信息传递通过传感器节点实现,由于传感器节点具有能量、计算能力有限等特点,需要进行数据融合。物联网在进行数据融合过程中易受到各种类型的攻击,为了保证融合结果的真实性和可靠性,建立了一种基于数据和能量可信的信任模型,仿真结果表明该模型具有一定的可靠性。

关键词:物联网;数据融合;信任模型

中图分类号:TP212.9;TP393.08 **文献标志码**:A **文章编号**:1673-2928(2015)02-0022-03

物联网被认为是继计算机、互联网、移动通信网络之后的又一次信息产业革命。它通过各种可能的网络接入,实现物与物、物与人的泛在连接,从而实现对物品和过程的智能化感知、识别和管理[1]。实现物联网的关键技术之一是无线传感器网络,它通过传感器节点实现数据的采集和传递。由于传感器节点受到能量和计算能力有限等约束,需要进行数据融合。保证融合过程中节点数据的安全性是物联网实现基础信息采集和后续应用的基本要求[2]。

近年来,对网络的可信研究已经成为一个热点[3]。信任是传感器节点在数据交互或合作中的信誉度,能够降低节点之间的交互风险。所谓信任模型,就是根据节点本身与其他节点之间交互的历史数据进行量化,建立评价体系,通过计算信任值来判断节点的可信程度[4]。

本文针对物联网中传感器节点存在不安全因素的问题,利用节点的数据和剩余能量综合评价建立信任模型。计算节点的数据信任值和能量信任值,并根据其在不同环境下的重要性,分别赋予不同的权重,用式(1-1)计算节点信任值。其中T_C表示节点信任值,T_D表示节点的数据信任值,T_E表示节点的能量信任值,μ_1和μ_2表示权重,$\mu_1+\mu_2=1$。

$$T_C=\mu_1*T_D+\mu_2*T_E \tag{1}$$

1 节点的信任模型

1.1 数据信任值的计算

在物联网中,传感器节点感知的数据在进行融合时不仅与节点本身的历史数据有关(即时间相关),也与同区域内其他节点的数据有关(即空间相关),并且节点行为特征随时间的变化规律具有某些统计特征[5]。因此,计算节点的信任值可以利用同一区域内节点采集的数据在时间、空间上的相关性,这样能够减少节点之间的数据交换。

1.1.1 相似度矩阵

若物联网中参与数据融合的节点集合为$S=(s_1,s_2,\cdots,s_n)$,$z_i(k)$表示k时刻节点s_i的输出,$\Phi(k)$表示状态转移矩阵,$G(k)$表示过程噪声分布矩阵,$H(k)$表示输出矩阵,$V(k)$表示具有零均值的高斯噪声向量,$W(k)$表示正定协方差矩阵的高斯噪声向量。采用Kalman滤波算法[6]进行状态更新。可用式(2)描述系统的状态方程和输出方程。

$$\begin{cases}X(k+1)=\Phi(k)X(k)+G(k)V(k)\\Z(k)=H(k)X(k)+W(k)\end{cases} \tag{2}$$

由于节点所处的环境和自身行为不一致,状态估计向量会略有差异。为度量这一差异,用$C_{ij}(k|k)=P_i(k|k)+P_j(k|k)$表示两个测量的估计误差协方差之和,定义k时刻的状态估计向量的标准化差为式(3)。由正态型隶属度函数的模糊测度可定义k时刻两状态向量的相似度为式(4)。

$$u_{ij}(k)=C_{ij}^{-1/2}(k|k)\left[\hat{X}_i(k|k)-\hat{X}_j(k|k)\right] \tag{3}$$

$$d_{ij}(k)=\exp[-bu_{ij}^T(k)u_{ij}(k)] \tag{4}$$

其中b是系数,$u_{ij}(k)$和$d_{ij}(k)$分别表示列矢量和标量。由于同一区域中数据融合过程由独立的节点组成,因此状态向量间的相似程度也代表了节点测量值之间的相似程度。

由以上相似度可得k时刻参与数据融合各节点在同一区域的相似度矩阵为式(5)。

$$D(k)=\begin{bmatrix}1 & d_{ij} & \cdots & d_{1n}\\ d_{21} & 1 & \cdots & d_{2n}\\ & & \ddots & \\ d_{n1} & d_{n2} & \cdots & 1\end{bmatrix} \tag{5}$$

收稿日期:2014-11-21

基金项目:蚌埠学院2014年院级自然科学项目(2014ZR08);安徽省大学生创新训练项目(AH201311305069)。

作者简介:朱程(1984-),女,江苏镇江人,蚌埠学院计算机科学与技术系助教,硕士,研究方向:计算机网络。

相似度矩阵描述了k时刻物联网中同一区域节点$S=(s_1,s_2,\cdots,s_n)$的测量在空间分布的信息,是对节点空间信任值的计算。时间系列{D(k),k=1,2,…}描述了到当前时刻为止节点在时间分布的信息,是对节点时间信任值的计算。

1.1.2 节点的数据信任值计算

设初值为零,$c_i(k)$表示k时刻节点i的计数器。$d_{ij}(k)$表示式(5)中第i行第j列,若$d_{ij}(k)\geq E_1$ (E_1是阈值),则计数器加1。$c_i(k)$表示k时刻与节点i测量数据较为相似的节点数目。$c_i(k)$越大,表示k时刻节点i的数据与大多数节点数据一致,这些数据可能组成一个真值的集合;$c_i(k)$越小,表示k时刻节点i的数据与大多数节点数据不一致,成为假值的可能性较大,那么可信的程度就较低。可见$c_i(k)$表示节点数据一致性的度量。定义k时刻节点i的一致性测度为式(6)。

$$p_i(k)=c_i(k)/n \tag{6}$$

$p_i(k)$是一种可能性测度,显然$0\leq p_i(k)\leq 1$。则$p(k)=[p_1(k),p_2(k),\cdots,p_n(k)]$表示k时刻节点集合$S=(s_1,s_2,\cdots,s_n)$的一致性向量。

对物联网中节点i而言,其自身可靠性也是影响可信度的一个重要因素,这种可靠性通常会通过自身测量的时间系列表现出来,而节点行为过程可看成是节点按照时间次序排列的周期性读数。由于节点的计算和存储能力有限,因此在节点上只能保存一段时间内的数据。设$[p_i(1),p_i(2),\cdots,p_i(k)]^T$表示节点i一致性测度的时间序列,则式(7)表示综合的一致性测度。

$$\bar{p}_i(k)=\frac{1}{k}\sum_{t=1}^{k}p_i(t) \tag{7}$$

如果序列波动不大,说明节点i的可靠性较高。则节点i的可靠性测度为一致性测度的方差,式(8)表示节点行为信任可靠值的计算。

$$\sigma_i^2(k)=\frac{1}{k}\sum_{t=1}^{k}\left[\bar{p}_i(k)-p_i(k)\right]^2 \tag{8}$$

信任度高的节点一致性较大且可靠性较高,即$\bar{p}_i(k)$较大而$\sigma_i^2(k)$较小。而对于节点i,$\bar{p}_i(k)$的大小与$\sigma_i^2(k)$的大小并没有必然的联系。因此,采用映射$f[\bar{p}_i(k),\sigma_i^2(k)]$综合,使节点行为可信度与$\bar{p}_i(k)$正相关,与$\sigma_i^2(k)$负相关。定义节点的数据可信度为式(9),其中$0<a\leq 1$。

$$T_D(k)=f[\bar{p}_i(k),\sigma_i^2(k)]=[1-a\sigma_1(k)]\bar{p}_i(k) \tag{9}$$

相似度需要计算n个节点两两之间的标准化差,一致性测度需要将阈值E_1与n^2维的相似度矩阵元素依次比较,计算的复杂度较高。为减少计算量,使用式(10)和式(11)的递推公式计算综合一致性测度和可靠性测度。

$$\bar{p}_i(k)=\frac{k-1}{k}\bar{p}_i(k-1)+\frac{1}{k}p_i(k) \tag{10}$$

$$\sigma_i^2(k)=\frac{k-1}{k}\left\{\sigma_i^2(k-1)+\frac{1}{k}[p_i(k)-\bar{p}_i(k)]^2\right\} \tag{11}$$

1.2 能量信任值的计算

在物联网中,节点之间的数据传输是建立在以簇为基础的网络结构上的,一般簇成员节点将采集到的数据直接发给簇头节点,簇头节点对接收到的数据进行融合,再将融合后的数据通过一跳或多跳的方式发送给基站。节点依靠电池来供电,每个节点的生命期与整个网络的生命期息息相关。如果过分集中消耗某一节点的能量,会造成节点的过早失效,从而影响整个网络。因此,在进行数据融合时,要及时了解目前网络中节点的剩余能量,确定节点能量信任值,避免低竞争力节点能量过度消耗。本文采用与文献[7]相同的无线通信能耗模型进行节点能耗分析,如图1所示。

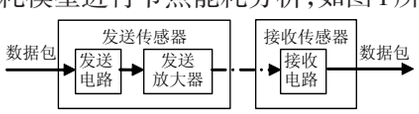

图1 无线通信能耗模型

若节点发送$l$bit的信息到距离d,节点消耗的能量模型为式(12)。E_{elec}表示发送节点和接收节点每发送和接收单位比特的能耗值,ε_{fs}和ε_{mp}表示发射放大器的单位能耗。

$$E_C=\begin{cases}l*E_{elec}+l*\varepsilon_{fs}*d^2 & d<d_0\\ l*E_{elec}+l*\varepsilon_{mp}*d^4 & d\geq d_0\end{cases} \tag{12}$$

d_0表示传输距离阈值,当实际的传输距离小于阈值时,节点能耗与距离的平方成正比,当实际的传输距离大于阈值时,节点能耗与距离的四次方成正比。由此可见,在进行数据传输时,应通过节点逐跳接力的方式传递数据,而尽量避免直接向远距离节点传输数据,达到减少能耗的目的。

若用E_S表示节点的初始能耗,E_C表示发送能耗,E_O表示正常的工作能耗,那么节点的当前能量可表示为$E_S-E_C-E_O$,则节点的能量信任值T_E表示为式(13)。T_E越大,节点的剩余能量越多,采用当前节点进行数据传输就越可靠。

$$T_E=\frac{E_S-E_C-E_O}{E_S} \tag{13}$$

1.3 仿真结果及分析

仿真实验采用UC Berkley大学开发的仿真工具NS2,MAC层协议设定为802.11,采用路由协议DSR,将本文建立的模型在不信任行为检测率方面与文献[8]中单纯依靠数据信任度的BTSR算法进行仿真比较。不信任行为指节点的身份认证是正确的,而传输的数据是错误的,且与正常值有一定的偏差,节点不信任行为的概率是不正常行为的节

点数目与节点总数的比值。

在仿真试验中，将1024个节点均匀部署在100m*100m的区域中。设节点的无线通信半径为$\sqrt{2}$m，每个节点的能量初值为0.5J，数据包大小为525bytes，控制包大小为256bytes，发送数据的单位能耗E_{elec}为50nJ/bit，ε_{fs}为50pJ/(bit*m^2)，ε_{mp}为0.005 pJ/(bit*m^4)。

在BTSR算法中，节点的信任值只考虑了数据信任值，即μ_1和μ_2的取值分别为100%和0%，而在本文的信任模型中，节点的信任值除了与数据信任值相关外，还与能量信任值有关，在实验中μ_1和μ_2分别取值为50%和50%，实验结果如图2所示。

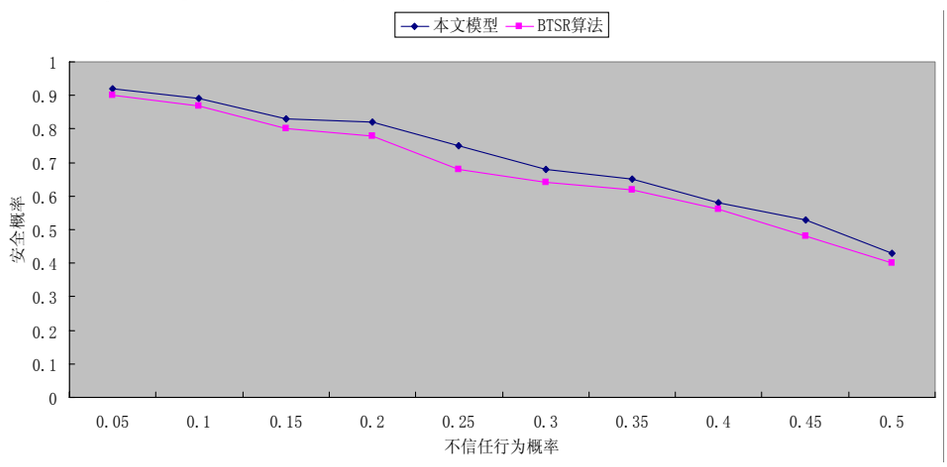

图2 仿真实验结果分析

图2表明，与BTSR算法相比，本文所建立的模型在发生相同的不信任行为概率时，其安全概率更高，网络也相对更可靠。

2 结论

本文利用节点行为的时间和空间相关性计算节点之间的相似度，并得出节点的数据信任值，通过剩余能量计算节点的能量信任值，在不同的环境下赋予不同的权重，综合得出节点的信任值，从而提出了一种在物联网中进行数据融合的信任模型。分析和仿真实验表明，当网络中有大规模的不安全行为时，本文建立的模型与BTSR算法相比，具有较高的安全概率。

参考文献：

[1] 刘海涛，马建，熊永平.物联网技术应用[M].北京：机械工业出版社，2011.

[2] 胡向东，魏琴芳，唐慧.物联网中数据融合的信誉度模型与仿真[J].仪器仪表学报，2010，11(11)：2636-2640.

[3] 林闯，彭雪海.可信网络研究[J].计算机学报，2005，28(5)：751-758.

[4] 江自兵.基于信任管理的无线传感器网络容错技术的研究[D].芜湖：安徽工程大学，2011.

[5] 刘敏华，萧德云.基于相似度的多传感器数据融合[J].控制与决策，2004，19(5)：534-537.

[6] JOHN M R. Fusion of multi-sensor data[J].The IntJ of Robotics Research, 1988,7(6): 78-96.

[7] 何延杰，李腊元，邢明彦.WSN中一种能量均衡的分簇路由协议的设计[J].传感技术学报，2009，22(10)：1510-1514.

[8] 朱程，周鸣争，许金生.BTSR:一种基于行为可信的安全数据融合与路由算法[J].计算机应用，2008，28(11)：2820-2823.

[9] 刘艳飞.基于分层信任管理的无线传感器网络信任模型[D].太原：太原理工大学，2012.

Trust Model for Internet of Things Based on Trust Data and Energy

ZHU Cheng

(Department of Computer Science and Technology, Bengbu University, Bengbu 233030, China)

Abstract: The Internet of Things, which is surging the third tide of information technology, has tremendous application prospect. It transmits information based on sensor nodes. Data aggregation is necessary for Internet of things, as one of its characteristic, has limited energy, calculation and etc. It could be easily threatened during data aggregating. To guarantee the authenticity and reliability of the data resulting from aggregation, a model based on trust data and energy is proposed, simulation experiments approve that the model is reliable.

Key words: internet of things; data aggregation; trust model

(责任编辑：赵建周)