

基于信任和权重的无线传感器网络数据融合模型

张 峰 郑洪源 丁秋林

(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 在无线传感器网络中,数据融合的可靠性是一个非常重要的问题并且受到了广泛的关注。为此,提出一种基于信任和权重的无线传感器网络数据融合模型(TWDFM)。在该模型中,传感器节点通过构建信任表选举可靠簇头,簇头根据权重检测异常节点并融合可信数据。仿真实验表明,该模型可以有效提高数据融合的安全性和准确性。

关键词 无线传感器网络,信任,权重,数据融合

中图分类号 TP393

文献标识码 A

DOI 10.11896/j.issn.1002-137X.2017.05.007

Trust and Weight Based Data Fusion Model in Wireless Sensor Networks

ZHANG Feng ZHENG Hong-yuan DING Qiu-lin

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract In wireless sensor networks, the reliability of data fusion is a very important issue. It has been widely concerned. Thus, a trust and weight based data fusion model (TWDFM) was proposed in this paper. In this model, sensor nodes elect reliable cluster head by building trust tables, and cluster head detects abnormal nodes according to the weights and fuses the credible data. The results of simulation show that this model can effectively improve the safety and accuracy of data fusion.

Keywords Wireless sensor network, Trust, Weight, Data fusion

1 引言

无线传感器网络(WSNs)由大量的传感器节点构成,每个节点采集周围环境的信息,然后将数据传送到基站。如今,无线传感器网络已逐步被应用于军事侦查、农业监测等领域,但是传感器节点有限的电源供应、计算能力、存储资源和通讯带宽制约了无线传感器网络的应用和发展。

与传统无线网络不同,无线传感器网络的能耗问题^[1-2]必须予以考虑。传感器节点会产生大量的冗余数据,而传输这些数据将耗费大量的能量。研究发现,计算能耗要比传输能耗少得多^[19],因此将数据融合后再进行传输可以节省能量。数据融合技术就是通过对原始数据的采集、传输、综合、过滤、相关及合成来消除冗余数据,减少数据传输量,从而减少能量消耗。本文针对数据融合技术的采集、传输环节进行了深入研究,从而提出了基于信任和权重的数据融合模型。

另一个需要考虑的问题即数据的可靠性问题^[3-4]。通常,在数据融合算法中数据都是默认可靠的。然而,传感器节点因受到各种外界因素的影响(如环境突变、恶意攻击^[5]等)可能会产生不可靠的数据。加密技术^[6]可以用来解决这个问题,但是又不足以保护网络安全。因此,本文引入了信任和权重机制来弥补它的缺陷,以提供更加安全可靠的数据。

针对上述问题,国内外学者做了大量的研究和实践。Izadi等人^[7]设计了一种基于模糊的数据融合方法,即传感器

节点采集数据并通过模糊逻辑控制器计算置信因子,再根据置信因子区分真实值并传送到簇头,簇头利用模糊逻辑进行多传感器数据融合,减少了数据传输和数据冗余,从而降低了能量损耗,延长了网络生命周期。Heinzelman等人^[8]提出了低功耗自适应集簇分层(LEACH)协议,其基本思想是以循环方式随机选取簇头,并将能量负载平均分配到每个传感器节点,以达到减少能量损耗的目的;然而,LEACH默认所有节点都是安全可靠的,并没有考虑受损节点或恶意节点成为簇头的情况。Zhou等人^[9]提出了基于传感器节点自主行为的信任评估模型,传感器节点通过监听邻居节点的行为取得直接或间接的信任值,簇头再根据D-S证据理论计算得到综合信任值,通过信任评估可以有效地识别恶意节点,避免恶意节点成为簇头。Crosby等人^[10]设计了一种分布式的基于信任的簇头选举机制,通过监听邻居节点的传输过程构建信任表,计算信任度,然后根据信任度选举可靠簇头,保证了数据融合的可靠性和网络安全。Fu和Liu^[12]构造了一个双簇头数据融合模型,在该模型中每个簇根据信誉系统选举两个簇头,它们各自进行数据融合并将结果传输到基站,基站根据融合结果计算相异系数,如果相异系数超出阈值,则将簇头加入黑名单并重新选举簇头,进而消除受损节点,避免受损节点成为簇头。但是,仅仅保证簇头的可靠性是不够的,还需保证融合数据是可信任的。Atakli等人^[11]在分层网络结构的基础上提出了一种加权信任评估策略,其通过比较传感器节点采集

到稿日期:2016-03-12 返修日期:2016-08-12 本文受江苏省产学研联合创新资金项目(SBY201320423)资助。

张 峰(1991—),男,硕士生,主要研究方向为信息系统及集成、信息安全等,E-mail:zfwork@sina.com;郑洪源(1973—),男,博士,副教授,主要研究方向为信息系统、知识工程;丁秋林(1936—),男,博士,教授,博士生导师,主要研究方向为信息系统、企业信息化。

的数据和最终的数据融合结果不断更新加权信任值,并将该值用于检测异常节点和筛选可信数据,具有良好的性能和可扩展性。

本文结合加权信任评估,在改进基于信任的双簇头选举模型^[12]的基础上,提出了基于信任和权重的无线传感器网络数据融合模型(Trust and Weight based Data Fusion Model, TWDFM)。在该模型中,簇内选举可靠簇头,簇头融合可信数据,保证了数据融合的可靠性和网络的安全性。

2 假设

(1)无线传感器网络由大量的廉价传感器节点构成,由于质量较差,电源供应和计算存储能力有限,传感器节点极易遭受攻击或损坏。因为受损节点通常以堵塞、丢包、伪造信息等方式攻击网络,所以防止受损节点成为簇头可以有效保护网络安全。异常节点则是指受到外界因素影响产生错误数据或异常信息的节点。

(2)无线传感器网络采用多层分级结构(见图 1)。所有传感器节点处于第一层,它们被划分成簇,每个簇都有一个簇头,用于管理整个簇;簇内节点可以相互通信,包括簇头。无线传感器网络中的所有簇头构成了第二层,它们不仅可以相互通信,而且可以将信息传输到基站。第三层是基站,用于接收和处理整个无线传感器网络的信息,一般是安全可靠的。

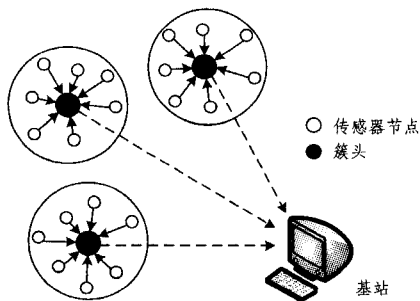


图1 WSN拓扑

(3)簇内每个节点都有可能被选举为簇头,并具有数据融合的能力。每个节点有唯一的ID,该ID唯一标识该节点。

(4)所有的传感器节点都共享一个全双工的无线信道并在混合模式下工作,比如节点A发送一个消息经过节点B到节点C,节点A在发送之后即可监听节点B转发消息到节点C。每个节点都拥有3种密钥:主密钥、簇密钥和对偶密钥。无线传感器网络中的所有节点共享一个主密钥,可以接收来自基站的广播消息。每一个簇共享一个簇密钥,不同簇的簇密钥各不相同。簇密钥支持基站到簇的多播,也支持簇间通讯。对偶密钥则用于簇内节点间的通讯。本文注重对传输机制的研究,对于密钥分布不再赘述。

(5)簇内通讯是同步的,且采用时分复用(TDM)调度。簇头根据簇内节点的数量为每个节点分配向其传输数据的时隙,簇内每个节点只能在分配到的时隙内进行数据通讯。时分复用调度防止了簇内消息的碰撞,但同时也限制了簇内节点的数量。

3 TWDFM 设计

3.1 框架概述

如图2所示,整个TWDFM框架由两大模块构成:节点

模块和簇头模块。节点模块包括4个子模块:分簇、簇头选举、信任表的构建与更新、权重的初始化与更新。簇头模块包括3个子模块:加权异常节点检测、可信数据融合、融合结果的上传与反馈。

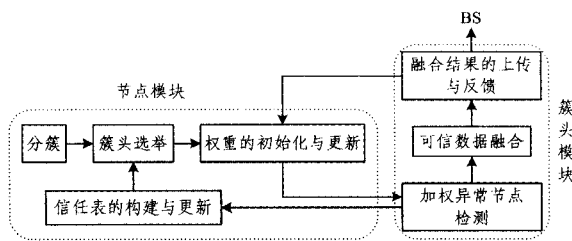


图2 TWDFM框架

每个模块都有其独特的功能,它们相互作用,构成了有机的整体。在节点模块中,所有传感器节点经过分簇后都会被赋予一个初始权重。每个传感器节点通过监听邻居节点的传输过程建立信任表。当簇头选举发起时,传感器节点根据内置的信任表选举可靠簇头。在簇头模块中,簇头收集簇内每个节点的权重,划分可信节点和异常节点,并在簇内广播黑名单(异常节点信息)。簇内节点重置异常节点的信任度和权重,同时簇头选择可信节点的数据进行融合,然后将融合结果分别发往基站和簇内节点。基站综合所有融合结果并做出决策,而簇内节点将存储数据与融合结果进行比较,然后根据比较结果更新权重。

下文将对比两大模块做详细介绍。

3.2 节点模块

3.2.1 分簇

无线传感器节点部署完毕之后,通过分簇算法将无线传感器网络分成单个簇,每个簇随机产生一个簇头。由于在短时间内,刚部署的传感器节点不可能被攻击或者受损,因此所选簇头一般是安全可靠的。簇头根据每个簇内节点的剩余电量为其分配一个权重 w ,并存储在相应节点中。然后传感器节点开始采集周围环境的信息,并进行计算和存储。

3.2.2 信任表的构建与更新

一切准备就绪后,簇头开启时分复用(TDM)调度并通知每个簇内节点。每个传感器节点只能在其调度时隙内进行数据传输,其余时间允许它们监听簇内邻居节点的传输过程。通过这种被动监听,在每个节点和邻居节点间建立信任关系。它们可以轻易地探测到邻居节点是否不断地丢包或者存在异常行为。每个传感器节点不断地记录和存储其邻居节点的行为来维持信任表。

考虑到距离、能耗等问题,监听对象仅限于邻居节点,而非簇内所有节点,所以很有必要给出邻居节点的概念。如图3所示,当节点A开始将采集到的数据传输到簇头时,簇内其他节点即可监听它的传输过程。每个节点的传输过程都可以被其广播范围内的其他节点监听到,所以本文把邻居节点定义为传输节点广播范围内的所有节点。例如,节点A的广播范围就是以节点A为圆心的圆,节点B和节点C在节点A的广播范围内,所以它们是节点A的邻居节点,可以监听到节点A的传输过程。同理,节点C不在节点B的广播范围内,所以节点C不能监听到节点B的传输过程。

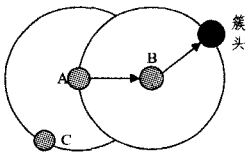


图 3 节点到簇头的传输

信任指对其他人未来某个行为的主观期望。类似地,在无线传感器网络中,通过直接或者间接地观察某个节点过去的行为,将信任度作为某个节点可靠性的预测。每个节点通过监听邻居节点的传输过程来计算得到信任度并存储。

传感器节点可以通过接收应答得知数据是否发送成功,而它的邻居节点也可以监听到此应答。邻居节点还可以通过监听转发过程的应答判断消息是否被修改。通常,应答可以提供下列信息:数据包被弃置、数据内容被修改、地址被修改^[10]。由于信任表中的信任参数必须是可度量的,因此把应答提供的信息作为信任参数来建立信任表,如表 1 所列。

表 1 信任表

节点	X_0	...	X_n
数据包接收 R_N			
数据包转发 F_N			
数据包修改 DM_N			
数据包地址修改 AM_N			
信任度 $T_N(X_i)$			

节点 X_i 的信任度用 $T_N(X_i)$ 来表示,计算公式如下:

$$T_N(X_i) = w_1 d_1 + w_2 d_2 + w_3 d_3 + \gamma \tag{1}$$

其中, w_1, w_2, w_3 表示权重,根据当前网络设定; γ 是预设的常量,等于当前网络中的平均丢包率; d_1, d_2, d_3 则与信任参数相关,由式(2)计算得到:

$$d_1 = \frac{F_N(X_i)}{R_N(X_i)}, d_2 = 1 - \frac{DM_N(X_i)}{F_N(X_i)}, d_3 = 1 - \frac{AM_N(X_i)}{F_N(X_i)} \tag{2}$$

3.2.3 簇头选举

当 1) 簇头的剩余能量低于某一阈值 e 或者 2) 簇头的服务时间超出某一阈值 t 时,重新选举簇头,能量阈值 e 和时间阈值 t 都可以预先设置。在新簇头选举过程中,簇头、候选节点、普通节点都各自发挥着不同的作用,具体簇头选举过程如下。

1. if 簇头剩余能量 $\leq e$ or 簇头服务时间 $\geq t$
2. 簇头在簇内广播一个重新选举簇头的消息
3. 统计候选节点的得票数
4. if 票数相同
5. 随机选择一个候选节点
6. else
7. 选择票数最高的节点作为候选节点
8. end
9. 簇头发送确认消息给候选节点
10. if 候选节点剩余能量 $\geq e$ and 权重 $w \geq \theta$
11. 选择该候选节点为簇头
12. else
13. 回到步骤 2
14. end

当满足上述两种情况之一时,簇头会在簇内广播一个重新选举簇头的消息,所有节点开始给新簇头投票。簇头记录投票,选择两个票数最高的节点作为候选节点,然后簇头发送确认消息给候选节点,若候选节点都具备成为簇头的条件,则票数高者作为新簇头,票数低者作为备用簇头;否则,将失效节点加入黑名单,重复选举过程,最后将选举结果和黑名单在簇内广播。

候选节点收到簇头的确认消息时,必须发送一个应答给簇头。如果候选节点剩余能量超过阈值 e 并且权重 w 大于 θ (将会在 3.3.1 节对权重 w 和权重阈值 θ 做具体介绍),则发送一个确认应答,否则发送一个失效应答,过程如下。

1. if 剩余能量 $\geq e$ and 权重 $w > \theta$
2. 发送一个确认应答到簇头
3. else
4. 发送一个失效应答到簇头

选择两个节点作为候选簇头节点,若簇头选举成功,则将副簇头作为备用簇头。一般情况下,备用簇头和普通节点无区别,当簇头发生故障时,备用簇头则会代替簇头执行相关任务。此外,在某个时间点,备用簇头可能不再具备成为簇头的条件,因此备用簇头必须定期地发送状态消息给簇头。当备用簇头失效时,簇头会广播一个重新选举备用簇头的消息,所有节点投票选举新的备用簇头,选举过程与簇头选举过程类似。

普通节点接收到重新选举簇头的消息时,选择信任表中信任度最高的两个节点作为候选节点,加上簇密钥后发送给簇头。普通节点接收到黑名单消息时,在信任表中将黑名单上的节点的信任度置为 -1,使其不可能被选举成为簇头。

3.2.4 权重的初始化与更新

无线传感器网络分簇以后,簇头为每个簇内节点分配一个初始权重 w ,一般情况下,每个节点的初始权重相等。

权重是加权异常节点检测和可信数据融合的基础,具体应用将在 3.3.1 节介绍。

当数据融合完成以后,簇头在簇内广播融合结果,每个节点将存储数据和融合结果进行比较,过程如下。

1. 计算存储数据和融合结果的偏差 ϵ
2. if $\epsilon > \sigma$
3. 采集信息不准确,权重降低: $w = w \times \alpha$
4. else
5. 采集信息准确,权重不变

引入一个偏差阈值 σ ,用于控制融合数据的准确程度。由于采集的数据各式各样,可能是 true 或 false,也可能是小数或整数,因此引入误差是必要的。

若采集信息不准确,则将该节点的权重降低, α 的定义如下:

$$\alpha = 1 - e^{-\frac{m-s}{k}} \tag{3}$$

其中, m 是融合过程中的异常节点个数, s 是簇内节点个数, k 是控制变化速率的参数。图 4 是 α 函数的变化曲线,假设 s 为 20, k 为 4。当簇内异常节点较少时, α 变化较慢,权重下降缓慢,对数据融合影响不大;当簇内异常节点较多时, α 变化较快,权重下降迅速,导致无法继续进行数据融合,保证了数据融合的安全性和准确性。

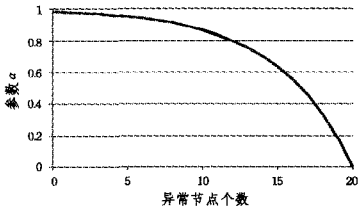


图 4 α 函数

3.3 簇头模块

3.3.1 加权异常节点检测

在簇头发起数据融合前,需先进行异常节点检测。由 3.2.4 节可知,用权重 w 来衡量传感器节点采集信息的准确程度,权重越大,准确性越高,所以设定一个权重阈值 θ 来区分可信节点和异常节点,过程如下。

- 1. 簇头收集簇内每个节点的权重 w_i
- 2. if 节点的权重 $w_i < \theta$
- 3. 此节点为异常节点,加入黑名单
- 4. else
- 5. 此节点为可信节点,进行数据融合

当簇内所有节点区分完毕后,簇头将黑名单在簇内进行广播,异常节点将自己的权重置为 0,其他节点将其信任度置为-1。之所以其他节点将异常节点的信任度置为-1,是因为当该节点出现异常时,则认定它不能再作为簇头进行数据融合。

3.3.2 可信数据融合

在检测出异常节点的同时,筛选出了可信数据。有理由相信,簇头在融合可信数据之后,得到的结果将更可靠且更接近实际情况。

本文采用卡尔曼滤波法^[15-16]来融合数据。卡尔曼滤波法是一种利用线性系统状态方程,通过系统的观测数据对系统状态进行最优估计的算法。首先,假设一个系统模型:

系统状态方程: $X(k) = AX(k-1) + W(k)$ (4)

传感器观测方程: $Z(k) = HX(k) + V(k)$ (5)

其中, $X(k)$ 是 k 时刻的系统状态, A 是系统的状态转移矩阵; $Z(k)$ 是 k 时刻的观测值, H 是观测矩阵; $W(k)$ 和 $V(k)$ 分别表示系统过程和观测的高斯白噪声,它们的协方差矩阵分别为 Q 和 R 。

在上述系统模型中,利用卡尔曼滤波器即可得到系统状态的最优估计值,即融合数据。下面用 5 个公式来对卡尔曼滤波器进行描述:

$X(k|k-1) = AX(k-1|k-1)$ (6)

$X(k|k-1)$ 是根据上一状态得到的估计值, $X(k-1|k-1)$ 是上一状态的最优估计值。

$P(k|k-1) = AP(k-1|k-1)A' + Q$ (7)

$P(k|k-1)$ 是 $X(k|k-1)$ 对应的协方差矩阵, $P(k-1|k-1)$ 是 $X(k-1|k-1)$ 对应的协方差矩阵, A' 是 A 的转置矩阵, Q 是系统过程的协方差矩阵。

通过式(6)和式(7)得到系统状态的估计值后,再由传感器节点采集系统状态的观测值。结合估计值和观测值,可以得到下一状态 k 的最优估计值 $X(k|k)$:

$X(k|k) = X(k|k-1) + K_g(k)(Z(k) - HX(k|k-1))$ (8)

其中, K_g 为卡尔曼增益:

$K_g(k) = \frac{P(k|k-1)H'}{HP(k|k-1)H' + R}$ (9)

为了使卡尔曼滤波器不断地递推下去直到系统过程结束,必须更新 k 状态下 $X(k|k)$ 的协方差矩阵:

$P(k|k) = (I - K_g(k)H)P(k|k-1)$ (10)

其中, I 为 1 的矩阵,当系统进入 $k+1$ 状态时, $P(k|k)$ 就是式(7)的 $P(k-1|k-1)$ 。

将卡尔曼滤波法应用到无线传感器网络中,通过卡尔曼滤波器即可将可信数据进行融合,从而得到可靠的融合结果。

3.3.3 融合结果的上传与反馈

数据融合完成之后,簇头将融合结果分别上传到基站并在簇内广播。基站将所有簇头上传的融合结果进行综合,做出决策;而簇内节点则将存储数据和融合结果进行比较,然后根据比较结果更新权重。

4 仿真

本文采用 OPNET^[17-18] 进行模型仿真实验。为了分析 TWDFM 的性能,将 200 个无线传感器节点随机部署在 500m×200m 的场景中,每个节点的最大传输距离为 70m,初始能量为 0.2J。MAC 层采用基于 TDMA 的简单协议,数据传输速率为 1Mb/s。每个节点每秒产生一个数据包,且数据包长度为 32Byte。簇头节点的能量阈值 e 设为 0.05J,时间阈值 t 设为 1000s。每个节点的权重 w 初始化为 1,权重阈值 θ 设为 0.2。此外,场景还设置了一个结果收集节点,用于收集仿真过程中的性能参数。

如上所述,本文利用信任机制来区分受损节点和可靠节点,尽可能选举可靠节点成为簇头,从而使数据融合更加安全可靠。实验以丢包率作为参考,用于区分受损节点和可靠节点,将受损节点的丢包率设为 40%,可靠节点的丢包率设为 1%。受损节点具备伪造信息的能力,即选举簇头时,受损节点会随机选择一个节点进行投票,而不是根据信任度来选择。

此外,本文还利用权重机制来区分异常节点和可信节点。由假设(1)可知,异常节点会产生错误数据或异常信息,从而影响数据融合结果。特别要说明,现实中受损节点很可能是异常节点,因为受损节点可以伪造信息,但是两者又不能完全等同,可靠节点也可能在传输过程中出现数据异常的情况。所以出于严谨,本文根据传感器节点产生数据的准确性再予以细分。实验假设每个传感器节点都能探测温度,采集的温度值服从高斯分布,异常节点和可信节点的度量模型如表 2 所列。异常节点的均值高于可信节点的均值,并且波动更大,可以起到影响融合结果的作用,异常节点数量越多,效果则越明显。

表 2 可信节点和异常节点的比较

节点类型	度量模型	均值	标准差
可信节点	高斯分布	真实值	2
异常节点	高斯分布	真实值 * 1.2	3

4.1 安全可靠分析

本文通过分析受损节点被选举为簇头的概率,来说明数据融合的可靠性。

将信任机制和双簇头选举机制^[12] 进行比较,如图 5 所示。当簇头选举不采用任何机制时,受损节点被选举为簇头的概率随受损节点比例的增长而线性增长。当受损节点比例低于 20% 时,两种机制表现得都非常好。当比例大于 60% 且小于 75% 时,所提信任机制表现得稍好。由于受到权重机制的影响,异常节点会被视为受损节点并加入黑名单,从而使无线传感器网络更加安全可靠。但是,当受损节点比例达到 75% 时,概率就急剧增加。原因在于,当受损节点所占比例较

大时,过多的错误投票导致无法保证选举出可靠簇头,信任机制失去了作用。当然,大多数情况下受损节点所占比例较小,所以信任机制有着不错的效果。

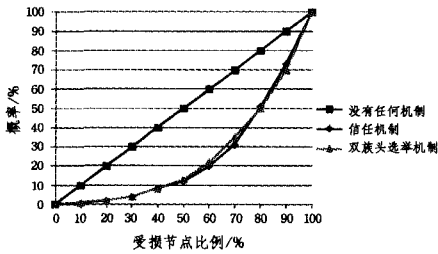


图 5 受损节点成为簇头的概率

4.2 准确性分析

本文通过比较是否使用 TWDFM 产生的融合结果,来说明该模型对数据融合的准确性的影响。

如上所述,可信节点和异常节点的度量模型服从高斯分布。假设环境温度为 20℃,两种节点的概率密度函数如图 6 所示。可以发现,可信节点的均值为 20;而异常节点的均值为 24,且分布相对分散。显然,异常节点的存在会使融合结果产生偏差,比例越大,偏差就越大。

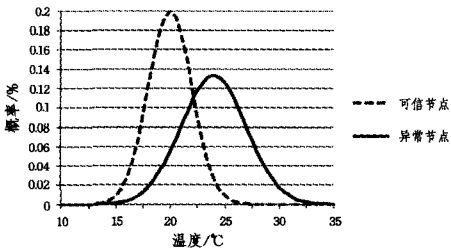


图 6 传感器节点度量模型

假定异常节点的比例为 30%,通过分析数据融合结果随时间的变化曲线(见图 7),来说明 TWDFM 对数据融合结果的准确性的影响。

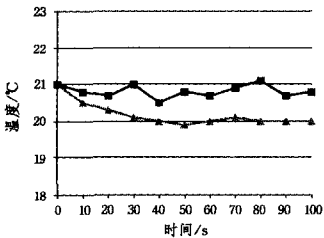


图 7 融合结果变化曲线

如图 7 所示,当不使用 TWDFM 时,融合结果和真实值总是存在偏差,并且偏差是不确定的,原因在于融合结果受到了异常节点的影响。然而,当使用 TWDFM 时,虽然在开始阶段由于受到异常节点的影响,融合结果也高于真实值,但是融合结果很快就逼近真实值,且趋于稳定。这是因为权重机制发挥了至关重要的作用,随着时间的推移和融合结果的更新,有异常节点被不断地加入黑名单,因而融合结果就越来越接近真实值。

4.3 能耗分析

如图 8 所示,将 TWDFM 和双簇头选举模型^[12]进行比较。可知,双簇头选举模型的能耗总是高于 TWDFM。这是

因为,在双簇头选举模型中,每个簇内总是有两个簇头各自进行数据融合,增加了数据传输,消耗了更多的能量。然而,不论是 TWDFM,还是双簇头选举模型,为了提高数据融合的安全性和准确性,都增加了计算存储和数据传输,所以它们的总能耗都高于不使用任何模型的情况。特别要说明,实验中研究的模型都是构建在分簇路由协议上的,虽然 TWDFM 增加了多余的数据传输(主要是控制消息和应答),但是相比于传感器节点采集的数据而言,在总体上还是减少了数据冗余和数据传输量。

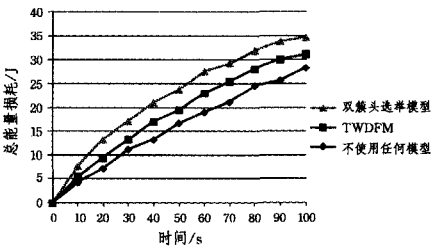


图 8 网络总能量损耗

结束语 本文提出了一种基于信任和权重的无线传感器网络数据融合模型,通过信任机制选举可靠簇头,权重机制检测异常节点并融合可信数据,旨在提高数据融合的安全性和准确性。仿真实验表明,该模型可以有效提高数据融合的可靠性。然而,文中并没有考虑能量损耗的问题,为了保证数据融合的安全可靠性,增加了许多数据传输,带来了多余的能量损耗。未来工作将在如何平衡能量损耗与安全可靠性之间进行,以尽可能降低能量损耗并实现高效的性能。

参 考 文 献

[1] ISHMANOV F, MALIK A S, KIM S W. Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): a comprehensive overview[J]. European Transactions on Telecommunications, 2011, 22(4): 151-167.

[2] LI L, LI W J. The analysis of data fusion energy consumption in WSN[C]// System Science, Engineering Design and Manufacturing Informatization (ICSEM). Guiyang: IEEE, 2011: 310-313.

[3] KUMAR M, DUTTA K. A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks[M]. Springer India, 2015: 1-15.

[4] KUMAR V, JAIN A, BARWALP N. Wireless sensor networks security issues, challenges and solutions[J]. International Journal of Information & Computation Technology, 2014, 4(8): 859-868.

[5] BALLAV B, RANA G. A Review of Routing Attacks in MANET and WSN[C]// International Journal of Engineering Development and Research(IJEDR). 2015: 1401-1406.

[6] HAYOUNI H, HAMDI M, KIM T H. A Survey on Encryption Schemes in Wireless Sensor Networks[C]// Advanced Software Engineering and Its Applications (ASEA). Haikou: IEEE, 2014: 39-43.

[7] IZADI D, ABAWAJY J H, GHANAVATI S, et al. A Data Fusion Method in Wireless Sensor Networks[J]. Sensors, 2015, 15(2): 2964-2979.

- [2] ORAN S, EITAN A. An efficient polling MAC for wireless LANs [J]. *IEEE/ACM Transactions on Networking*, 2011, 4(9): 439-451.
- [3] MA M, ZHU Y, CHENG T H. A bandwidth guaranteed polling MAC protocol for Ethernet passive optical networks [C] // *Proc. of IEEE INFOCOM 2003*, San Francisco, IEEE, 2003: 22-31.
- [4] CAI Q, DING H W, LIU Q L, et al. An effective polling MAC scheme for wireless sensor networks [J]. *Information Technology Journal*, 2013, 12(22): 6631-6635.
- [5] JIANN C G, PEI K L, YIN S C, et al. On 5G radio access architecture and technology [J]. *IEEE Wireless Communications*, 2015, 22(5): 2-5.
- [6] XU C N, LI C, WANG Z G, et al. DLSOMAC: a MAC protocol oriented to distributed wireless link scheduling technology [J]. *Acta Automatica Sinica*, 2014, 40(12): 2747-2755. (in Chinese)
徐朝农, 李超, 王智广, 等. DLSOMAC: 一个面向分布式无线链路调度技术的 MAC 协议 [J]. *自动化学报*, 2014, 40(12): 2747-2755.
- [7] VICTOR S, MARK H, CHEN B R, et al. Simulating the power consumption of large-scale sensor network applications [C] // *Proc. of the 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, USA, ACM, 2004: 188-200.
- [8] CANO C, BELLALTA B, CISNEROS A, et al. Quantitative analysis of the hidden terminal problem in preamble sampling WSNs [J]. *Ad Hoc Networks*, 2011, 10(1): 19-36.
- [9] ZIOUVA E, ANTONAKOPOULOS T. CSMA/CA performance under high traffic conditions: throughput and delay analysis [J]. *Computer Communications*, 2002, 25(3): 313-321.
- [10] MAGISTRETTI E, GUREWITZ O, KNIGHTLY E W. 802.11ec: Collision avoidance without control messages [C] // *Proc. of Mobicom 2012*, ACM, Istanbul, Turkey, 2012: 65-76.
- [11] ZHANG X, SHIN K G. Gap sense: lightweight coordination of heterogeneous wireless devices [C] // *Proc of IEEE INFOCOM 2013*, IEEE, Turin, Italy, 2013: 3094-3101.
- [12] CHEBROLU K, DHEKNE A. Esense: communication through energy sensing [C] // *Proc. of Mobicom 2009*, IEEE, Beijing, China, 2009: 85-96.
- [13] J X Y, W J L, L M Y, et al. Hitchhike: riding control on preambles [C] // *Proc. of Infocom 2014*, IEEE, Toronto, Canada, 2014: 2499-2507.
- [14] SOUVIK S, ROMIT R C, SRIHARI N. CSMA/CN: carrier sense multiple access with collision notification [C] // *Proc. of the Mobicom 2010*, ACM, Chicago, USA, 2010: 25-36.
- [15] JAMIESON K, BALAKRISHNAN H. PPR: partial packet recovery for wireless networks [C] // *Proc of SigComm 2007*, ACM, Kyoto, Japan, 2007: 409-420.
- [16] KIM H, HOU J C. Improving protocol capacity for UDP/TCP traffic with model-based frame scheduling in IEEE802.11-operated WLANs [J]. *IEEE Journal of Selected Areas on Communications*, 2004, 22(10): 1987-2003.
- [17] CALIF, CONTI M, GREGORI E. Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit [J]. *IEEE/ACM Transactions on Networking*, 2000, 8(6): 785-799.
- [18] BONONI L, CONTI M, GREGORI E. Runtime optimization of IEEE 802.11 wireless LANs performance [J]. *IEEE Transaction on Parallel and distributed system*, 2004, 15(1): 66-80.
- [19] JAMALI A, HEMAMI S M S, BERENJKOUB M, et al. An adaptive MAC protocol for wireless LANs [J]. *Journal of Communications and Networks*, 2014, 16(3): 311-321.
- [20] DINESH B, EMILY M, SACHIN K. Full duplex radios [C] // *Proc of Sigcomm 2013*, ACM, Hong Kong, 2013: 375-386.
- [21] LINHE K, XUE L. mZig: enable multi-packet reception in ZigBee [C] // *Proc of Mobicom 2015*, ACM, Paris, 2015: 552-565.

(上接第 41 页)

- [8] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocol for wireless sensor networks [C] // *Hawaii International Conference on System Sciences*, Hawaii, IEEE, 2000: 10.
- [9] ZHOU J M, LIU F, LU Q Y. Data Fusion Based on Node Trust Evaluation in Wireless Sensor Networks [J]. *Journal of Sensors*, 2014, 68(9): 907-913.
- [10] CROSBY G V, PISSINOU N, GADZE J. A framework for trust-based cluster head election in wireless sensor networks [C] // *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Columbia, MD, IEEE, 2006: 13-22.
- [11] ATAKLI I M, HU H, CHEN Y, et al. Malicious node detection in wireless sensor networks using weighted trust evaluation [C] // *Proceedings of the 2008 Spring Simulation Multiconference*, Ottawa, Canada, 2008: 836-843.
- [12] FU J S, LIU Y. Double cluster heads model for secure and accurate data fusion in wireless sensor networks [J]. *Sensors*, 2015, 15(1): 2021-2040.
- [13] VAZIFEHDAN J, PRASAD R V, NIEMEGEREERS I. Energy-efficient reliable routing considering residual energy in wireless ad hoc networks [J]. *IEEE Transactions on Mobile Computing*, 2014, 13(2): 434-447.
- [14] ANJALI, SHIKHA, SHARMA M. Wireless sensor networks: Routing protocols and security issues [C] // *2014 5th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Hefei: IEEE Computer Society, 2014: 1-5.
- [15] LU X, WANG X, WANG H. Optimal information fusion Kalman filtering for WSNs with multiplicative noise [C] // *2012 International Conference on System Science and Engineering (IC-SSE)*, Liaoning: IEEE, 2012: 152-157.
- [16] RIBEIRO A, SCHIZAS I D, ROUMELIOTIS S, et al. Kalman filtering in wireless sensor networks [J]. *Control Systems*, IEEE, 2010, 30(2): 66-86.
- [17] KHAN T A, BEG M T, KHAN M A. Performance Analysis of WLAN using OPNET [J]. *International Journal of Innovative Technology and Exploring Engineering*, 2013, 2(5): 2278-2375.
- [18] MAO Y M, ZHANG D W, KAN F L. Simulation Research on MAC Layer Protocol Base on OPNET Modeler [J]. *Advanced Materials Research*, 2014, 945: 2349-2352.
- [19] POTTIE G J, KAISER W J. Wireless integrated network sensors [J]. *Communications of the ACM*, 2000, 43(5): 51-58.