

引用格式:黄颖,费莉,赖小龙.带有隐私保护的无线传感网能量有效数据融合机制[J].微电子学与计算机,2019,36(7):65-69. [HUANG Y,FEI L,LAI X L. Energy-efficient wireless sensor network data fusion mechanism with privacy protection method[J]. Microelectronics & Computer,2019,36(7):65-69.]

带有隐私保护的无线传感网能量有效数据融合机制

黄 颖,费 莉,赖小龙

(重庆邮电大学移通学院 通信与物联网工程学院,重庆 401520)

摘 要: 传感数据的节能传输与隐私保护对深化无线传感网的应用具有重要的意义. 提出带有隐私保护的无线传感网能量有效数据融合机制,以解决当前无线传感网数据融合机制效率较低且缺乏隐私安全保护的问题. 设计了传感数据隐私保护方法,通过在传感节点对传感数据进行加密,保障传感数据的隐私安全. 研究了能量有效的数据融合机制,基于深度学习理论,设计了有效的数据融合模型,提高传感数据融合的效率. 仿真结果表明,所提机制可有效保障传感数据的隐私安全,提高数据融合的效率,并降低节点能量消耗.

关键词: 无线传感网;能量有效;数据融合;隐私保护

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2019)07—0065—05

Energy-efficient wireless sensor network data fusion mechanism with privacy protection method

HUANG Ying,FEI Li,LAI Xiao-long

(Institute of Communication and Internet of Things Engineering, College of Chongqing University of Posts and Telecom Mobile Telecommunications, Chongqing 401520, China)

Abstract: The energy-saving transmission and privacy protection of sensor data is of great significance for deepening the applications of wireless sensor network. An energy-efficient wireless sensor network data fusion mechanism with privacy protection method is proposed to solve the problem that the current data fusion mechanism is less efficient and lacks privacy protection method. The sensor data privacy protection method is designed to protect the privacy of the sensor data by encrypting the sensor data at the sensor node. The energy-efficient data fusion mechanism is studied. Based on the deep learning theory, an efficient data fusion model is presented to improve the efficiency of sensor data fusion process. Simulation results show that the proposed mechanism can effectively guarantee the privacy of sensor data, improve the efficiency of data fusion, and reduce the energy consumptions of nodes.

Key words: wireless sensor network; energy-efficient; data fusion; privacy protection

1 引言

嵌入式技术、无线通信技术及微机电系统技术的快速发展,推动了无线传感器网络(Wireless Sensor Network, WSN)技术的进步^[1-3]. WSN 因其自组织、长寿命、部署灵活等特点,被广泛应用于环境监测、智慧医疗、智能交通、战场侦察等诸多领

域^[4-5]. WSN 以多点协作的方式,采集其部署范围内监测对象的状态信息,并对监测信息进行处理,以获取监测对象的真实物理状态. 传感节点受限于其几何尺寸与硬件集成程度,通常体积较小,计算、存储、能量资源都非常有限. 此外,在实际的 WSN 应用场景中,为实现对监测范围的全覆盖,传感节点通常都为冗余部署,使得传感数据具有较高的冗余性,将所

有原始传感数据都发送给汇聚节点将极大地消耗节点有限的能量资源^[6-7]. 并且, WSN 收集的数据有被恶意节点窃取的危险. 为了解决上述问题, 研究人员提出适用于 WSN 的安全数据融合机制, 在传感节点采集、发送数据的过程中, 采用数据融合与安全性保障技术, 降低传输数据的冗余性, 节省节点和链路资源开销, 并保障数据传输的安全^[8-10].

目前, 研究人员对 WSN 数据融合机制进行了深入研究. 文献[11]提出了一种基于神经网络的 WSN 数据融合方法, 以有效提升数据传输效率, 降低网络能耗. 文中设计了基于 Hamming 网络的 CNN-LEACH 聚类协议与基于神经网络的 SMP-SO-BP 优化算法, 并将之应用于 WSN 数据融合过程. 文献[12]提出了一种低延迟和低能耗的 WSN 数据融合算法-LDLEC, 该算法将 WSN 中的节点划分为多个不均匀的簇, 每个簇采用自底向上的方法构建拓扑结构, 从而降低数据传输的延迟和能耗. 文献[13]提出 WSN 中基于三角模块算子的多传感器数据融合算法, 使用 Dixon 方法消除原始数据中的异常数据, 并采用 OLSF 支持函数来计算每个数据集的数据. 此外, 选择合适的三角模块算子来获取最终的融合结果, 该机制的计算复杂度较低, 集成度较高. 然而, 上述三种机制都基于浅层学习模型设计数据融合方法, 去除传感数据的冗余性效果较为有限. 并且, 其缺乏对传感数据隐私安全的保护. 为此, 文献[14]提出了一种高效的隐私保护数据压缩融合机制-CS-HE, 采用同态加密函数来阻止恶意节点对传感数据的分析与追踪, 以实现传感数据的隐私保护. 但是, 该机制虽考虑了传感数据隐私性的保护, 但在数据传输过程中, 仅采用简单的数据压缩方法来部分消除传感数据的冗余性, 使得数据传输的能耗过大.

针对上述问题, 本文提出带有隐私保护的无线传感网能量有效数据融合机制 (Energy-efficient wireless sensor network data fusion mechanism with privacy protection method, EDFP).

2 网络模型

如图 1 所示, 无线传感器网络由汇聚节点、簇头节点、传感节点构成. 传感节点随机布放在监测环境中. 本文采用 LEACH^[15] 分簇协议对无线传感器网络进行分簇, 每个分簇只有一个簇头节点. 整个监测环境内只有一个汇聚节点, 汇聚节点位于监测环境的中心. 传感节点与簇头节点采用电池供电, 汇聚节

点为外部电源供电. 传感节点周期性采集其部署范围内的监测对象数据, 并对数据进行加密处理后传输给其所在分簇的簇头节点. 簇头节点收集其分簇内传感节点发送的数据, 并对数据进行融合处理后传输至汇聚节点. 汇聚节点负责将无线传感器网络采集的数据传输至外部网络.

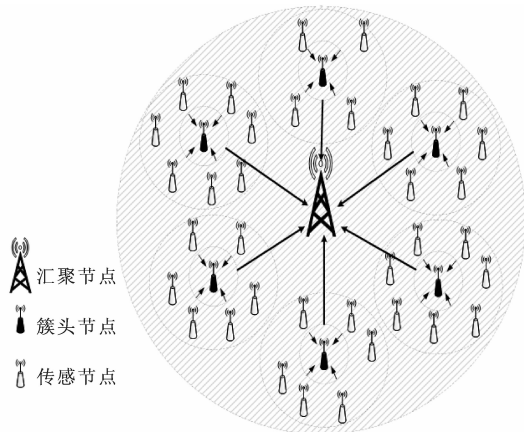


图 1 无线传感器网络模型

3 传感数据隐私保护方法

在 WSN 簇内数据传输过程中, 部分簇内传感节点的恶意行为可能会导致数据的隐私泄露, 从而为 WSN 带来极大的安全隐患. 本文首先提出了传感数据隐私保护方法, 通过对传感节点所采集的数据进行加密, 从而从源头对传感数据的隐私性以及完整性进行保护.

簇内每个传感节点生成密钥 $k_x = (k_s, k)$, 其中, k_s 为传感节点与汇聚节点之间的共享密钥, k 为全网所有传感节点共同维护的共享密钥.

汇聚节点生成 N 个互异的素数 $(q_1, q_2, \dots, q_N)$, 并以 $(q_1, q_2, \dots, q_N)$ 为因子, 生成椭圆曲线 p , 如式(1).

$$p = \prod_{i=1}^N q_i \quad (1)$$

则传感节点与汇聚节点间的共享密钥 $k_s = (q_1, q_2, \dots, q_N, m)$. 取 N 个阶数为 p 的点 $\{\epsilon_1, \epsilon_2, \dots, \epsilon_N\}$, 则全网传感节点共同维护的共享密钥 $k = (k_1, k_2, \dots, k_N)$, 其中, $k_i = p \times \epsilon_i / q_i, i \in [1, N]$.

密钥 k 由汇聚节点向 WSN 内包括簇头节点与传感节点在内的所有节点进行广播. 由于簇内每个传感节点采集的数据不同, 因此, 需根据数据编号对数据进行排序, 并依据次序将数据映射到数据段的相应位置. 假定 C_j^i 表示 WSN 中第 j 个分簇的第 i 个

传感节点,则 C_i^j 在第 t 轮周期内采集的数据可表示为 $S_{ij}^\lambda(t)$, 其中, λ 表示其数据类型, 则其经过编码后的值可表示为:

$$cd_i^j(t) = S_{ij}^1(t) \cup S_{ij}^2(t) \cup \dots \cup S_{ij}^\lambda(t) \quad (2)$$

式中, $S_{ij}^\lambda(t) = \xi(\mu - 1)$, μ 为传感数据类型的数量, ξ 为每种数据类型所需比特数, 表示如下:

$$\xi = \log(m_\lambda \times \gamma) \quad (3)$$

式中, m_λ 为具有第 λ 种数据类型的传感节点数量; γ 为第 λ 种传感数据的最大长度. 为增强密钥的随机性与实时性, 数据加密密钥在不同的周期内需动态改变, 密钥更新方法如式(4).

$$k_x(t) = \text{SHA}(k_x, t) \quad (4)$$

式中, $\text{SHA}(\cdot)$ 为 hmacSHA-1 伪随机函数. 同理, 认证标签也需周期性更新, 更新方法如式(5).

$$l_x(t) = \text{SHA}(l_x, t) \quad (5)$$

由此, 可得传感节点 C_i^j 在 t 轮周期内所采集的数据的密文 $\text{ED}_i^j(t)$, 如式(6).

$$\text{ED}_i^j(t) = cd_i^j(t) + k_x(t) \bmod H \quad (6)$$

式中, H 为大素数.

传感节点在采集监测对象的状态数据后, 采用上述方法对数据进行加密, 并将数据传输至簇头节点.

4 能量有效数据融合机制

分簇内传感节点由于部署的空间位置较近, 其采集的数据之间存在较大的冗余性. 若簇头节点直接将所有传感节点采集的数据传输至汇聚节点, 则将极大地消耗簇头节点有限的能量资源. 因此, 本文基于深度信任网络模型^[16], 通过将多个受限玻尔兹曼机(Restricted Boltzmann Machine, RBM)进行级联, 构建簇内传感数据的深度认知网络模型, 从而提取簇内传感数据的主要特征, 实现对传感数据的有效融合, 并将融合后的数据传输至汇聚节点, 达到降低簇头节点数据传输能耗的目的.

假定簇内传感节点集合为 $\Psi = \{\psi_1, \psi_2, \dots, \psi_n\}$, 其中, n 为簇内传感节点的数量. 簇内传感节点采集的经加密处理后的传感数据集合为 $\Pi = \{\pi_{\psi_1}, \pi_{\psi_2}, \dots, \pi_{\psi_n}\}$. 所提基于深度信任网络的数据融合模型如图2所示, 由可见层、隐层、输出层三层组成.

单个 RBM 由可见层 v 和隐层 h 两层神经元组成, v_i 为可见层的第 i 个神经元, h_j 为隐层的第 j 个神经元. 可见层 v 用于簇内传感数据集合 $\Pi = \{\pi_{\psi_1}, \pi_{\psi_2}, \dots, \pi_{\psi_n}\}$ 的输入, n 为可见层神经元个数,

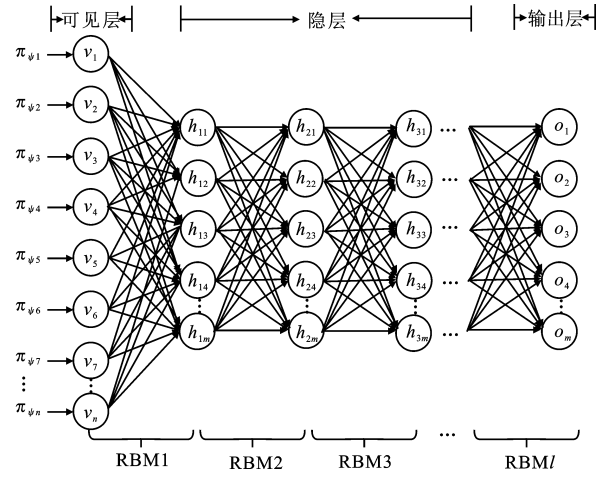


图2 数据融合模型

也为簇内传感节点个数. 隐层 h 可视为簇内传感数据特征的提取器. RBM 的层间全连接, 层内无连接.

假定 RBM 可见层神经元的状态向量 $v = [v_1, v_2, \dots, v_n]$, 隐层神经元状态向量 $h = [h_1, h_2, \dots, h_m]$, m 为隐层神经元数量. 则对于给定的状态组合 (v, h) , RBM 系统所具有的能量为:

$$E(v, h | \theta) = - \sum_{i=1}^n a_i v_i - \sum_{j=1}^m b_j h_j - \sum_{i=1}^n \sum_{j=1}^m v_i w_{ij} h_j \quad (7)$$

式中, $\theta = \{a, b, w\}$ 为 RBM 系统的参数集合; $a_i \in a$ 为可见层神经元的偏置; $b_j \in b$ 为隐层神经元的偏置; $w_{ij} \in w$ 为连接可见层神经元 i 与隐层神经元 j 之间的权值. 当 θ 中的参数为确定数值时, (v, h) 的联合概率分布如式(8)、(9).

$$P(v, h | \theta) = \frac{e^{-E(v, h | \theta)}}{Z(\theta)} \quad (8)$$

$$Z(\theta) = \sum_{v, h} e^{-E(v, h | \theta)} \quad (9)$$

提取簇内传感数据特征的关键在于求解传感数据矩阵 $\Pi = \{\pi_{\psi_1}, \pi_{\psi_2}, \dots, \pi_{\psi_n}\}$ 的概率分布 $P(v | \theta)$. $P(v | \theta)$ 为 (v, h) 的联合概率分布 $P(v, h | \theta)$ 的边缘分布, 如式(10).

$$P(v | \theta) = \sum_h P(v, h | \theta) = \frac{\sum_h e^{-E(v, h | \theta)}}{Z(\theta)} \quad (10)$$

研究表明, 归一化因子 $Z(\theta)$ 的计算复杂度较高, 因此, 无法通过计算 $Z(\theta)$ 确定传感数据矩阵的概率分布 $P(v | \theta)$. 然而, 由于 RBM 神经元的连接具有层间全连接, 层内无连接的特征. 因此, 给定可见层的神经元状态时, 隐层神经元的激活状态条件

独立,即当可见层神经元的状态向量 v 已知时,隐层第 j 个神经元的激活概率如式(11).

$$P(h_j = 1 \mid v, \theta) = \frac{1}{1 + \exp(-b_j - \sum_i v_i w_{ij})}$$

(11)

RBM 具有对称结构,当隐层神经元状态向量 h 给定时,可见层神经元的激活状态也条件独立,则可见层第 i 个神经元处于激活状态的概率为.

$$P(v_i = 1 \mid h, \theta) = \frac{1}{1 + \exp(-a_i - \sum_j h_j w_{ij})}$$

(12)

由此,即可估计簇内传感数据的概率分布 $P(v \mid \theta)$,实现对输入的簇内传感数据的重构.将簇内传感数据集 $\Pi = \{\pi_{\psi_1}, \pi_{\psi_2}, \cdots, \pi_{\psi_n}\}$ 作为可见层神经元的输入,并代入 RBM1 中对传感数据进行重构,将 RBM1 隐层的输出结果作为 RBM2 的可见层输入.继续进行计算直至 RBM 1 的隐层输出分簇传感数据集的特征向量 $O = [o_1, o_2, \cdots, o_m]$. 则可用 RBM 1 的输出层 $O = [o_1, o_2, \cdots, o_m]$ 表征分簇传感数据集的特征.

采用上述方法对簇内数据进行融合,融合后的整簇数据密文如式(13).

$$ED_i^{\text{all}} = \sum_{j=1}^n ED_i^j(t) \bmod H$$

(13)

簇头节点融合后的整簇数据认证标签 l_i^{all} 如式(14).

$$l_i^{\text{all}} = \sum_{j=1}^n l_i^j(t) \bmod P$$

(14)

式中, P 为大素数.

簇头节点将融合后的数据传输至汇聚节点,汇聚节点根据当前融合轮数生成传感节点与汇聚节点间的密钥 $k_x(t)$, 然后计算融合标签 $l_i^{\text{all}'}$, 计算方法如式(15).

$$l_i^{\text{all}'} = ED_i^{\text{all}} k_x(t) + \sum_{j=1}^n l_i^j(t) \bmod P$$

(15)

若 $l_i^{\text{all}} \neq l_i^{\text{all}'}$, 则说明传感数据在传输过程中部分丢失,汇聚节点直接丢弃此融合数据.

若 $l_i^{\text{all}} = l_i^{\text{all}'}$, 则通过完整性验证,汇聚节点依据解码规则提取不同类型数据的融合值,解码过程如下所示.

$$cd_i^{\text{all}}(t) = ED_i^{\text{all}} - \sum_{x=1}^n k_x(t)$$

(16)

$$m_s^{\text{all}} = cd_i^{\text{all}}(t) [(\mu - 1)\xi, \mu\xi - 1]$$

(17)

式中, $cd_i^{\text{all}}(t)$ 为第 t 轮簇内传感数据的融合结果.

5 仿真实验与结果分析

本文采用 Matlab 对所提 EDFP 机制进行了性能验证,并与典型的 LDLEC^[12]、CS-HE^[14] 方法进行了对比.主要验证的性能指标为隐私泄漏率、数据融合效率、平均剩余能量.仿真参数设置如表 1 所示.

表 1 仿真参数设置

参数	数值
区域面积/m ²	500×500
传感节点数量/个	45~150
传感节点存储空间/GB	1
传感节点通信半径/m	50
传感节点初始能量/J	100
簇头节点通信半径/m	100
簇头节点存储空间/GB	5
簇头节点初始能量/J	1 000
数据传输速率/(Mb/s)	1

如图 3,不同传感节点数量下 EDFP、CS-HE、LDLEC 三种方法的隐私泄漏率呈现出逐渐升高的趋势.这是由于随着传感节点数量的增多,网络中的恶意节点数量也增大,窃取传感节点隐私数据的行为增多,造成隐私泄漏的概率变大.由图 3 中可看出,所提 EDFP 相比 CS-HE 与 LDLEC,在隐私泄漏率方面,可平均分别降低约 19.1%、27.4%.

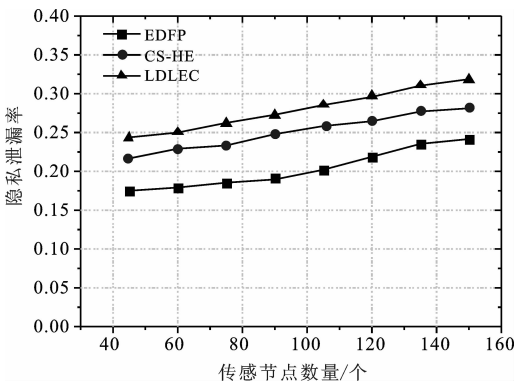


图 3 不同传感节点数量下的隐私泄漏率

如图 4,不同传感节点数量下 EDFP、CS-HE、LDLEC 三种方法的数据融合效率呈现出逐渐升高的趋势.这是因为随着传感节点数量增多,需融合处理的传感数据的数量随之增大.但三种方法都提出了有效的数据融合方法,对传感数据进行融合处理.因此,当传感数据的数量增多时,数据融合的效率并不会受到影响.反之,由于三种机制的数据融合方法

设计较为合理,因此,随着传感节点数量增大,数据融合效率逐渐升高.图 4 还表明,所提 EDFP 相比 CS-HE 与 LDLEC,在数据融合效率方面,可平均分别提高约 12.7%、17.6%.

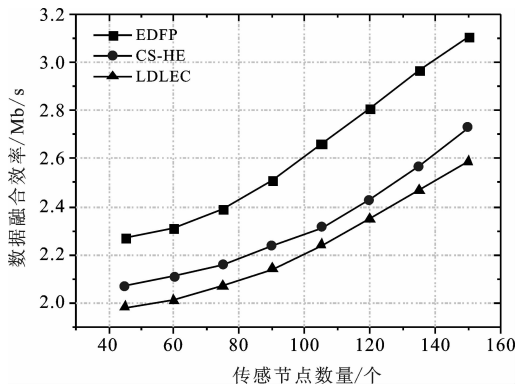


图 4 不同传感节点数量下的数据融合效率

由图 5 可知,在不同的网络运行时间下,EDFP、CS-HE、LDLEC 三种方法的簇头节点平均剩余能量逐渐减少.这是由于随着网络运行时间的增加,簇头节点需传输的数据量逐渐增多,而数据的传输需耗费大量的能量资源,由于簇头节点为电池供电,因此,其能量消耗随传输的数据量增多而逐渐增大,剩余的能量资源逐渐减小.图 5 还表明了,所提 EDFP 相比 CS-HE 与 LDLEC,在平均剩余能量方面,可平均分别提高约 14.8%、24.5%.

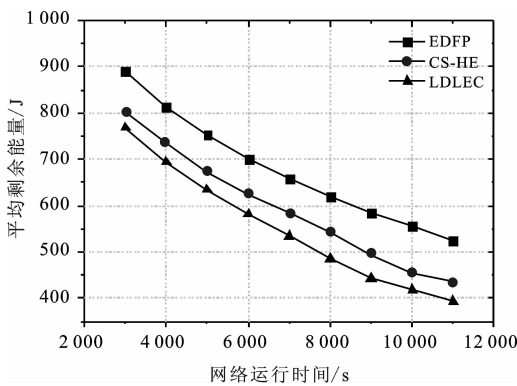


图 5 不同网络运行时间下的平均剩余能量

所提 EDFP 通过在传感节点上对传感数据进行加密,从而保障传感数据的隐私性与安全性.并且,基于深度信任网络模型,在簇头节点上对簇内传感数据进行有效融合,减少簇头节点向汇聚节点传输的数据量,从而,降低簇头节点的数据传输能耗.LDLEC 与 CS-HE 对数据的融合方法设计基于浅层学习模型,对数据的融合效果较为有限.并且,LDLEC 并未考虑传感数据的隐私保护问题.因此,

所提 EDFP 相比 LDLEC 与 CS-HE,在隐私泄露率、数据融合效率、平均剩余能量方面均可获得较大的性能增益.

6 结束语

传感数据的节能传输与隐私保护技术的发展进步可推动无线传感网的进一步深入应用.提出带有隐私保护的无线传感网能量有效数据融合方法.设计了传感数据隐私保护方法,保障传感数据的隐私安全.研究能量有效的数据融合机制,提高传感数据融合的效率.仿真结果表明,所提机制可有效保障传感数据的隐私安全,提高数据融合的效率,并降低节点能量消耗.然而,本文所作研究工作未考虑传感节点可充电的情况,未来拟研究可充电传感节点的高效数据融合机制.

参考文献:

- [1] CHENG L, NIU J, LUO C, et al. Towards minimum-delay and energy-efficient flooding in low-duty-cycle wireless sensor networks[J]. Computer Networks, 2018, 134(4): 66-77.
- [2] LAJARA R, PÉREZ-SOLANO J J, PELEGRI-SEBASTIÁ J. Predicting the batteries' state of health in wireless sensor networks applications[J]. IEEE Transactions on Industrial Electronics, 2018, 65(11): 8936-8945.
- [3] LIU J, SHEN H, YU L, et al. Characterizing data deliverability of greedy routing in wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2018, 17(3): 543-559.
- [4] 任志玲,张广全,林冬,等. 无线传感器网络应用综述[J]. 传感器与微系统,2018,37(3):1-10.
- [5] 俞姝颖,吴小兵,陈贵海,等. 无线传感器网络在桥梁健康监测中的应用[J]. 软件学报,2015,26(6): 1486-1498.
- [6] 高洁,吴宪海,文琼瑶. 基于节点轮换的无线传感器网络节能策略研究[J]. 传感技术学报,2018,31(3): 477-482.
- [7] 杨浩. 无线传感器网络环境下能量有效的虚拟坐标构建[J]. 小型微型计算机系统,2018,39(2):245-248.
- [8] 窦桂琴,万润泽,张兴艳. 基于模糊理论的无线传感器网络数据融合算法[J]. 微电子学与计算机,2012,29(9):133-136.
- [9] 余修武,范飞生,周利兴,等. 无线传感器网络自适应预测加权数据融合算法[J]. 传感技术学报,2017,30(5):772-776.