WSN 中基于贝叶斯压缩感知的信息隐藏传输研究*

熊继平,赵 健,宣利峰
(浙江师范大学 数理与信息工程学院 图形与图像处理研究所,浙江 金华 321004)

摘 要:提出了一种无线传感器网络中,在压缩感知域内对敏感数据进行嵌入及提取的安全传输框架。在该框架中,传感器节点利用压缩感知技术对敏感数据进行编码,在基站端利用基于贝叶斯的压缩感知重构算法进行敏感数据的恢复。充分利用压缩感知技术特点,编码的复杂性转移到基站,而传感器节点仅需执行简单的线性运算,从而在实现敏感信息安全传输的同时减少了能量消耗。仿真结果表明,该算法能够在无线传感器网络中实现敏感数据的安全传输,并且具有抗噪性强的特点。

关键词:贝叶斯压缩感知;无线传感器网络;信息隐藏;噪声信道

中图分类号:TP219.9;TN929.5 **文献标识码**:A **文章编号**:1674-7720(2014)05-0062-05

Research on the information hiding transmission in WSN based on Bayes compressive sensing

Xiong Jiping, Zhao Jian, Xuan Lifeng
(Institute of Image and Graphics Processing, School of Mathematics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China)

Abstract: This paper proposes a novel embedding and secure transmission framework of sensitive data based on compressive sensing domain in wireless sensor networks. In this framework, sensor nodes encode sensitive data using compressive sensing technology, and base stations decode the sensitive data using Bayes compressive sensing reconstruction algorithm. In this method, the algorithm complexity is transferred to the base station, while sensor nodes only need to do simple linear operations which highly reduce the energy consumption. The simulation result indicates that this method can realize secure transmission of data in WSN even under noise environment.

Key words: Bayes compressive sensing; wireless sensor network; information hiding; noise channel

无线传感器网络[1]WSN(Wireless Sensor Network)是以数据为中心的网络,常被应用于军事、国防、物流、监测等领域,这些数据一旦被第三方恶意截获,将危及到全局 WSN 安全性,因此必须采取措施来保护 WSN 中的敏感数据。对称加密技术 SET(Symmetric Encryption Technique)是目前广泛应用于 WSN 的安全方法之一[2],其特点是安全性较好,但所需的计算复杂度较高。由于 WSN 传感器节点安装的操作系统处理能力和电池能耗的限制条件,如果采用 SET 技术,那么整个 WSN 的生命周期将大大缩减。信息隐藏 IH(Information Hiding)技术也是一种保障数据安全性的可靠方法。肖湘蓉等[3]第一次将信息隐藏技术与 WSN 结合起来,通过最低有效位算法将敏感信息嵌入到常规信息中,实现不被恶意感知的目的。但是该方法还存在两个问题:首先,在应用 LSB 算法前,敏感信息仍然需要通过对称加密方法进行加密;其次,对于无线信道的抗噪性较弱。

压缩感知[4-6]CS(Compressive Sensing)是一种信号处理领域新提出的技术,已在认知无线电、图像处理、计算机视觉、机器学习等诸多领域产生了深远的影响[7-10]。该理论表明,当信号满足稀疏性或者在某一变换域稀疏时,那么该信号能够通过少量测量值精确重构出来。CS 编码简单的特点与 WSN 的网络结构高度契合,也即对传感器节点的编码要求非常低,目前利用 CS 实现数据的能量有效传输已经成为热门的研究方向[11-15]。Xiong

*基金项目:浙江师范大学计算机软件与理论省级重中之重学科开放基金(ZSDZZZZXK28);浙江省教育厅项目(Y200805325)

Jiping 等[16]首次将CS编码方案应用到无线传感器网络的敏感数据传输中，在无噪和丢包信道中能够很好地工作，但其在噪声信道中不能准确获得敏感数据。因此，本文针对无线信道中存在的噪声干扰问题，进一步提出一种基于贝叶斯压缩感知[17]BCS（Bayesian Compressive Sensing）的有噪信号重构算法，在降低编码端计算开销的同时实现数据的高效敏感传输和精确重构。

本文首先介绍贝叶斯压缩感知理论、随机贝叶斯重构方法及优化的自适应重构方法，然后将其引入无线传感器网络的敏感信息安全传输框架中，接着通过实验仿真验证方法的有效性，最后总结全文并指出下一步研究方向。

1 贝叶斯压缩感知理论

BCS理论就是从贝叶斯算法的角度来重构压缩测量值，实现信号传输的目的。假设原始信号 $\boldsymbol{x}(N\times1)$ 在某一组基 $\boldsymbol{B}$ 下是可压缩或者可稀疏的，则CS测量值可以表示为：

$$\boldsymbol{y}=\boldsymbol{\Phi B}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{\Phi\omega} \tag{1}$$

其中，$\boldsymbol{\Phi}$ 为传感矩阵，$\boldsymbol{B}$ 为稀疏矩阵，$\boldsymbol{\omega}$ 为传输信号 $\boldsymbol{x}$ 在 $\boldsymbol{B}$ 的稀疏表示，$\boldsymbol{y}$ 为测量矩阵。在BCS理论中，需要一个 $\boldsymbol{\omega}$ 在某组基 $\boldsymbol{B}$ 上为稀疏的先验置信；$\boldsymbol{y}$ 从压缩测量值观测获得，旨在为权值 $\boldsymbol{\omega}$ 提供一个后验置信（密度函数）。贝叶斯框架在执行压缩测量时为加性噪声提供一个后验密度函数估计，因此，可以通过BCS解决信道噪声问题。

1.1 贝叶斯角度的压缩感知

假设噪声信号 n 由均值为0、方差 σ^2 未知的高斯噪声近似构成，则可以得到：

$$\boldsymbol{y}=\boldsymbol{\Phi\omega}+n \tag{2}$$

由式(2)可以得到高斯似然模型为：

$$p(\boldsymbol{y}|\boldsymbol{\omega},\sigma^2)=(2\pi\sigma^2)^{-M/2}\exp\left(-\frac{1}{2\sigma^2}\|\boldsymbol{y}-\boldsymbol{\Phi\omega}\|^2\right) \tag{3}$$

在贝叶斯公式中，通过在 $\boldsymbol{\omega}$ 中放置稀疏促进先验获得其稀疏性。目前广泛采用的稀疏先验是拉普拉斯密度函数[18-19]：

$$p(\boldsymbol{\omega}|\lambda)=(\lambda/2)^N\exp\left(-\lambda\sum_{i=1}^{N}|\omega_i|\right) \tag{4}$$

由于拉普拉斯先验与高斯似然不为共轭，直接采用拉普拉斯先验很难实现，因此，相关贝叶斯推理不会表现为闭型。通过构造分层先验构造拉普拉斯先验：

$$p(\boldsymbol{\omega}|\alpha)=\prod_{i=1}^{N}N(\omega_i|0,\alpha_i^{-1}) \tag{5}$$

其中，α_i 是高斯密度函数的精度值。对超参数 α 赋Gamma先验：

$$p(\alpha|a,b)=\prod_{i=1}^{N}\Gamma(\alpha_i|a,b) \tag{6}$$

其中，a 和 b 是Gamma分布的两个参数。通过求解超参数 α 的边缘分布，全局先验 $\boldsymbol{\omega}$ 通过式(5)和(6)估计获得：

$$p(\boldsymbol{\omega}|a,b)=\prod_{i=1}^{N}\int_0^{\infty}N(\omega_i|0,\alpha_i^{-1})\Gamma(\alpha_i|a,b)\,\mathrm{d}\alpha_i \tag{7}$$

当 ω_i 是观测数据且 $N(\omega_i|0,\alpha_i^{-1})$ 为似然函数时，密度函数 $\Gamma(\alpha_i|a,b)$ 是 α_i 的共轭先验。式(7)中的积分能够被估计，并且服从Student-t分布。选取适当的 a 和 b，Student-t分布在 $\omega_i=0$ 处附近获得峰值，因此式(7)中的先验能够满足多数 ω_i 的值为0，促进其先验稀疏性。

1.2 随机的贝叶斯CS重构

假定超参数 α 和 $\alpha_0=1/\sigma^2$ 已知，给定CS测量值 $\boldsymbol{y}$ 和投影矩阵 $\boldsymbol{\Phi}$，后验 $\boldsymbol{\omega}$ 服从多元高斯分布：

$$p(\boldsymbol{\omega}|\boldsymbol{y},\alpha,\sigma^2)\propto\prod_{i=1}^{N}N(\mu,\sum) \tag{8}$$

其中，均值和协方差分别为：

$$\mu=\alpha_0\sum\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{y} \tag{9}$$

$$\sum=(\alpha_0\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{\Phi}+A)^{-1} \tag{10}$$

其中，$A=\mathrm{diag}(\alpha_1,\alpha_2,\cdots,\alpha_N)$。此问题亦为相关向量机（RVM）的学习问题，而此时相关向量机中相关的学习问题转换成了获取超参数 α 和 $\alpha_0=1/\sigma^2$。在RVM中，这些超参数通过求解type-II最大似然获得的数据进行估计[20]。求解权值 $\boldsymbol{\omega}$ 的边缘密度，α 和 α_0 边缘似等价于表示为对数 $L(\alpha,\alpha_0)$：

$$\begin{aligned}L(\alpha,\alpha_0)&=\log\ p(\boldsymbol{y}|\alpha,\alpha_0)\\&=\log\int p(\boldsymbol{y}|\boldsymbol{\omega},\alpha_0)\ p(\boldsymbol{\omega}|\alpha)\,\mathrm{d}\boldsymbol{\omega}\\&=-\frac{1}{2}[K\log2\pi+\log|\boldsymbol{C}|+\boldsymbol{y}^{\mathrm{T}}\boldsymbol{C}^{-1}\boldsymbol{y}]\end{aligned} \tag{11}$$

其中，$\boldsymbol{C}=\sigma^2\boldsymbol{I}+\boldsymbol{\Phi A}^{-1}\boldsymbol{\Phi}^{\mathrm{T}}$。采用 α 和 α_0 点估计的type-II最大似然近似法最大化式(9)，能够通过EM算法[21]实现并获得：

$$\alpha_i^{\mathrm{new}}=\frac{\gamma_i}{\mu_i^2},\quad i\in\{1,2,\cdots,N\} \tag{12}$$

其中，μ_i 是式(9)中计算第 i 次的先验平均值；定义 $\gamma_i=1-\alpha_i\sum_{ii}$，$\sum_{ii}$ 是式(10)后验方差第 i 次迭代的对角元素。噪声方差 $\sigma^2=1/\alpha_0$，得到：

$$1/\alpha_0^{\mathrm{new}}=\frac{\|\boldsymbol{y}-\boldsymbol{\Phi\mu}\|_2^2}{K-\sum_i\gamma_i},\quad i\in\{1,2,\cdots,N\} \tag{13}$$

μ、$\sum$ 和 α、α_0 可以交替进行迭代计算直到满足收敛条件。最后可以得到信号 $\boldsymbol{x}=\boldsymbol{B\omega}$ 后验密度函数也是一个多元高斯分布，均值和协方差为：

$$E(\boldsymbol{x})=\boldsymbol{B}\mu \tag{14}$$

$$\mathrm{Cov}(\boldsymbol{x})=\boldsymbol{B}\sum\boldsymbol{B}^{\mathrm{T}} \tag{15}$$

其中，协方差矩阵的对角元素产生一个 x 重构精度的误差条（Error Bars），以式（14）中均值的形式表示。

最近对 RVM 算法的理论分析[20-21]表明，RVM 为 l_0 范数稀疏性测量提供一个比 l_1 范数更加紧的近似值，证明在最差的场景中，RVM 也能优于其他广泛使用的稀疏表示算法。

1.3 优化的贝叶斯 CS 重构

在原始 CS 结构中，随机投影 $\boldsymbol{\Phi}$ 由基本随机变量的独立同分布实现构成。此外，早期的文献用于估计 $\boldsymbol{\omega}$ 的 CS 算法采用的是一个如式（16）的点估计方法：

$$\widetilde{\boldsymbol{\omega}}=\arg\min_{\boldsymbol{\omega}}\{\|\boldsymbol{y}-\boldsymbol{\Phi\omega}\|_2^2+\rho\|\boldsymbol{\omega}\|_1\} \tag{16}$$

然而这些方法都没有考虑信号 x 的不确定性，因此 $\boldsymbol{\Phi}$ 的自适应设计在这些方法中不适用。根据式（14）、（15）中定义，上一节中讨论的 BCS 算法能够实现对 x 的有效计算，因此考虑自适应随机投影 r_{K+1} 的可行性来减少不确定性。该框架已经在实验设计及机器学习中被研究。

信号 x 的后验估计是一个均值 $E(\boldsymbol{x})=\boldsymbol{B}\mu$、协方差 $\mathrm{Cov}(\boldsymbol{x})=\boldsymbol{B}\sum\boldsymbol{B}^{\mathrm{T}}$ 的多元高斯分布，因此 x 的微分熵（Differential entropy）满足：

$$\begin{aligned}h(\boldsymbol{x})&=-\int p(\boldsymbol{x})\log p(\boldsymbol{x})\mathrm{d}\boldsymbol{x}=\frac{1}{2}\log|\boldsymbol{B}\sum\boldsymbol{B}^{\mathrm{T}}|+\mathrm{const}\\&=\frac{1}{2}\log|\sum|+\mathrm{const}\\&=-\frac{1}{2}\log|\boldsymbol{A}+\alpha_0\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{\Phi}|+\mathrm{const}\end{aligned} \tag{17}$$

其中，常量 const 独立于投影矩阵 $\boldsymbol{\Phi}$。由于 $\boldsymbol{A}=\mathrm{diag}(\alpha_1,\alpha_2,\cdots,\alpha_N)$，因此 CS 测量值 y 的微分熵独立性通过 α 和 α_0 的点估计定义。

在迭代过程中，选取最优新投影 r_{K+1} 来最小化公式（17）中的微分熵。通过增加一个用 r_{K+1} 表示且大小为 $(K+1)$ 行向量来增广 $\boldsymbol{\Phi}$ 实现。用 $h_{\mathrm{new}}(\boldsymbol{x})$ 表示增加该新的投影向量 $\boldsymbol{\Phi}$ 后的微分熵：

$$h_{\mathrm{new}}(\boldsymbol{x})=h(\boldsymbol{x})-\frac{1}{2}\log|1+\alpha_0\boldsymbol{r}_{K+1}^{\mathrm{T}}\sum\boldsymbol{r}_{K+1}| \tag{18}$$

其中，α_0 和 $\sum$ 通过前一步的 K 测量值估计获得。为了最小化 h_{new}，只要求解 $\boldsymbol{r}_{K+1}^{\mathrm{T}}\sum\boldsymbol{r}_{K+1}$ 的最大值，也即：

$$\boldsymbol{r}_{K+1}^{\mathrm{T}}\sum\boldsymbol{r}_{K+1}=\boldsymbol{r}_{K+1}^{\mathrm{T}}\mathrm{Cov}(\boldsymbol{\omega})\boldsymbol{r}_{K+1}=\mathrm{Var}(\boldsymbol{y}_{K+1}) \tag{19}$$

通过推导，式（19）等价于求预期测量值 y_{K+1} 方差的最大值。换言之，投影 r_{K+1} 应该被用于组成数据大多不确定的测量值 y_{K+1}，实现相关测量值的最大化利用。

本章提出自适应框架为新投影 r_{K+1} 的选取提供一个较好的设置，在优化为目的情况中，x 的不确定性将较大程度地减少。如果能够自适应地设计新投影 r_{K+1}，将执行一个矩阵的特征分解（Eigen Decomposition），并且被选作具有最大特征值的特征向量 r_{K+1} 的表示。在随后仿真过程中，选取具有最大特征值的特征向量作为新投影 r_{K+1}。

2 基于 BCS 的 WSN 敏感信息传输模型

2.1 典型 WSN

在一个典型的单跳 WSN 中，每一个节点都是通过无线信道与基站进行通信的。本文假设每个传感器节点都具有多传感器感知模块，能够同时采集不同的敏感信息和常规信息。在目标区域部署 WSN 前，设定各个传感器节点 N_i 与基站共享密钥 K_i，各自存储在掉电不会丢失的存储区中。单跳 WSN 由部署在一定区域的传感器节点和基站组成，通过 BS 来采集各个节点的感知数据。单跳 WSN 的拓扑结构如图 1 所示。

图 1 单跳 WSN 的拓扑结构图

2.2 噪声信道数据敏感信息传输模型

建立一个基于 BCS 的单跳 WSN 敏感信息传输的模型，如图 2 所示。在传感器节点编码端，敏感数据通过 BCS 嵌入到常规载体数据中构成目标传输数据；目标传输数据通过具有噪声干扰的无线信道；在解码端，采用 BCS 解码算法重构敏感数据，利用向量作差和相乘获得常规载体数据，实现原始信号敏感的传输。

图 2 基于 BCS 的有噪丢包数据安全敏感传输模型

本文采用的编解码算法流程如图 3 所示。

3 仿真结果及分析

3.1 基于随机 BCS 的噪声信道仿真结果与分析

为了验证提出方法的有效性，利用 MATLAB 模拟构建了一个噪声为 $n\sim N(0,\sigma^2 I)$ 的无线信道。当传输数据通过无线信道时，利用噪声控制函数，模拟实现对数据的加噪控制。在解码端，分别采用凸优化算法、基追踪重构法和本文采用的随机 BCS 算法重构数据，通过比较体现 BCS 的优势。此外，本文还对 BCS 进行相应的改进，采用优化 BCS 方法对数据进行重构。

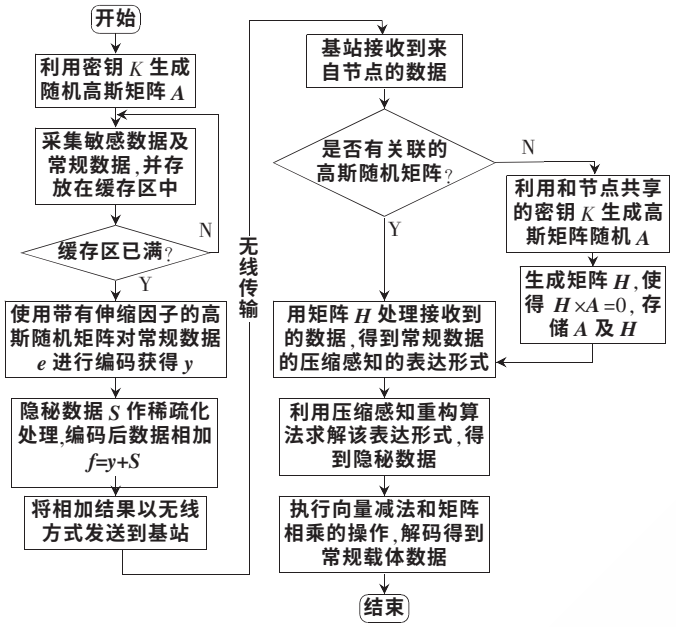

图 3 无线传感器编解码端算法流程

敏感信息 S 的长度 $m=512$，常规载体数据长度为 $n=256$。ρ 表示敏感信号 S 的稀疏率，ρ 值越大，信号越不稀疏，传输的敏感数据越多，但重构所得到的数据效果越差。因此，通过仿真选取一个合适的 ρ 值，减少对重构效果影响的同时增加有效数据传输。常规载体数据 e 的长度为 $n=256$，测量值的采样点个数 k 随着迭代次数而变化。投影矩阵 Φ 由一个 $k\times m$ 的高斯分布 $N(0,1)$ 矩阵构成，此处将 Φ 的行向量归一化到单位量级。噪声信号由均值为 0、标准差为 $\sigma=0.005$ 的高斯分布模拟产生。重构敏感信息衡量标准为均方误差、重构时间，其中，重构时间用 t 来表示，用于衡量算法的计算速度。

图 4 和表 1 分别给出了本文的仿真结果，其中，测量值采样点个数 $k=100$，稀疏率 $\rho=5\%$。图 3(a)表示原始信号，图 3(b)、(c)、(d)分别表示 3 种方法的重构情况。由图可知，在噪声信道中，BCS 重构在零点附近更加平滑，具有更好的去噪效果；而采用凸优化和基追踪[16]则包含较多毛刺信号，表明其无法消除重构数据中的噪声。此外，采用基本重构法和 BP 重构法会产生部分信号的丢失。从重构时间角度来看，采用贝叶斯压缩感知技术所需要的重构时间要小得多。

表 1 噪声无线信道下 3 种不同 CS 重构算法比较($k=100$)

CS 重构	凸优化	BP 重构	BCS 重构
MSE	0.026	0.047	0.002 7
t/s	0.79	1.45	0.18
稀疏度	512	512	25

3.2 基于优化 BCS 的噪声信道仿真结果与分析

图 5 给出了随机 BCS 方案和优化 BCS 方案的重构误差对比图。从中可以看出，优化 BCS 方法具备更好的性能，也即在相同的测量个数情况下，基于优化 BCS 的重构信号具有更高的信噪比。

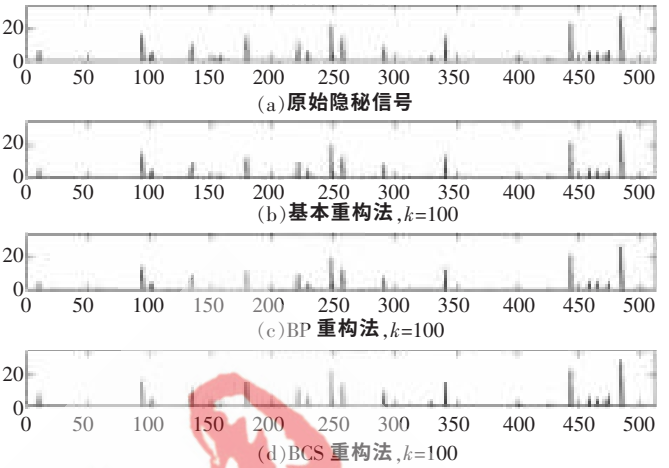

图 4 噪声信道中 3 种重构效果对比($m=512$，$n=256$，稀疏率 $\rho=5\%$)

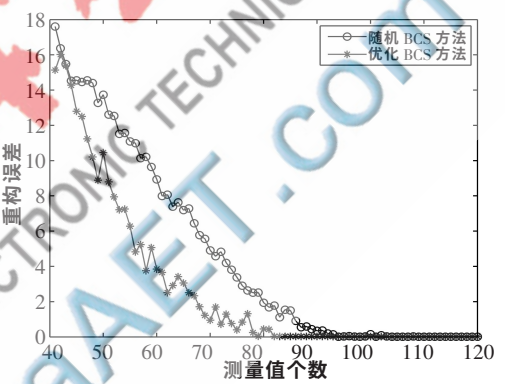

图 5 噪声丢包信道中重构均方误差对比($m=512$，$n=256$，稀疏率 $\rho=5\%$)

物联网应用的大面积推广和应用对数据的安全传输需求将会越来越迫切，本文研究了作为物联网网络基础的无线传感器网络中的敏感信息安全传输问题。提出了有噪信道下的基于贝叶斯压缩感知的敏感信息安全传输框架，并进行了模拟仿真。从仿真效果来看，本方案能够抵御一定的噪声，有效地恢复敏感数据和常规数据。

本文提出的信息隐藏方案本质上是在压缩感知域进行敏感信息的嵌入以及提取，明显不同于传统的基于空间域和频域的嵌入方案，因此在一定程度上可以促进信息隐藏技术的发展。此外，本文的关注点是敏感信息的有效嵌入和提取，对这种压缩感知框架下的信息隐藏技术进行隐秘性以及安全性等分析是今后研究的内容和主要方向。

参考文献

[1] YICK J, MUKHERJEE B, DIPAK GHOSAL. Wireless sensor network survey [J]. Computer Networks, 2008,52(12):2292-2330.

[2] ALI S T, SIVARAMAN V, DHAMDHERE A, et al. Secure key loss recovery for network broadcast in single-hop wireless sensor networks [J]. Ad Hoc Networks, 2010,8(6):668-679.

[3] Xiao Xiangrong, Sun Xingming, Yang Lincong, et al. Secure data transmission of wireless sensor network based on information hiding [C]. Fourth Annual International Conference on Mobile and Ubiquitous Systems, 2007: 1-6.

[4] DONOHO D L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.

[5] CANDÉS E, TAO T. Decoding by linear programming[J]. IEEE Transaction on Information Theory, 2005, 51(12): 4203-4215.

[6] STROHMER T. Measure what should be measured: progress and challenges in compressive sensing[J]. Signal Processing Letters, IEEE, 2012, 19(12): 887-893.

[7] Yi Yang. Perceptual compressive sensing for image signals[C]. ICME, 2009: 89-92.

[8] Wang Ying, POLO Y L, PANDHARIPANDE A, et al. Distributed compressive wide-band spectrum sensing[C]. Information Theory and Applications workshop, IEEE, 2009: 178-183.

[9] KANG L W, LU C S. Distributed compressive video sensing [C]. 2009 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2009: 1169-1172.

[10] LUO C, WU F, SUN J, et al. Compressive data gathering for large-scale wireless sensor networks [C]. Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, ACM, 2009: 145-156.

[11] 孙洪,张智林,余磊.从稀疏到结构化稀疏:贝叶斯方法[J].信号处理,2012,28(6):759-773.

[12] 唐亮,周正,石磊,等.基于能量均衡的无线传感器网络压缩感知算法[J].电子与信息学报,2011,33(8):1919-1923.

[13] WANG J, TANG S, YIN B, et al. Data gathering in wireless sensor networks through intelligent compressive sensing [C]. INFOCOM, 2012 Proceedings IEEE, 2012: 603-611.

[14] SHEN Y, HU W, RANA R, et al. Nonuniform compressive sensing for heterogeneous wireless sensor networks[J]. IEEE Sensors Journal, 2013, 13(6): 2120-2128.

[15] 练秋生,刘芳,陈书贞.基于块 A* 正交匹配追踪的多传感器数据联合重构算法[J].电子与信息学报,2013,35(3):721-727.

[16] Xiong Jiping, Xuan Lifeng, Huang Tao, et al. Novel covert data channel in wireless sensor networks using compressive sensing[J]. Journal of Networks, 2012, 7(10): 1523-1529.

[17] Ji Shihao, Xue Ya, LAWRENCE C. Bayesian compressive sensing[J]. IEEE Transactions on Signal Processing, 2008, 56(6): 2346-2356.

[18] TIPPING M E. Sparse Bayesian learning and the relevance vector machine[J]. Journal of Machine Learning Research, 2001(1): 211-244.

[19] GEORGE E I, MCCULLOCH R E. Approaches for Bayesian variable selection[J]. Statistica Sinica, 1997(7): 339-373.

[20] WIPF D P, RAO B D. l_0-norm minimization for basis selection [C]. Advances in Neural Information Processing Systems (NIPS 17), 2005.

[21] WIPF D P, RAO B D. Comparing the effects of different weight distributions on finding sparse representations [C]. Advances in Neural Information Processing Systems (NIPS 18), 2006.

(收稿日期:2013-11-14)

作者简介:

熊继平,男,1982 年生,副教授,研究生导师,主要研究方向:压缩感知、信号处理和互联网安全。