A Reliable Data Gathering Algorithm for Clustering WSNs Based on Trust Model*

CHEN Hui, ZHANG Chunyu*

(*Anhui University of Science & Technology, College of Computer Science and Engineering, Huainan Anhui* 232001, *China*)

Abstract: Aiming at the problem that the reliability of monitoring data becomes low due to abnormal or interfered nodes in wireless sensor networks(WSNs), a data gathering algorithm based on trust model is proposed. The algorithm firstly uses the box model to select the nodes whose data values change greatly at the current moment and determines whether they are abnormal data nodes. Then, whether data is collected is determined according to the proportion of abnormal data nodes and the credibility of nodes. When the number of abnormal nodes is lower than the set threshold, data is collected after filtering out the abnormal nodes with low credibility based on the trust model; when is higher than the set threshold, the urgent data transport mechanism for the occurrence of monitoring events is activated to ensure the rapid data collection. The simulation results show that the average detection rate of the proposed algorithm is about 9.14% higher than that of the classical trust model RFSN under different proportions of abnormal nodes, and the average data gathering accuracy is about 20% higher than that of the original HEED protocol.

Key words: WSN; clustering structure; data gathering; trust model

EEACC: 7230 **doi**: 10.3969/j.issn.1004-1699.2021.11.017

基于信任模型的分簇 WSNs 可靠数据采集方法*

陈 辉*, 张春雨

(安徽理工大学计算机科学与工程学院, 安徽 淮南 232001)

摘 要: 针对无线传感器网络由于节点异常或受干扰等原因导致网络监测数据可靠性降低的问题, 提出一种基于信任模型的可靠数据采集方法。该方法首先利用箱型模型筛选当前时刻采集的数据值变化较大的节点, 并判断其是否为异常数据节点; 然后, 根据异常数据节点的占比和节点可信度确定数据是否被采集。当数据异常节点数量低于设定阈值时, 基于信任模型过滤掉可信度低的非正常节点后再对数据进行采集; 当高于设定阈值时, 启动监测事件发生时的紧急数据传输机制, 以保障紧急数据的快速收集。仿真实验结果表明: 该算法在不同异常节点占比下较经典信任模型 RFSN 平均检测率高 9.14%左右; 较原生 HEED 协议平均数据采集准确率高 20%左右。

关键词: 无线传感器网络; 分簇结构; 数据收集; 信任模型

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2021)11-1530-07

无线传感器网络 WSN(Wireless Sensor Network)在军事、医疗和工业等方面有着广泛的应用, 集中体现在数据收集和事件监测方面[1-2]。然而, 无线传感器节点多为电池供电, 计算能力和带宽容量有限, 且经常部署在一些恶劣的环境中。这些因素极易导致节点出现异常和受到干扰, 进而造成监测数据的可靠性得不到保障[3]。无线传感器网络是以数据为中心的网络, 对突发事件的快速响应和数据的可靠采集是非常必要的[4-6]。

通常 WSN 中异常数据一方面由于节点自身故障或外界环境干扰引起的数据异常; 另一方面由突发事件引起的数据变化超出正常幅度。前者直接关

项目来源: 国家自然科学基金项目(61170060); 安徽省自然科学基金项目(1608085ME122); 安徽省重点教学研究项目(2020jyxm0458)

收稿日期: 2021-01-27 **修改日期**: 2021-05-20

系着网络监测数据可信度,而后者则是无线传感器网络监测重点,因此 WSN 数据异常检测和可靠性传输很有必要[7]。无线传感器网络中异常数据检测通常借助统计学方法或充分利用邻近节点之间的空间相关性。如文献[8]基于隐马尔科夫模型的数据异常检测方法,以先验数据为参考判断新产生的数据轨迹偏差,但阈值的设定需要大量数据支撑;文献[9]利用 K-Means 均值聚类对异常数据进行分类,对所有数据对象依据相似程度进行划分,该方法更适合集中式异常检测,对所有数据进行聚类算法复杂性较高。数据采集是无线传感器网络主要功能之一,而采集数据的可靠性直接决定着网络的安全运行[10],但仅对异常数据进行筛选还不能完全满足对无线传感器网络数据可靠性的要求。无线传感器网络中数据来自众多传感器节点,因此,传感器节点的可靠性是影响数据采集可靠性重要诱因之一,而信任模型的出现解决了传感器节点路由选择、数据认证等方面问题,为节点可靠性判断提供了理论支撑。目前,信任模型已广泛应用在无线传感器网络领域[11-13],其中,文献[11]通过信任模型帮助寻找可靠的节点,提高了节点之间的协作和系统的性能;文献[12]提出一种基于时间因素的 WSN 信任模型,利用动态反馈机制计算节点信任度,同时引入时间衰减模型降低网络时延、增加模型可信度;文献[13]在直接信任度计算时使用异常衰减修正贝叶斯方程,并以熵作为参考为节点信任度赋权,很好地克服了主观赋值的局限性。此外,借助 UAVs(Unmanned Aerial Vehicles)[14-15]可较为准确验证数据可靠性,但 UAVs 使用成本较高。当前 WSN 数据采集多以去冗余、降能耗为目的,如文献[16]用历史数据来降低冗余数据的采集,该算法只有在监测区域数据波动较小的情况下效果较好;采用压缩感知(Compressed Sensing)技术[17-18]对数据进行采集,能有效缓解硬件资源的压力,但压缩采集会导致部分数据的失真。而随着物联网应用要求的不断提高,如车联网、自动驾驶等,感知层数据可靠性变得尤为重要。

在实际应用中传感器节点一般以恒定频率进行数据的采集和传输,多数情况下数据是缓慢变化的,如温度、湿度、压力等。这种情况下“不可靠节点”的存在直接影响着检测结果的准确性,因此节点可靠性和数据可靠性的准确判断关系到网络的 QoS(Quality of Service)。基于多数节点出现“数据异常”为突发事件所致,少数节点出现“数据异常”一定概率上是节点异常或干扰所致的事实,本文提出一种基于信任模型的数据收集方法(Algorithm of Trust-based Data Gathering,AT-DG)。该算法以分簇型网络拓扑结构为基础,首先,基于数据时间相关性和空间相关性区分数据异常与否,并统计异常数据占比。然后,根据异常数据占比的不同采取不同的数据采集策略。对于少数“数据异常”,通过簇首节点信任评估机制判断节点可信度,进而得出异常数据产生原因,并采取相应的采集策略;对于多数“数据异常”,启动监测事件发生时的数据采集机制,实现紧急数据包的采集和传输。AT-DG 算法在保证一般数据可靠收集的同时,可实现监测事件发生时的快速响应。

1　网络模型

分层的 WSN 网络拓扑结构因其简单高效便于管理广泛应用在各种监测活动中。相邻传感器节点按照一定规则进行组合,形成一个“簇”,如图 1 所示。每个簇都有一个簇首和若干成员节点组成,并且簇间成员节点感知覆盖区域有一定重合。另外,同一簇内的成员节点在通信行为和空间特征上具有较高的相关性,这也使在簇头建立信任模型成为可能。同时,事件的发生也表现为部分簇内数据变化差异较大,以簇为单位的异常检测机制更容易实现。

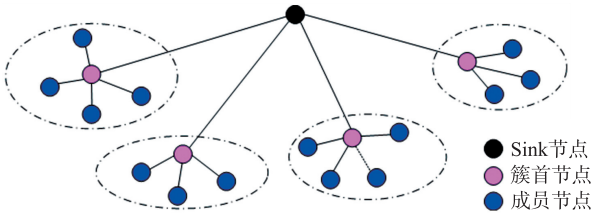


图 1　分簇的网络拓扑结构

本文依据 HEED 协议对网络进行层次划分,且网络中传感器节点满足以下条件:①网络中节点位置一旦确定就不在移动,且每个节点都有唯一的标识;②网络中只有唯一的 Sink 节点,网络中数据路由由簇首直接或间接地发送到 Sink 节点;③簇内各成员节点位置相邻且只能和本簇簇首通信;④每个节点通信半径、路由能耗相同且能源不可再生。

2　数据采集方案

2.1　数据异常判别和采集规则

通常情况下,如果簇内多数节点监测数据发生突变,监测事件应当是大概率发生,而少数节点监测数据发生突变很大程度上是采集数据错误。因此,可以通过设定异常数据占比的阈值来区分异常数据是监测事件发生还是错误数据。对于异常数据的判断,统计学中采用基于距离的方法可对异常数据进

行定义,即数据前后变化的差值[19]。为了突出异常数据的变化量和异常数据的占比,阈值的设定首先要针对数据变化量的定义,然后再判断这些节点占的比重,进而判断是事件发生还是数据错误。数据级异常检测通常利用节点数据流的时间性和空间性等特点,通过比较当前异常数据与历史数据、邻节点数据差异,进而计算节点信任度。数据异常检测方法中基于分类的方法由于其检测精度受到数据集规模的影响,不适合在资源受限的无线传感器网节点实现,而基于统计的异常检测更符合无线传感器网要求,其中四分位数展布法计算量小且收敛速度快,因此文中选用四分位展布法的箱型模型作为异常检测的依据。

基于监测数据的时间相关性设置大小为 M 的数据窗口,如图 2 所示。对于节点 i,当前时刻 t 采集的数据为 $a_i(t)$ 并记 $t=n\times\Delta t$,Δt 为采样间隔,则上一时刻,即 $(n-1)\times\Delta t$ 时刻采集数据为 $a_i(t-1)$。簇首利用箱型模型,即式(1)对节点 i 前 $M-1$ 个数据进行箱型计算并划分可信区间 $[\varepsilon_a,\varepsilon_b]$。如果 $a_i(t)$ 在 $[\varepsilon_a,\varepsilon_b]$ 区间外即数据偏差过大判断为异常数据。

$$\begin{cases}\varepsilon_a=Q_1-1.5\mathrm{IQR}\\ \varepsilon_b=Q_3+1.5\mathrm{IQR}\end{cases} \tag{1}$$

式中:Q_1 和 Q_3 分别为 $M-1$ 个数据中下四分位和上四分位值,在计算分位时采用向下取整策略来确定 Q_1 和 Q_3 的值。其中 $\mathrm{IQR}=Q_3-Q_1$。通过历史数据对簇内各节点进行区间划分,以该区间作为当前时刻数据异常的判断依据。

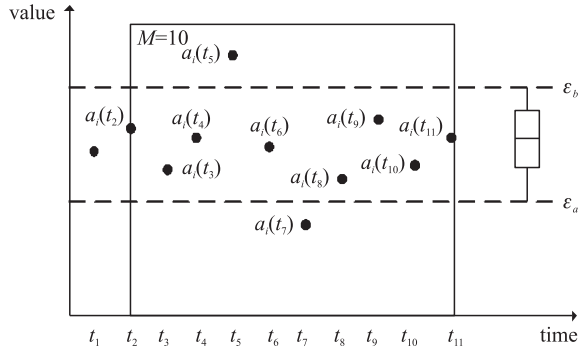


图 2 基于箱型模型的数据异常判断

监测事件的发生主要表现为局部性数据变化,而事件规模大小与数据变化节点个数成正相关。因此,数据异常占比 θ 可定义为数据异常节点数与簇内总结点输之比。

$$\theta=\frac{N}{N_{\mathrm{CH}}} \tag{2}$$

式中:N 为当前时刻簇首基于式(1)统计出该簇内数据异常节点数,N_{CH} 为该簇内成员节点总数。由于算法基于网络异常规模的大小为采集依据,并且监测事件的发生具有小概率性和局域性,为了研究方便本文取 $\bar{\theta}=0.25$ 为规模阈值。在实际应用中,可根据监测系统的性能来调整 $\bar{\theta}$ 取值。依据 θ 值的不同,数据采集规则如下:①当 $0<\theta<\bar{\theta}$,小部分异常值出现,可能由节点异常引起,采用基于信任模型的采集方式;②当 $\theta\geqslant\bar{\theta}$,多数节点出现数据异常,可能由事件发生引起,启动紧急数据采集机制。

2.2 基于信任模型的节点筛选

对于少数节点出现数据异常有可能是节点故障导致的,但也不排除由事件发生引起的数据异常。为此,对于出现数据异常的节点要从节点和数据两方面进行考虑,通过节点信任度[20]和数据偏移量的计算,为可靠性数据采集方案提供理论依据。

2.2.1 节点信任度计算

节点的通信质量是数据可靠性重要保障,节点级信任度可利用簇内节点通信行为和数据相关性进行计算。基于文献[10]和[13]所利用的 Bayes 信任管理框架同时对 beta 分布进行拟合,利用节点中历史交互记录计算节点可信度。通过已知条件概率密度参数表达式和先验概率,结合贝叶斯公式可以为后验事件提供决策。则节点 i 和节点 j 信誉分布 $\mathrm{reputation}_{ij}$ 可表示为:

$$\mathrm{reputation}_{ij}\sim\mathrm{Beta}(\alpha+1,\beta+1) \tag{3}$$

式中:α 和 β 分别表示节点 i 和节点 j 历史交互成功和失败次数。节点交互历史及邻节点的相似程度作为节点故障的主要依据,由贝叶斯评估方法可得节点 i 关于节点 j 概率密度分布函数为:

$$f(\varphi_{ij}|\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\varphi_{ij}^{\alpha-1}(1-\varphi_{ij})^{\beta-1} \tag{4}$$

式中:φ_{ij} 为交互成功的概率,且 $\alpha>0$,$\beta>0$,则对于簇首节点 j 和异常节点 i,在成功交互 α_{ij} 次 和失败交互 β_{ij} 次 时,簇首对异常节点 i 的可信度可表示为:

$$D_i=E[\mathrm{Beta}(\alpha,\beta)]=E[f(\varphi_{ij}|\alpha,\beta)]=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \tag{5}$$

2.2.2 数据偏移度计算

在节点可信度计算的基础上,引入数据偏移度来提高采集模型准确性。数据偏移度是指节点当前监测的数据同历史数据以及邻节点数据的偏差程度,通过异常节点历史数据和邻节点数据进行计算。对于异常节点 i 的数据偏移度的计算过程是:选取同簇通信半径内 k 个邻居节点,设 k 个邻节点当前采集数据为 $a_{i1},a_{i2},\cdots,a_{ik}$,则邻节点数据均值为:

$$E_k=\frac{1}{k}\sum_{j=1}^{k}a_{ij} \tag{6}$$

同时对于异常节点 i 在窗口内取当前时刻前 $M-1$ 个历史数据,历史均值为 E_i,则异常节点 i 的数据偏移度为:

$$T_i=\omega|a_i-E_i|+(1-\omega)|a_i-E_k| \tag{7}$$

式中:a_i 为异常节点 i 当前采集的数据,ω 为平衡系数且 $\omega\in[0,1]$,ω 的大小决定了历史数据和邻节点数据的权重。

2.2.3　异常数据节点综合信任度计算

对于数据异常节点的判断要综合考虑节点本身的质量和数据偏移程度,式(5)和式(7)分别给出了节点质量和数据偏差的定义。节点信任度越高且与周围节点数据偏差越小,该数据异常节点可靠性就越高。异常节点 i 的综合信任度 Trust_i 可表示为:

$$\mathrm{Trust}_i=\varphi D_i+(1-\varphi)\left|1-\frac{T_i}{a_i}\right| \tag{8}$$

式中:φ 为平衡系数且 $\varphi\in[0,1]$,而节点信任度是一个逐渐积累的过程,所以在更新当前时刻信任度时需要考虑前一时刻节点信任度值,即当前信任值 $\mathrm{Trust}_i^{\mathrm{Now}}=\kappa\mathrm{Trust}_i+(1-\kappa)\mathrm{Trust}_i^{\mathrm{Befor}}$,其中 κ 为平衡系数,$\mathrm{Trust}_i^{\mathrm{Befor}}$ 为前一时刻节点信任度。当异常节点 i 的综合信任度 $\mathrm{Trust}_i^{\mathrm{Now}}$ 大于阈值 λ 时,采信该节点数据,启动紧急数据传输机制;当小于阈值 λ 时,数据可信度较低,过滤该节点数据。

2.3　紧急数据可靠传输机制

目前,对于数据可靠传输机制的研究主要从拥塞控制和可靠性保障两方面入手。突发事件会引起数据激增,而簇首缓存空间有限,大量数据的涌入会造成队列溢出,导致数据包传输时延和丢包率急剧增加。因此,针对紧急情况下突增数据流,需要充分利用整个网络资源来确保紧急数据的可靠性传输。另外,分簇结构下各簇首在数据传输过程中存在着的链路竞争和数据冲突也关系着紧急数据可靠性传输问题。

基于以上突发事件数据流特点,提出一种冗余协助传输机制(Redundant Assistance Mechanism,RAM)。RAM 充分利用处于正常状态下的簇首资源,基于紧急数据优先的路由思想,该方式保证了紧急事件的准确感知和及时预警。具体 RAM 工作流程如下:

Step 1　簇首检测到异常节点信任度高或异常节点超过规模阈值时,立即启动紧急数据传输机制;

Step 2　簇首节点采用多链路传输策略,向其下游发送紧急请求,请求信息包含该簇位置信息;

Step 3　下游簇首节点接到请求消息后,降低自身簇内数据采集频率和减少其他簇首数据转发,并提高请求簇首数据转发优先级来确保紧急簇首数据传输;

Step 4　异常数据采集完毕,各簇首恢复正常采集机制。

RAM 通过提高紧急簇首优先级并降低下游簇首采集频率来满足紧急数据传输需要,如图 3 所示。RAM 机制虽然牺牲了部分层次的数据采集,但可以最大程度地保障网络对突发事件的及时上报和处理。实际上突发事件的频率较低,该机制的设置对网络整体性能的影响并不大。

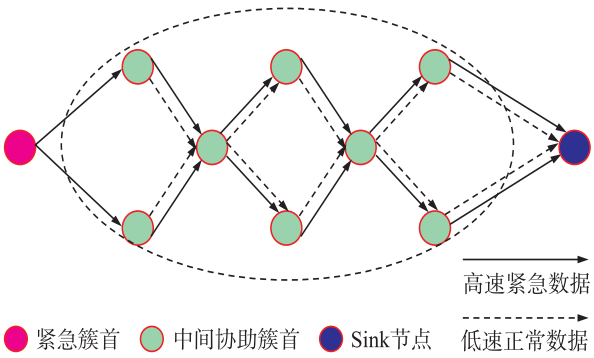


图 3　紧急数据传输机制

2.4　数据采集方法

无线传感器网络最为重要的是当监测事件发生,如森林火灾、瓦斯泄漏等而引起的数据流异常时,传感器节点要能够准确感知、快速传达到汇聚节点。因此,为了保证监测事件发生时,监测数据能够及时可靠传输和收集,可采用差异化的数据收集策略。

无线传感监测网络中“异常数据”的出现可能是由节点故障产生的错误数据,也可能是事件发生引起数据突变。由于传感网的监测数据大部分都是重要程度较低的冗余数据,这些数据之间的差异较小,“异常数据”主要表现为少数节点出现数据异常,而事件发生引起的极富价值的“异常数据”表现为多数节点的数据异常。通过异常数据占比阈值的划分来判断“异常数据”类型,对前一种数据异常采用基于信任模型的采集方式,对后一种数据异常启动紧急数据采集方案。

因此,对于正常的普通数据采用常规的数据传输方式,对于异常数据,根据异常数据占比情况,采用过滤方式或紧急传输策略。异常数据占比低于设定的阈值,采用基于信任度模型的过滤机制,异常数据占比超过设定的阈值的异常数据,采用紧急数据传输策略,数据采集方案如图 4 所示。

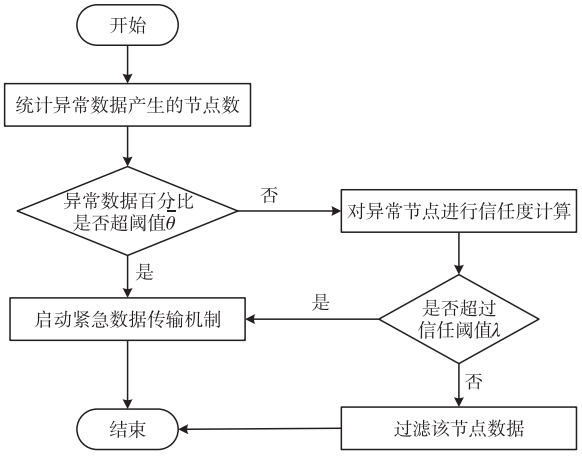


图 4 数据采集方案

3 仿真与性能分析

为了验证 AT-DG 算法数据采集的准确性和及时性,本文使用 MATLAB 作为仿真工具验证算法相关性能。在 100×100 矩形区域随机分布传感器节点,基于 HEED 协议对网络进行层次划分。相关仿真实验参数配置如表 1 所示。

表 1 仿真实验参数

参数	数值
路由协议	HEED
网络大小	100×100
初始能量	0.2 J
簇半径 r	20 m
初始信任度	0.5
异常节点比	5%、10%、15%、20%
节点数量	150
簇首比例	0.1

3.1 信任模型性能分析

基于信任度的数据异常类型的判断是 AT-DG 算法的基础,本文的信任度模型基于节点交互和数据偏移两个维度进行建模,利用信任度区分数据异常节点正常与否。因此,是否能够有效检测出非正常节点是衡量该模型的重要指标。结合本文以数据异常为导向的信任评估,算法的检测率定义为检测出的异常节点占总异常节点的比例。为了验证信任模型的有效性,实验中设置 150 个传感器节点,依据 HEED 协议对网络进行层次划分,在不同的异常节点占比下对本文算法和经典信任模型 RFSN[21](Reputation based framework for sensor networks)的检测率进行对比,结果如图 5 所示。随着网络中异常节点比例增加,AT-DG 和 RFSN 检测率均呈现下降趋势,但 AT-DG 算法以数据和节点质量为依据,平均检测率比 RFSN 算法高出 9.14 左右%。

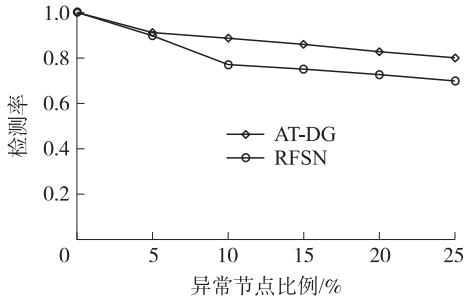


图 5 检测率对比

此外,选取在异常节点占比 15%时随机选取一个簇,检测该簇内正常节点和异常节点信任度均值变化趋势。实验过程中异常节点随机分布在网络中,正常节点可准确上报环境中的数据,簇内所有节点属性相同并设初始信任度为 0.5。实验选取前 50 个采样周期该簇内节点信任度均值变化,如图 6 所示。其中,前 15 次采样中,由于正常节点和异常节点报告数据差值较大,信任度区分效果不明显;随着采样次数的增加,异常节点不良行为造成可信度降低,进而导致异常节点信任度均值逐渐下降,而正常节点始终表现良好。由此说明,基于信任模型可以较好的区分异常数据节点的类型,为数据可靠性采集提供决策支撑。

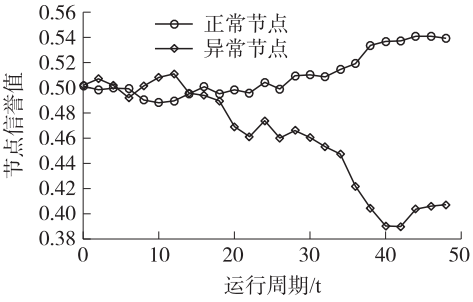


图 6 节点信任度对比

3.2 网络性能分析

为了验证 AT-DG 算法数据采集性能,在数据采集准确率和网络能耗与原生 HEED 算法进行试验对比。图 7 是数据采集准确率对比,试验时随机选取一个簇模拟事件发生,对正常节点和异常节点数据包进行标记,统计 Sink 节点接收到正常节点数据

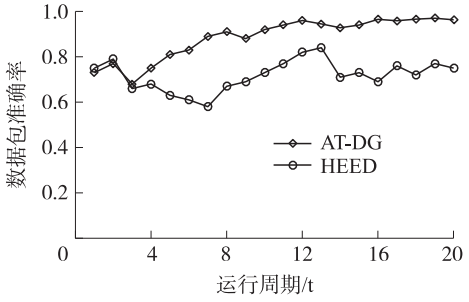


图 7 数据包接收准确率对比

量占总数据量的百分比作为试验结果。试验对比前 20 次采用结果进行对比,HEED 协议数据包准确率受异常节点影响平均准确率为 71.75%左右。而 AT-DG 算法加入异常数据检测机制,对异常节点数据包进行过滤,随着仿真轮次的增加,平均准确率维持在 91.73%左右,较原生 HEED 协议平均数据采集准确率高 20%左右。

图 8 是 AT-DG 算法节点总能耗变化曲线。从图 8 可以看出在相同的轮转周期内,AT-DG 总能耗小于原生 HEED 算法。其中,HEED 协议在 2 200 轮次时网络总能耗已经达到最值(节点全部死亡),而 AT-DG 算法下网络生命持续到 3 200 轮次。此外,AT-DG 引入紧急数据传输机制,避免了因突发事件引起大规模数据传输,均衡网络负载,节点出现死亡现象较 HEED 协议迟 200 轮次左右。以上表明 AT-DG 能量利用率更高,网络寿命更长。

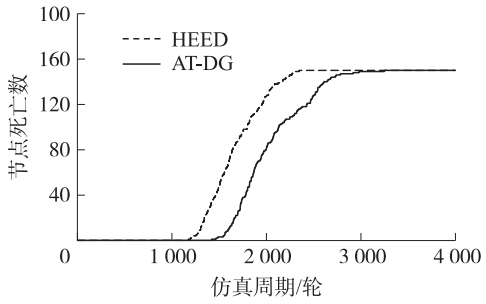


图 8　网络总能耗对比

4　结束语

为了解决因数据异常造成的决策误判问题,本文基于分簇的无线传感器网络拓扑结构,结合事件监测特点,以异常数据为出发点设计了 AT-DG 数据可靠性收集算法。通过建立异常数据节点的信任度模型,计算异常数据节点的信任度,对节点异常类型进行判断,进而采取相应的数据采集机制。仿真结果表明 AT-DG 算法在事件监测中能够精准、及时对数据进行处理,该算法可广泛用于层次型无线传感器网络数据的采集当中以提高监测数据采集的可靠性。

参考文献:

[1] 徐平平,刘吴,褚宏云,等. 无线传感器网络[M]. 北京:电子工业出版社 2013:15-28.

[2] 李春若,邹子贤. 面向无人机协助的 WSNs 的数据收集策略[J]. 传感技术学报,2021,34(1):124-128.

[3] 陈辉,张春雨. 一种基于卡尔曼滤波的分簇 WSNs 拥塞检测与控制方案[J]. 传感技术学报,2020,33(4):579-585.

[4] Rashid M M, Gondal I, Kamruzzaman J. Mining Associated Patterns from Wireless Sensor Networks[J]. Computers, IEEE Transactions on,2015,64(7):1998-2011.

[5] Mahmood M A,Seah W K,Welch I. Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead[J]. Computer Networks,2015,79(14):166-187.

[6] 周国辉,靳书坤,张伟,等. 基于证据推理规则的无线传感器网络数据可靠性分析[J]. 传感技术学报,2020,33(11):1644-1654.

[7] 朱晓娟,陆阳,邱述威,等. 无线传感器网络数据传输可靠性研究综述[J]. 计算机科学,2013,40(9):1-7,15.

[8] Wang Chen,Lin Hong Zhi,Jiang Hong Bo. Trajectory-Based Multi-Dimensional Outlier Detection in Wireless Sensor Networks Using Hidden Markov Models[J]. Wireless Networks, 2014, 20(8): 2409-2418.

[9] Wazid M,Das A K. An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless SensorNetworks[J]. Wireless Personal Communications,2016,90(4):1971-2000.

[10] 魏琴芳,袁岳义,胡向东. 基于骨干节点安全角色层级化的 WSN 安全模型[J]. 重庆邮电大学学报(自然科学版),2019,31(5):722-728.

[11] Ishmanov F,Malik A S,Kim S W,et al. Trust Management System in Wireless Sensor Networks: Design Considerations and Research Challenges[J]. Transaction on Emerging Telecommunication Technologies,2015,26(2):107-130.

[12] 赵治国,谭敏生,夏石莹,等. 基于时间因素的无线传感网络信任模型[J]. 计算机工程与设计,2017,38(4):883-887.

[13] 周治平,邵楠楠. 基于贝叶斯的改进 WSNs 信任评估模型[J]. 传感技术学报,2016,29(6):927-933.

[14] Ouyang Yan,Zeng Zhiwen,Li Xiong,et al. A Verifiable Trust Evaluation Mechanism for Ultra-Reliable Applications in 5G and Beyond Networks[J]. Computer Standards & Interfaces, 2021, 77: 103519-103534.

[15] Huang S,Liu A,Zhang S,et al. BD-VTE: A Novel Baseline Data Based Verifiable Trust Evaluation Scheme for Smart Network Systems[J]. IEEE Transactions on Network Science and Engineering, 2020,99:1-18.

[16] 应可珍,周贤年,毛科技,等. 一种改进区域生长法的 WSN 数据采集算法研究[J]. 小型微型计算机系统,2019(3):567-572.

[17] 王泉,张纳温,张金成,等. 压缩感知在无线传感器网络数据采集中的应用[J]. 传感技术学报,2014,27(11):1562-1567.

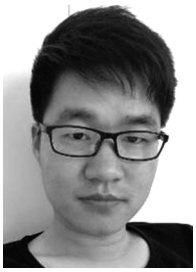
[18] 万叶晶,叶继华,江爱文. 一种基于时空相关性和异常检测的改进 WSN 节能策略[J]. 传感技术学报,2017,30(8):1267-1273.

[19] 谭德坤,付雪峰,赵嘉,等. 基于异常数据驱动的 WSN 簇内数据融合方法[J]. 传感技术学报,2017,30(2):306-312.

[20] 苏耀鑫. 基于信任度的 WSN 信任模型研究[J]. 电光与控制,2018,25(3):32-36.

[21] Saurabh Ganeriwal, Laura K Balzano, Mani B Srivastava. Reputation-Based Framework for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks(TOSN),2008,4(3): 15-20.

陈　辉(1973—),男,博士,副教授,硕士生导师,主要研究方向为无线传感器网络,煤矿安全监控与通信等,1115858010@qq.com;



张春雨(1993—),男,硕士研究生,主要研究方向为无线传感器网络。