doi: 10.12068/j.issn.1005-3026.2019.06.006

基于信任模型的 WSNs 安全数据融合算法

叶正旺[1,2], 温 涛[1,3], 刘振宇[1,3], 付崇国[1,3]
(1. 东北大学 计算机科学与工程学院, 辽宁 沈阳 110169; 2. 通化师范学院, 吉林 通化 134002;
3. 大连东软信息学院, 辽宁 大连 116023)

摘 要: 为了抵御无线传感器网络内部的恶意攻击行为和故障节点的误操作行为对数据融合结果的影响,提出一种基于信任模型的多层不均匀分簇无线传感器网络安全数据融合算法. 该算法基于多层不均匀的分簇网络拓扑实现安全数据融合能够有效均衡网络中节点的能耗. 通过节点间的通信行为和数据相关性建立信任评估模型,并引入动态的信任整合机制和更新机制,实现簇内和簇间的信任评估,选择可信融合节点并将可信节点所收集的数据进行基于信任值加权的数据融合. 仿真实验表明,该算法能够实现精确的信任评估,有效识别内部恶意攻击节点,得到的数据融合结果具有较高的精确度,实现了安全的数据融合.

关 键 词: 安全;数据融合;信任模型;无线传感器网络;恶意节点
中图分类号: TP 393 **文献标志码**: A **文章编号**: 1005-3026(2019)06-0789-06

An Algorithm of Trust-based Secure Data Aggregation for Wireless Sensor Networks

YE Zheng-wang[1,2], *WEN Tao*[1,3], *LIU Zhen-yu*[1,3], *FU Chong-guo*[1,3]
(1. School of Computer Science & Engineering, Northeastern University, Shenyang 110169, China; 2. Tonghua Normal University, Tonghua 134002, China; 3. Dalian Neusoft University of Information, Dalian 116023, China. Corresponding author: YE Zheng-wang, E-mail: yezhengwang@neusoft.edu.cn)

Abstract: To resist the influence of the malicious attacks and the malfunctions of fault nodes in wireless sensor networks (WSNs) on data aggregation, this paper proposes an algorithm of trust-based secure data aggregation for WSNs. The algorithm is based on multi-layer non-uniform clustering network topology to achieve secure data aggregation, which can effectively balance the network energy consumption. The trust evaluation model is established based on the communication behavior and data correlation among the nodes. The dynamic trust integration mechanism and update mechanism are introduced to realize the trust evaluation intra-cluster and inter-cluster. Based on the trust value, a trusted aggregation node is chosen in the cluster to complete data fusion of trusted nodes. Simulation results show that the algorithm can achieve accurate and effective trust evaluation, identify internal malicious nodes, and obtain the data aggregation results with high accuracy.

Key words: security; data aggregation; trust model; wireless sensor network; malicious node

随着无线通信、微电子技术的发展,无线传感器网络得到了快速发展并被应用于很多行业进行数据收集和监测[1]. 但由于传感器网络是受限的,数据融合技术成为无线传感器网络的主要研究方向之一,因为数据融合技术[2-3]可以去除网络中产生的大量冗余数据,减少冗余数据传输和通信开销,延长网络生命周期. 但很多数据融合算法中假定网络内部传感器节点是安全的,即所有的节点都没有被妥协,都是可信任的,但现实中无线传感器节点常常被部署在开放环境下工作,极易被俘获、破坏、攻击或者发生故障,导致错误的数据注入、数据篡改或者产生错误的数据. 错误的

收稿日期: 2017-11-15
基金项目: 国家自然科学基金资助项目(61772101,61170169,61602075); 吉林省教育厅科学研究资助项目(JJKH20180861KJ).
作者简介: 叶正旺(1982-),男,辽宁朝阳人,东北大学博士研究生; 温 涛(1962-),男,辽宁大连人,东北大学教授,博士生导师.

数据就有可能导致判定错误,进而造成不可挽回的损失,尤其是在一些对数据精确度比较敏感的应用中,如医疗和战区监控等. 因此,建立安全可靠的数据融合算法非常有必要[4].

目前,国内外对无线传感器网络安全数据融合的相关研究大多数采用身份认证、加密、入侵检测等方法,但仅仅依靠认证、加密等方法的安全数据融合算法并不能完全保障数据融合的安全. 这是因为一旦网络中的合法节点被俘获,这些安全机制就没有任何意义[5]. 另外,传统的加密、认证机制也不能处理节点故障导致的异常数据. 针对被妥协的内部恶意节点和故障节点,现已被证明比较有效的防御措施是基于信任模型的安全方法[6-7]. 文献[8]首次提出了基于信任管理模型的安全数据融合算法(RDAT),RDAT 通过功能性评估实现节点之间的信任评价,可以发现网内的恶意节点,实现安全的数据融合. 但该算法中仅考虑节点间的信任评价,没有考虑能耗、链路对安全的影响. 文献[9]在 RDAT 算法基础上提出了能够实现节点能效性和链路可靠性的、基于混合型信任管理模型的安全数据融合算法(iRTEDA),该算法不仅通过信任模型进行了节点间的信任评估,还增加了节点的能量和路由链路可用性的考虑. 因此,iRTEDA 算法能够及时、有效地识别俘获节点,并实现融合数据安全、可靠的传输. 文献[10]在 iRTEDA 算法基础上提出了一种基于节点间关系强度的信任评估方法实现安全数据融合,在 iRTEDA 算法信任模型的基础上增加了二手信息的评价来实现信任评估,获得的融合数据更加精确,确保融合数据的安全. 但以上三种基于信任管理模型的安全数据融合算法,只是实现简单的内部恶意妥协节点的识别,而没有考虑针对信任模型的策略性内部恶意攻击行为.

本文提出了一种基于信任模型的安全数据融合算法(algorithm of trust-based secure data aggregation,ATSDA). 首先,建立多层不均匀的分簇拓扑结构,在每个簇中实现簇头节点与融合节点分开管理的方式实现数据融合,有效均衡网络中节点的能量消耗. 其次,通过节点间通信行为和数据相关性来完成节点间的信任评估,有效抵御网络中的各种恶意节点攻击. 第三,建立簇内安全数据融合和簇间安全数据判断机制. 通过簇内信任评估有效过滤掉簇内恶意节点和异常节点,对簇内可信节点所收集的数据进行加权数据融合. 通过簇间信任评估实现簇头节点间的信任评估,进行恶意簇头节点的识别,有效抵制簇内共谋节点对簇头节点的影响. 实验仿真表明,本文提出的安全数据融合算法能够准确评估节点间的可信性,识别网络中各种内部恶意攻击节点和异常节点,有效保障网络数据融合结果的安全性.

1 假设与网络模型

假设具有相同属性的传感器节点随机部署在一个二维空间中,每个节点都分配一个唯一的标识. 本文的能量消耗模型和网络结构采用与先前研究成果[11]相同的方法,节点发送 k 比特数据到距离 d 的接收器消耗的能量 E_t 表示为

$$E_t = \begin{cases} (E_{elec} + d^2 E_{amp1})k, & d < d_0; \\ (E_{elec} + d^4 E_{amp2})k, & d \geqslant d_0. \end{cases} \tag{1}$$

其中,E_{elec}表示发射或接受每比特数据电路损耗的能量. 若传输距离小于阈值 d_0,功率放大损耗采用自由空间模型;当传输距离大于等于阈值 d_0 时,采用多路径衰减模型. E_{amp1} 和 E_{amp2} 分别代表自由空间模型和多径衰减模型中功率放大的能量损耗.

节点接收 k 比特数据时消耗的能量表示为

$$E_r = kE_{elec}. \tag{2}$$

将网络划分为多层不均匀分簇拓扑结构,根据每个节点与 Sink 节点的距离,将网络节点划分为不同的层,根据能量模型式(1)中的通信半径 d_0,将网络划分为 L 层. 设 $\mathrm{dist}(s,i)$ 是节点 i 到基站 Sink 的距离. 则节点 i 所在的层 L_i 可以表示为

$$L_i = \left\lfloor 2 \times \frac{\mathrm{dist}(s,i)}{d_0} \right\rfloor. \tag{3}$$

$L = \max(L_i)$, $i = 1, 2, \cdots$. 通过式(3)对网络中的节点进行分层处理,簇头节点选择和建簇采用与文献[11]相同的方法,不同的是本文算法在簇中增加了专门用于进行数据融合的融合节点,因此节点被分为普通节点、簇头节点和融合节点. 具体的网络拓扑结构如图 1 所示,其中 r 代表层半径,$r = d_0/2$. 每个节点保存一个邻居节点的列表,存储 ID,通信信息和信任关系等.

2 基于信任模型的安全数据融合

为了抵御来自网络内部的恶意攻击行为对数据融合结果的影响,建立信任模型实现对恶意节点识别,并将可信节点的数据进行安全数据融合.

2.1 信任模型

2.1.1 直接信任计算

直接信任是节点 i 对节点 j 通过直接交互行

为给出的直接信任评估，本文运用简化的 Beta 信任模型对直接信任值进行计算. 直接信任评估模型采用先前研究工作[12]的模型，表示为

$$\mathrm{TD}_{ij}(t)=\frac{\alpha+1}{\alpha+\beta+2}\left(1-\frac{\beta}{W}\right)\left(1-\frac{1}{\alpha+\delta}\right). \quad (4)$$

其中：α 和 β 分别表示节点 i 与节点 j 在 t 时间内成功交互总数与不成功交互总数；$(1-F/W)$ 是惩罚函数，W 表示节点之间具有影响力的总通信次数；$(1-1/(S+\delta))$ 是调节函数，并不是一个线性函数，δ 是一个正常数，用来调节接近于 1 的速度. 节点之间的直接信任评估不仅考虑节点之间的通信行为，还对节点所采集的数据进行异常评估，建立本地异常数据过滤机制. 只有通信行为正常并且数据误差在允许范围内才被定义为成功交互，否则为不成功交互. 网络中收集的数据都具有空间相关性，本地异常数据过滤采用文献[13]中的方法进行异常数据发现：通过定义本地允许异常阈值 $\lambda_i(t)$ 进行异常数据过滤，通过本地邻接点与该节点收集数据的差值是否在允许误差阈值范围内进行异常数据判断. 如果 $|x_j(t)-x_i(t)|<\lambda_i(t)$，则为正常节点；否则为不正常节点. 每个节点的本地允许误差阈值表示为

$$\lambda_i(t)=\frac{1}{|N_i|}\sum_{j\in N_i}\left|x_j(t)-\frac{x_i(t)+\sum_{j\in N_i}x_j(t)}{|N_i|+1}\right|. \quad (5)$$

其中：N_i 代表节点 i 的邻居集合；$|N_i|$ 表示节点 i 邻居节点的个数.

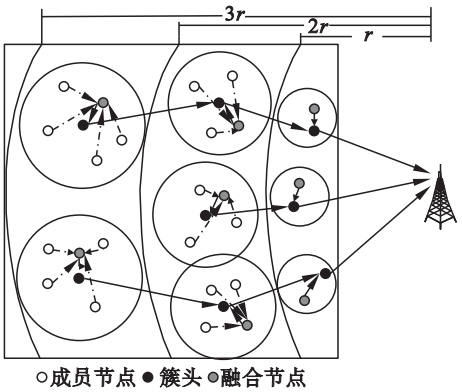

图 1　多层不均匀分簇网络拓扑结构

Fig. 1　Multi-layer non-uniform clustering topology

2.1.2　间接信任计算

间接信任是由第三方对评估节点行为做出的评价，但第三方节点（共同邻居节点）也存在不确定性，因此需要对第三方节点进行判断. 假设节点 i 和节点 j 共拥有 k 个共同邻居节点，且节点 i 对 k 个共同邻居节点的直接信任评估分别为 T_{i1}，$T_{i2},\cdots,T_{i(k-1)},T_{ik}$. 如果 $T_{ik}\geqslant\theta$（θ 为判断阈值且 $\theta=0.5$），则节点 k 被选为推荐信任节点，否则该节点被忽略.

为了避免推荐节点的诋毁攻击，按照可信推荐节点的信任值进行权重分配，推荐节点 N_n 的信任权重 $\bar{\omega}_n$ 计算公式如下：

$$\bar{\omega}_n=\frac{T_{in}}{\sum_{n=1}^{k_1}T_{in}},\ n=1,2,\cdots,k_1. \quad (6)$$

其中：T_{in} 代表节点 i 对 N_n 的直接信任；k_1 表示可信推荐节点的个数. $0\leqslant\bar{\omega}_n\leqslant1$，$\sum_{n=1}^{k_1}\bar{\omega}_n=1$. T_{nj} 代表共同邻居节点 N_n 对节点 j 的直接信任，$\bar{\omega}_n$ 是 T_{nj} 的信任权重. 由于信任具有传递性，所以间接信任 $\mathrm{TI}_{ij}(t)$ 计算公式为

$$\mathrm{TI}_{ij}(t)=\sum_{n=1}^{k_1}\bar{\omega}_nT_{in}T_{nj}. \quad (7)$$

2.1.3　信任的整合

通过直接信任与间接信任得到节点 i 对节点 j 在时间 t 的综合信任 $T_{ij}(t)$ 表示为

$$T_{ij}(t)=\varphi\mathrm{TD}_{ij}(t)+(1-\varphi)\mathrm{TI}_{ij}(t). \quad (8)$$

φ 为直接信任的权衡因子并且满足 $\varphi\in[0,1]$，定义为

$$\varphi=\frac{1}{2}+\frac{1}{\pi}\arctan\left(10\times\frac{k-\mathrm{COM}_{\mathrm{th}}}{N}\right). \quad (9)$$

其中：N 代表节点间交互的最大交互次数；$\mathrm{COM}_{\mathrm{th}}$ 代表节点间交互次数阈值，当交互次数高于阈值 $\mathrm{COM}_{\mathrm{th}}$ 时，直接信任积累更多的信任评估，则整合信任更依赖直接信任，因此 φ 随之变大. 否则，邻居节点之间的直接通信交互作用太小，难以判断被评估节点的好坏，而整合的信任值更依赖于间接信任值. 通过建立动态权重分配方法，φ 随着交互次数 k 的变化而动态变化，可以动态调整直接信任和间接信任的重要性.

2.1.4　信任更新机制

信任的评估需要历史记录的积累，为了精确实现信任评估需对节点信任进行信任更新，本文建立一种基于滑动时间窗口的诱导有序加权因子的更新机制以提高信任的灵活性和动态性. 该更新信任机制可以动态地调整参数和交互式历史窗口数来动态调整权重序列，完成信任值的动态更新. 使该信任模型能够适应不同的网络环境和安全要求.

经文献[14]论证，诱导有序加权平均因子适用于基于交互时间的信任序列. 通过最大离散度[15]计算各个窗口的权值，权重计算公式如下：

$$w_m^* = \frac{((m-1)\alpha - m)w_1^* + 1}{(m-1)\alpha + 1 - mw_1^*}. \quad (10)$$

其中:m 代表滑动窗口数量,α 为可调因子. 由式(10)可知分类权重系数向量的计算主要由两个参数确定:参数 α 和交互历史证据数目 m. 根据文献[14]可知,当 $\alpha \in [0.5,1]$ 时,权重系数的分布满足时间衰减的特性,α 的取值反映了信任模型对以往交互经历的遗忘程度,α 越大,历史经验就越容易被遗忘,因此可以通过动态调节 α 来满足不同需求的信任模型对历史经验的依赖程度. 参数 m 反映了信任值依赖历史经验窗口的个数,历史窗口数量越多对于节点间的信任评价越好,当然也就越浪费资源,消耗更多的能量. 因此,通过调节 m 和 α 可以得到不同的权重组合,来满足网络环境的变化和现实需求. 综合考虑网络中的能量消耗和安全需求,本文取适中的两个值进行实验,定义 $\alpha = 0.7, m = 4$.

2.2 簇内安全数据融合

簇内安全数据融合主要是通过簇内信任评价实现簇内异常节点和恶意节点的过滤并完成簇内可信节点的数据融合. 具体的实现过程如图 2 所示.

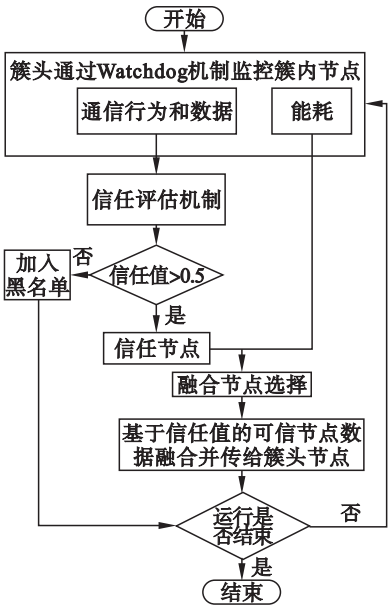

图 2 簇内安全数据融合实现过程

Fig. 2 Process of secure data aggregation within a cluster

2.2.1 簇内可信安全数据融合节点的选择

通过簇内信任评估建立簇头节点与每个节点的信任关系列表,并通过定义信任阈值 θ_1 对簇内节点进行信任评判,建立可信融合节点序列. 具体实现:

Input: 某时段簇头节点 CH 对簇中节点信任评价结果 $TD_{H,i}$,信任阈值 θ_1

Output:可信融合节点序列 ADDSensorList[i]

```
if TD_{H,i} ≥ θ1
    add(ADDSensorList[i]);
else
    add(BlackList[i]);
end
```

2.2.2 簇内可信融合节点的数据融合

簇内可信融合节点的数据融合是通过可信融合节点对可信簇内节点采集的数据进行数据融合,根据簇中可信融合节点序列 ADDSensorList[i]选择剩余能量高且高可信的节点作为融合节点. 簇头节点和融合节点进行交互,将本周期内的信任节点列表 ADDSensorList[i]发送给融合节点,融合节点根据本周期内可信节点的信任值分配可信节点的融合权重,进行加权数据融合.

可信节点的信任权重分配原则为:信任值越大,数据融合权重越大,反之亦然. 可信节点的融合权重表示如下:

$$WT_i = \frac{TD_{H,i}}{\sum_{i=1}^{n} TD_{H,i}}, \sum_{i=1}^{n} WT_i = 1. \quad (11)$$

其中:WT_i 表示簇中可信节点 i 的融合权重;n 表示簇中可信节点的个数.

融合节点对簇内可信节点的数据融合表示为

$$D_{agg}(t) = \sum_{i=1}^{n} WT_i \overline{D_i}. \quad (12)$$

其中:$D_{agg}(t)$ 表示本周期簇内安全数据融合的结果;WT_i 代表簇内节点 i 的信任融合权重;$\overline{D_i}$ 代表周期内融合节点 i 多轮采集数据的平均值.

2.3 簇间安全数据判断

簇间安全数据判断是通过监测簇头节点之间的通信行为和数据,实现簇头节点间的信任评估,得到簇间信任评价表. 通过簇头节点之间的信任评价对簇头节点进行信任判断,有效识别出妥协的恶意簇头节点,保障数据融合的精确性.

根据簇间的信任评价结果对簇头节点进行异常检测,当簇头节点的信任值大于 θ_2 时,该簇头节点属于可信的,将收集的数据发送至基站;否则,该簇头节点标记为可疑的簇头节点,θ_2 为异常检测信任阈值. 对于可疑的簇头节点进行标记并重新选择簇头节点. 通过可信的簇头节点建立跨层簇头节点之间的多跳路由,实现安全、可靠的数据传输.

Input: 某时段 CH(i)对 CH(j)的信任值 $T_{i,j}(t)$,信任阈值 θ_2

Output：不可信簇头节点集合 BlackList_CH[i]
　if $T_{i,j}(t) \geqslant \theta_2$
　　Translate to BS；
　else
　　add(BlackList_CH[i])；
　end

3　仿真与性能分析

将 200 个节点随机部署在 200 m × 200 m 的区域对本算法进行仿真实验. 为了验证本文安全数据融合算法具有安全、精确的数据融合能力，设计不同的实验环境，将本文的算法和经典的基于信任模型的安全数据融合算法 iRTEDA 在信任值、融合结果精确度、能耗方面进行对比分析. 实验中所有节点的初始信任值和信任阈值都与 iRTEDA 算法相同，取值为 0.5.

3.1　信任评估分析

分别对正常节点和恶意节点进行信任评估并与 iRTEDA 算法进行对比分析. 假设正常节点在通信过程中始终以正常的通信行为和数据进行交互，恶意节点表现为丢弃全部数据包. 正常节点和恶意节点的信任评估结果与 iRTEDA 算法评估结果对比如图 3 所示. 由图 3 可知，随着运行周期的增加，ATSDA 算法和 iRTEDA 算法中的正常节点的信任值逐渐增加并最终达到一个稳定的值，

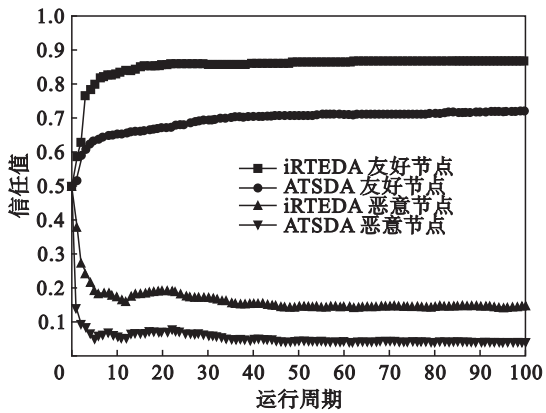

图 3　正常节点与恶意节点信任值对比
Fig. 3　Comparison of trust values of normal nodes and malicious nodes

恶意节点的信任值随之下降并最终达到一个较小的值. 但本文 ATSDA 算法正常节点的信任值始终低于 iRTEDA 算法的信任值，这是因为调节函数对信任关系的影响，有效避免短时间内信任的迅速提升. 对恶意节点的信任评价中，随着恶意行为数量的增加，ATSDA 算法的信任值明显低于 iRTEDA 算法，这是因为惩罚函数对恶意节点信任值惩罚，实现了信任值的急剧下降，使恶意节点的信任值更小，能够更直接反映节点的恶意行为. 因此，本文所提算法的信任模型对恶意节点的恶意行为评估得到较小的信任值，能够更快更精确识别出恶意节点.

当恶意节点为 On – Off 策略性攻击节点时，信任值对比如图 4 所示. On – Off 攻击采用正常行为和恶意行为交替出现来隐藏自己的身份(本文假设周期为 30). 由图 4 可以看出，在前 30 个运行周期，恶意节点表现为正常行为，ATSDA 算法和 iRTEDA 算法的信任值都随着运行周期的增加而提升，节点都具有较高的信任值. 在 30 个周期后，恶意节点表现为攻击行为，ATSDA 算法和 iRTEDA 算法的信任值在 31 周期时开始下降，但 ATSDA 算法的信任值更低，通过信任阈值可以将恶意节点识别. 因此，ATSDA 算法能够识别策略性攻击.

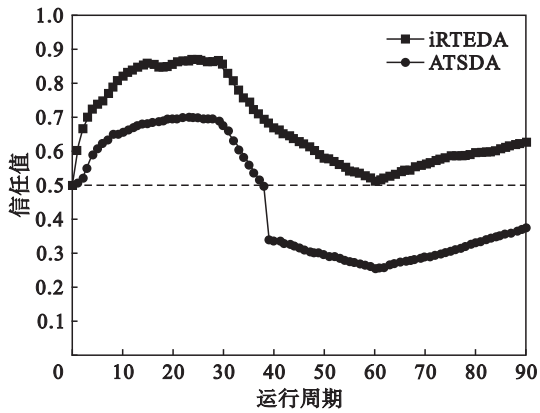

图 4　On – Off 攻击的信任值对比
Fig. 4　Comparison of trust values under On-Off attack

3.2　数据融合结果分析

为了验证安全数据融合算法的有效性，在数据篡改攻击、灰洞攻击、On – Off 攻击和诽谤攻击 4 种恶意节点共存的情况下，且每一种攻击所占比例为 25%，所有恶意节点所占比例为 30%，将 ATSDA 算法的数据融合的精确度与经典算法进行了对比. 得到的结果如表 1 所示，其中精确度定义为：[1 – 相对误差]. 通过表 1 可以看出，本文提出的 ATSDA 算法的数据融合精度更高.

表 1　融合结果精确度对比
Table 1　Comparison of aggregation accuracy

信任模型	RDAT[8]	iRTEDA[9]	改进[10]	ATSDA
精确度/%	80	83	91.1	95

3.3　能耗分析

由于无线传感器网络的受限性，在进行算法

设计时,一定要考虑能耗问题. 本文通过建立多层不均匀分簇拓扑结构,可以有效均衡网络中节点的能量消耗,有效延长网络的生命周期.

在数据篡改攻击、灰洞攻击、On – Off 攻击和诽谤攻击 4 种恶意节点共存,且每一种攻击所占比例为 25% ,所有恶意节点所占比例为 30% 的情况下,将 ATSDA 算法和 iRTEDA 算法的能量消耗率进行对比,结果如图 5 所示. 由图 5 可以看出,ATSDA 算法的能耗消耗率要高于 iRTEDA. 这是因为在 ATSDA 算法中需要进行簇内和簇间的信任评价,产生了额外的能耗. 但是,本文 ATSDA 算法的能量消耗率虽然比 iRTEDA 算法高,但与 iRTEDA 的运行周期和能量消耗率相比,并没有造成网络因能耗过大导致提前瘫痪. 因此,在不影响网络应用的前提下牺牲一定的网络能耗,该安全融合算法得到的信任评估结果和数据融合结果的精确性更高,具有较好的安全性.

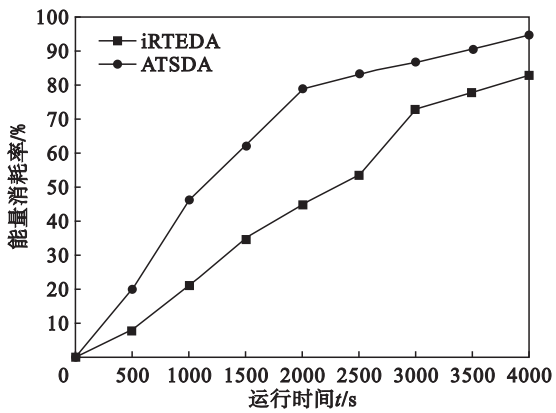

图 5 能量消耗率对比

Fig. 5 Comparison of the energy consumption

4 结 语

本文提出了一种基于信任模型的无线传感器网络安全数据融合算法,该算法通过监控节点之间的通信行为以及数据相关性实现节点之间的动态信任评估. 通过该信任模型进行簇内和簇间信任评估,将网络中的异常数据和恶意节点进行标记并剔除,并将可信节点收集的数据根据信任值进行加权融合. 实验结果表明,本文的安全数据融合算法能够准确评估节点的可信性,识别网络中的内部恶意节点和异常节点,有效保障数据收集的安全性.

参考文献:

[1] Gungor V C, Hancke G P. Industrial wireless sensor networks: challenges, design principles, and technical approaches[J]. *IEEE Transactions on Industrial Electronics*, 2009,56(10):4258 – 4265.

[2] Akkaya K, Demirbas M, Aygun R S. The impact of data aggregation on the performance of wireless sensor networks [J]. *Wireless Communications & Mobile Computing*, 2008, 8(2):171 – 193.

[3] Rajagopalan R, Varshney P K. Data-aggregation techniques in sensor networks: a survey[J]. *IEEE Communications Surveys & Tutorials*, 2006, 8(4):48 – 63.

[4] Ozdemir S, Xiao Y. Secure data aggregation in wireless sensor networks: a comprehensive overview [J]. *Computer Networks*, 2009, 53(12):2022 – 2037.

[5] Momani M, Challa S. Survey of trust models in different network domains [J]. *International Journal of Ad Hoc, Sensor and Ubiquitous Computing*, 2010, 1(3):1 – 19.

[6] 张仕斌,方杰,宋家麒. 一种面向 WSNs 的可信数据融合算法研究[J]. 小型微型计算机系统,2014,35(10):2347 – 2352.
(Zhang Shi-bin, Fang Jie, Song Jia-qi. Study on an algorithm of trusted data fusion oriented on WSNs [J]. *Journal of Chinese Computer Systems*, 2014, 35(10):2347 – 2352.)

[7] 杨黎斌,慕德俊,蔡晓妍. 无线传感器网络入侵检测研究[J]. 计算机应用研究,2008,25(11):3204 – 3208.
(Yang Li-bin, Mu De-jun, Cai Xiao-yan. Study on intrusion detection for wireless sensor network [J]. *Application Research of Computers*, 2008, 25(11):3204 – 3208.)

[8] Ozdemir S. Functional reputation based reliable data aggregation and transmission for wireless sensor networks [J]. *Computer Communications*, 2008, 31(17): 3941 – 3953.

[9] Liu C X, Liu Y, Zhang Z J. Improved reliable trust-based and energy-efficient data aggregation for wireless sensor networks [J]. *International Journal of Distributed Sensor Networks*, 2013, 9(5):1 – 11.

[10] Liu Y, Liu C X, Zeng Q A. Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks [J]. *Telecommunication Systems*, 2016, 62(2):319 – 325.

[11] Ye Z W, Wen T, Liu Z Y, et al. A security fault-tolerant routing for multi-layer non-uniform clustered WSNs [J]. *EURASIP Journal on Wireless Communications & Networking*, 2016, 2016(192):1 – 12.

[12] 叶正旺,温涛,刘振宇,等. 基于节点行为动态变化的 WSNs 信任模型[J]. 控制与决策,2017,32(4):715 – 720.
(Ye Zheng-wang, Wen Tao, Liu Zhen-yu, et al. Trust model based on dynamic change of node behavior for WSNs[J]. *Control and Decision*, 2017, 32(4):715 – 720.)

[13] Mi S, Han H, Chen C, et al. A secure scheme for distributed consensus estimation against data falsification in heterogeneous wireless sensor networks[J]. *Sensors*, 2016, 16(2):1 – 17.

[14] Li X Y, Gui X L. Cognitive model of dynamic trust forecasting[J]. *Journal of Software*, 2010, 21(1): 163 – 176.

[15] Fullér R, Majlender P. An analytic approach for obtaining maximal entropy OWA operator weights[J]. *Fuzzy Sets and Systems*, 2001, 124(1):53 – 57.