

基于无线传感器网络相关性的信息安全防御机制

洪勇*, 李平

(长沙理工大学 计算机与通信工程学院, 长沙 410004)

(* 通信作者电子邮箱 hongyong0913@qq.com)

摘要:当无线传感器网络中的传感节点被俘获时,可能发生内部攻击,从而致使系统信息安全缺失。针对这一情况,提出一种基于环状空间相关性模型的安全防御机制。基于环状空间相关性的模型,节点与节点之间进行信任值结合计算,相邻节点再对其进行信任评估,根据信任评估识别被俘获节点,间接去除被俘获节点信息,以达到信息的安全防御。仿真实验表明,经过机制改进后的各数据失真度有明显提高。该机制能有效识别并剔除虚假、恶意信息,提高系统的信息安全。

关键词:无线传感器网络;虚假数据;信息安全;空间相关性;失真度

中图分类号: TP309; TP393.08; TN926 **文献标志码:** A

Information security defense mechanism based on wireless sensor network correlation

HONG Yong*, LI Ping

(Computer and Communication Engineering Institute, Changsha University of Science and Technology, Changsha Hunan 410004, China)

Abstract: When the sensor nodes in Wireless Sensor Network (WSN) are captured, the internal attack may occur, thus resulting in a security deficiency of the system information. Regarding this, a security defense mechanism based on the annular space correlation model was proposed. The combined trust value between the nodes was calculated based on the model of the annular space, and the trust assessment again on its adjacent nodes was carried out. The captured nodes were recognized according to the trust assessment, and the information of the captured nodes were removed indirectly, thus achieving information security defense. The simulation results demonstrate that the data distortion has significantly improved by the optimized mechanism. This mechanism can effectively identify and remove errors and detrimental information, which improves the security of information in the system.

Key words: Wireless Sensor Network (WSN); false data; information security; spatial correlation; distortion degree

0 引言

随着微电子技术、计算机技术和无线通信技术的飞速发展和日益成熟,无线传感器网络(Wireless Sensor Network, WSN)^[1-3]逐渐被应用于军事、环境监测等多个领域,开始逐渐进入实用阶段。这种拥有计算和通信能力的微型传感器网络是由大量廉价微型传感器节点通过无线通信方式形成的多跳自组织网络,能够以协作的方式完成对部署区域内的各种监测对象数据的采集、传送和融合等工作,故其安全性^[4-5]尤为重要。WSN应用日益复杂,其安全需求也呈现多样性,传统的基于密码体系的安全机制主要用于抵抗外部攻击,无法有效解决由于节点被俘获而发生的内部攻击;而且由于传感器节点能力所限,当节点被俘获时很容易发生秘密信息泄露,如果无法及时识别被俘获节点,则整个网络将被控制。在实际战场环境或者无法实施物理保护的环境中,节点被俘获的现象极易发生,这就需要有效机制及时识别被俘获节点,有针对性地采取相应措施以减小系统损失。本文提出一种基于环状空间相关性模型的安全防御机制,观察节点间相互通信,计算各相关信任值,从而间接去除虚假、恶意信息,能大大提高系统的安全性。

1 WSN 中的空间相关性模型

1.1 传感器网络中原空间相关性模型框架

针对无线传感器网络的事件监测应用,Vuran等^[6-7]提出了一个空间相关性模型。该模型将事件源模拟为一个随机过程,在某一时刻事件源是一个随机变量。该模型将事件域中节点间的观测值模拟为联合高斯随机变量,将节点观测值和事件源信息也模拟为联合高斯随机变量;该模型还将每个节点观测信息的期望值处理为零,并认为事件源信息和节点观测值的方差均一样;此外,该模型认为事件源信息和节点观测值之间以及节点观测值之间存在的空间相关性只与距离有关,于是它采用一个能量指数模型来计算节点观测值间的空间相关性。事件域中每个节点将自己的观测值编码,然后通过网络发送到sink节点^[8-9];sink节点将接收到每个节点的信息解码,然后利用这些节点观测值作平均得到对事件源的估计。该模型以最小均方差为解码方法得到一个失真度公式,用失真度来度量对事件源估计的精确程度。

1.2 传感器网络中环状空间相关性模型框架

Vuran等提出的空间相关性模型对事件源的估计是所有发送数据节点观测值的均值,这造成sink节点对事件源的估计不精确,因此苏威等^[10]提出了一种环状空间相关性模型。

收稿日期:2012-08-20; **修回日期:**2012-09-18。 **基金项目:**国家科技重大专项(2011ZX03005-004-01);中国科学院先导课题(XDA06040100);国家863计划项目(2012AA050804);湖南省科技重大专项(2010GK3069)。

作者简介:洪勇(1989-),男,湖南衡阳人,硕士研究生,主要研究方向:传感器网络;李平(1972-),男,湖南长沙人,副教授,博士,CCF会员,主要研究方向:通信安全、传感器网络。

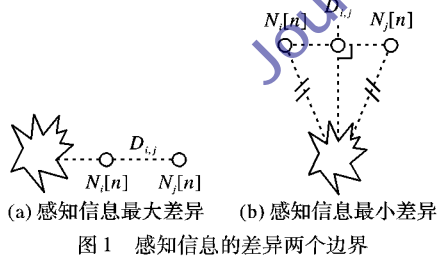
该模型对 Vuran 等提出的空间相关性模型假设不合理的地方进行了改进。首先,该模型假设每个节点观测值的期望不为零,这样能体现出每个节点的观测值随节点半径的不同而变化的情况;其次,该模型认为有着相同节点半径的节点观测值间相关性更高,于是假设节点半径相同的节点的观测值期望相同,节点半径不同的节点观测值期望不同。苏威等^[10]给出了一个适合于传感器网络异常事件监测应用的环状空间相关性模型和相应的估计方法。

2 虚假信息攻击模型

恶意节点是指敌方部署的外来节点,或者被敌方俘获的网络中的合法节点,恶意节点可能单个行动,也可能集体行动,多个恶意节点还有可能有计划地进行共谋,目前为止,还没有很好的一种方式去鉴别恶意节点。虚假数据攻击^[11-12]中,攻击者即恶意节点通过对经过的数据进行篡改,将虚假的数据通过网络汇聚到端节点,然后回传到基站,使用户接收到错误的信息,从而作出错误的决策。当攻击者本身就是数据源节点时,下游任何节点都无法鉴别数据的真实性。采取虚假数据攻击的攻击者一般都是被敌方俘获的网络内部节点,因而被俘节点的密钥等信息均已被敌方获取,只要节点按照基站的要求及时地发送和转发数据,攻击就难以被发现,因此这是一种极其隐蔽的攻击方式。两个极端相反的感知信息边界如图1所示,本文使用的相关符号定义如表1所示。

表1 本文使用的符号定义

字符	所代表意义
n_i	节点 i
nr_i	节点 i 的感知信息值
nt_i	节点 i 的感知时间值
ns_i	节点 i 的感知信息成功价值
nf_i	节点 i 的感知信息失败价值
cn_i	节点 i 的感知信息的一致价值
in_i	节点 i 的感知信息的不一致价值
B_i	节点 i 的使用寿命值
T_i	节点 i 的信任评估价值



如图1(a),在同一事件源中,节点 i, j 的感知信息分别为 nr_i, nr_j 。假设节点 i, j 距离固定为 $d_{i,j}$, 当两个节点同事件源在同一条直线上,且事件源在两节点对应的延长线上时,它们感知的信息差异值最大;另外一种情况如图1(b),同一事件源中同样假设节点 i, j 距离为 $d_{i,j}$, 当事件源在两节点之间的中垂线上时,两个节点感知的信息相似,其感知的信息差异值最小,且在理想状态下没有差异。

首先,定义节点 i 的基本信息为 $R_i = \langle nr_i, nt_i \rangle$, 节点 i, j 感知信息差异值为 $\theta_{i,j}$, 因此假设其信息差异函数如下:

$$\theta_{i,j} = f(d_{i,j}, d_i, d_j, R_{i,j}) \quad (1)$$

其中: $R_{i,j} = \langle R_i, R_j \rangle$ 表示着节点 i, j 与事件源的位置关系; $d_{i,j}$ 表示节点 i, j 的距离; d_i, d_j 分别表示节点 i, j 到事件源的距离。这个差异函数 f 提供了差异的边界值,保证在同一

个事件源下的一致性。在这个方法中,每个节点都知道这个边界的差异函数,可以利用这个函数来检查它的邻居节点的数据信息的合法性。

3 基于环状相关性的安全防御机制

节点间的空间相关性由于两两节点的距离远近和位置摆放,以及数据信息有着最大差异和最小差异,故很容易导致恶意节点俘获到用户节点,在空间相关性认同的最大差异与最小差异数据信息之间进行数据伪造,故用户很难发掘出恶意节点,这为恶意节点下一步侵略用户节点做出了铺垫。这样,对于整个无线传感器网络而言,传感器节点的数据信息没有任何安全可言。

为了更好地避免这类事件的发生,本文提出一种无线传感器网络系统的信任相关性的过滤机制。在无线传感器网络中,假设下游节点 sink 是正常的,然后让这个区域的每个传感器节点都能相互传递数据信息、路径信息、与事件源之间的关系等具体数值。通过检查所采集数据的信任^[13-15]一致性来实现安全的数据融合。这样,就能过滤掉虚假数据或者不一致的数据实现下一步的数据融合。

首先,当两个邻近节点 i, j 在同时观测一个事件源信息时,对于节点 i 来说,如果成功感知到事件源信息,且信息值与节点 j 相差不大,则节点 i 的成功次数加1,即 $ns_i = ns_i + 1$ 。对于检查节点 i 的感知数据的一致性问题,这是考虑数据的信任评估,它的一致性检查过程如下:

当 $0 \leq nr_i - nr_j \leq \theta_{i,j}$ 时, $cn_i = cn_i + 1$, 且 $nt_i = nt_j$; 当 $nr_i - nr_j < 0$ 或 $nr_i - nr_j > \theta_{i,j}$ 时, $in_i = in_i + 1$ 。

同样地,当两个邻近节点 i, j 感知事件源信息同时失败,对等地,两者感知信息失败价值次数会增加,即 $nf_i = nf_i + 1$ 与 $nf_j = nf_j + 1$ 。

对于节点的单个信任价值因子是否一致性作出判决,由 -1 和 $+1$ 表示, -1 和 $+1$ 分别各自代表不一致性与一致性。节点信任价值因子与周围邻近节点相关,对于单个信任评估因子的具体过程如下所示:

1) 一致性价值:

$$C_i = \frac{cn_i - in_i}{cn_i + in_i}; C_i \in [-1, 1] \quad (2)$$

2) 感知通信价值:

$$N_i = \frac{ns_i - nf_i}{ns_i + nf_i}; N_i \in [-1, 1] \quad (3)$$

3) 电池使用寿命值:

$$B_i \in [0, 1]$$

信任评估因素是信任评估的步骤,定义 W_i 为各个重要因素的权重,范围为0到+1,它与实际应用场所息息相关。节点 i 的信任估计价值由下面等式计算:当 $B_i \neq 0$ 时,

$$T_i' = \frac{W_1 C_i + W_2 N_i + W_3 B_i}{\sum_{i=1}^3 W_i} \quad (4)$$

其中 $W_i \in (0, 1]$; 当 $B_i = 0$ 时,传感器节点已经停止工作,故此时 $T_i = -1$ 。在信息聚集,环状模型的信息聚集基于每个节点的信任评估,为了聚集信息,把所有节点信息聚集在下游节点 sink 上,如图2所示。

又由于节点信息信任评估是聚集所有相邻节点信息的评估,且针对环状空间模型,节点都在同一个区域内,故能相互接收信息,任意节点在这些节点中占其一份,故得出下面的公式:

$$T_i = \frac{T_i'}{\sum_{j=1}^k (T_j + 1)} \quad (5)$$

其中 k 为能互相通信节点个数,无线传感器网络聚合着每一个成员节点的信任值。因为信息聚集是基于节点的信任值,恶意节点或妥协节点的虚假信息信任值低于常态节点,故可以自然地排除在外。通过这种机制,能够进一步排除其他相对虚假或恶意的信息,得到更准确的数据。文献[10]中给出的失真函数定义如下:

$$D(M) = \sigma_s^2 + \alpha^2 - 2 \frac{\sum_{i=1}^M E_i \left(\frac{\rho(s,i) \sigma_s^4}{\sigma_s^2 + \sigma_N^2} + \alpha a_i \right)}{\sum_{i=1}^M E_i^2} + \frac{\sum_{i=1}^M \sum_{j \neq i}^M E_i E_j \left[\frac{\rho(i,j) \sigma_s^6}{(\sigma_s^2 + \sigma_N^2)^2} + a_i a_j \right]}{\left(\sum_{i=1}^M E_i^2 \right)^2} \quad (6)$$

其中:节点之间的相关系数 $\rho(i,j)$ 、节点与事件源之间的相关系数 $\rho(s,i)$; σ_N^2 和 σ_s^2 分别为节点 i 的信息值的统计方差和噪声方差; α 是事件信息的期望; E_i 为 $e^{-\alpha d_i^q}$ 。其机制算法描述如下:

Input: all M matters generated by the Matlab or the NS-2 simulations

For 异常事件域 do

While ($B_i \neq 0$)

计算 $T_i, \forall i$;

If $F(T_i) \geq \sigma$;

计算 $D(M)$;

end

end

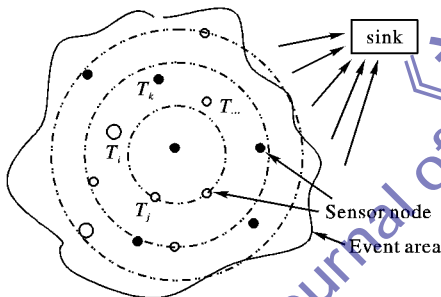


图2 安全防御机制的信息聚集

4 仿真实验与分析

针对传感器网络的异常监测应用,在实验中模拟了一个异常的温度源,此时模型选取参数 $\theta = 2$, 在一个半径为 500 单位长度的圆里面随机部署 50 个或更多传感器节点,事件源位于圆心,节点分别处于以事件源为中心的同心圆上面,然后能量衰减模型的参数分别取 $\alpha = 0.01$ 和 $\alpha = 0.05$ 。对于一个固定的网络拓扑结构,代表节点从这些节点中随机选取,对每个数目的代表性节点随机选 1000 次并分别根据代表性节点的位置利用公式计算出失真度,然后将这 1000 次的结果取平均值作为对应此数目代表性节点的平均失真度,结果如图 3。

图 3 分别描述了能量衰减模型在参数 $\alpha = 0.01$ 和 $\alpha = 0.05$ 下的失真度分布,从中可以看出,当代表节点数大于 30 时,经过机制改进后的各失真度都有所好转,但是效果不是很明显。但是,从图 4 可以看出受恶意节点攻击后的场景下,当代表节点数大于 20 时,经过机制改进后的各失真度明显优于之前。所以当事件区域的各节点受恶意节点攻击时,本文提出的安全防御机制能够有效抵御虚假信息,提高信息安全性。

当所选择的代表节点百分比 σ 不同时,所得出的结果也不同,如图 5 所示。在图 5 中,同样能量衰减模型的参数为

$\alpha = 0.01$ 和 $\alpha = 0.05$, 可以看出 $\sigma = 80\%$ 时优于选取所有节点,而 $\sigma = 50\%$ 时优于 $\sigma = 80\%$ 。这说明节点选取百分比越小,即 σ 值越小,其失真度越低,信息越准确。

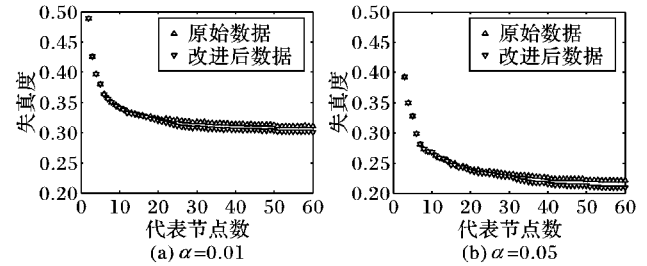


图3 正常状态下的相关性失真度分布

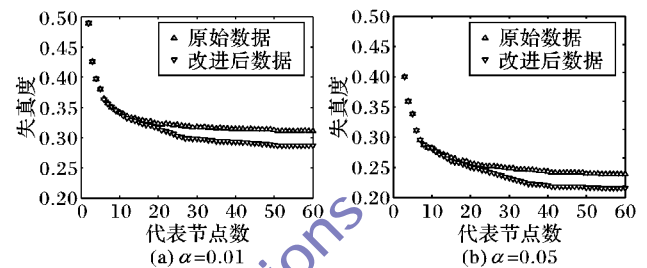


图4 受恶意节点攻击的相关性失真度分布

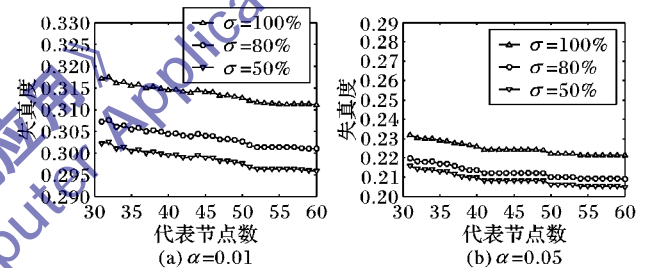


图5 不同 σ 值的失真度比较

5 结语

节点数量众多且分布稠密的传感器网络内部产生的数据中存在着很强的空间相关性。传感器网络中的空间相关性模型能探求网络中空间相关性。然而这样的空间相关性,很有可能发生传感器节点被敌方节点所俘获,产生虚假信息,从而对系统信息安全造成威胁。本文提出的一种基于 WSN 相关性的信息安全防御机制,通过节点与节点之间的信息相互影响,并将节点信任结合起来,可以很好地过滤掉虚假信息,很大程度上提高了系统的信息安全,使传递接受的信息更加准确。

参考文献:

- [1] 李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的概念、问题与进展[J]. 软件学报, 2003, 14(10): 1717-1727.
- [2] KARL H, WILING A. Protocols and architectures for wireless sensor networks[M]. New Jersey: Wiley, 2005.
- [3] CARDONE G, CORRADI A, FOSCHINI L. Reliable communication for mobile MANET-WSN scenarios[C]// IEEE Symposium on Computers and Communications. Piscataway: IEEE, 2011: 1085-1091.
- [4] 李平, 林亚平, 曾玮妮. 传感器网络安全研究[J]. 软件学报, 2006, 17(12): 2577-2588.
- [5] 裴庆祺, 沈玉龙, 马建峰. 无线传感器网络安全技术综述[J]. 通信学报, 2007, 28(8): 113-122.
- [6] VURAN M C, AKAN Ö B, AKYILDIZ I F. Spatio-temporal correlation: theory and applications for wireless sensor networks[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking — Special issue: In memory of Olga Casals, 2004, 45(3): 245-259.

法;对于 P@N 指标,ERM 在手枪类模型、吉他类模型、城堡类模型优于其他两种方法,在人脸类模型、椅子类模型、恐龙类模型、鱼类模型、鸟类模型均与另两种方法中的一种检索效果持平;对于 AP 指标,ERM 在人脸类模型、吉他类模型、鸟类模型均优于其他两种方法,在鱼类模型与 D2 形分布法检索效果持平。

表4 三种方法在九类模型下的五种评价指标结果

类别	方法	FT	ST	DCG	P@N	AP
人脸	ERM	0.84	0.84	98.81	0.06	0.98
	RM	0.84	0.84	98.09	0.06	0.97
	D2_SD	0.47	0.57	82.40	0.11	0.96
花	ERM	0.15	0.30	17.48	0.5	0.67
	RM	0.07	0.15	14	0.5	1
	D2_SD	0.23	0.23	20.04	0.33	0.58
椅子	ERM	0.30	0.46	25.06	0.2	0.61
	RM	0.15	0.23	27.13	0.5	1
	D2_SD	0.31	0.46	26.66	0.2	0.67
手枪	ERM	0.37	0.56	43.27	0.17	0.63
	RM	0.19	0.5	36.33	0.25	0.79
	D2_SD	0.16	0.13	17.5	0.5	0.56
吉他	ERM	0.68	1	73.56	0.07	0.98
	RM	0.75	0.93	73.34	0.07	0.95
	D2_SD	0.43	0.56	46.16	0.11	0.64
城堡	ERM	0.18	0.36	16.78	0.25	0.58
	RM	0.18	0.27	18.3	0.33	0.83
	D2_SD	0.09	0.09	12	1	1
恐龙	ERM	0.44	0.44	21.13	0.25	0.81
	RM	0.44	0.44	15.01	0.25	0.58
	D2_SD	0.11	0.11	10	0.33	1
鱼	ERM	0.69	0.77	54.55	0.1	0.99
	RM	0.69	0.77	53.85	0.1	0.94
	D2_SD	0.31	0.31	40.07	0.25	1
鸟	ERM	0.26	0.315	54.32	0.2	0.68
	RM	0.26	0.26	43.94	0.2	0.57
	D2_SD	0.21	0.42	27.11	0.25	0.41

4 结语

本文针对传统的射线法存在的不足,提出了扩展射线法。实验选择通用的普林斯顿大学的三维模型库,而且选取的类别所含面片数从数百到数万,能较好地覆盖不同面片的三维模型。10 组实验结果均表明本文方法的性能稳定,在大多数类别上优于原始射线法,但在有些类别,扩展射线法的效果反

而不足。这说明 D2 形分布、原始射线法以及扩展射线法均不能对所有类别得到较好的检索结果,而扩展射线法在多数类别上优于其他两种,所以对于三维模型的粗分类可以此方法。下一步计划结合机器学习方法建立人工监督机制,通过反馈机制得到更好的检索结果。

参考文献:

- [1] 徐世彪,车武军,张晓鹏. 基于形状特征的三维模型检索技术综述[J]. 中国体视学与图像分析, 2010, 15(4): 439-450.
- [2] 崔晨阳,石教英. 三维模型检索中的特征提取技术综述[J]. 计算机辅助设计与图形学学报, 2004, 16(7): 882-889.
- [3] 周明全,耿国华,韦娜. 基于内容图像检索技术[M]. 2 版. 北京:清华大学出版社, 2007: 179-183.
- [4] 杨育彬,林琛,朱庆. 基于内容的三维模型检索综述[J]. 计算机学报, 2004, 27(10): 1287-1310.
- [5] OSADA R, FUNKHOUSER T, CHAZELLE B, et al. Shape distributions[J]. ACM Transactions on Graphics, 2002, 21(4): 807-832.
- [6] 杨少博. 基于视觉图像的三维模型检索与语义标注技术研究[D]. 西安:西北大学, 2010.
- [7] 张明,李娟. 改进的三维模型形状分布检索算法[J]. 计算机应用, 2012, 32(5): 1276-1279.
- [8] 刘玉杰,张晓冬,李华. 正交样条矩与三维模型检索[J]. 计算机辅助设计与图形学学报, 2009, 21(7): 968-972.
- [9] VRANIC D, SAUPE D. 3D model retrieval [C]// SCCG 2000: Proceedings of Spring Conference on Computer Graphics. Budmerice, Slovakia: [s. n.], 2000: 89-93.
- [10] 王慧玲. 基于小波变换的三维模型特征提取技术的研究与实现[D]. 长春:东北师范大学, 2011.
- [11] SUZUKI M T, KATO T, OTSU N. A similarity retrieval of 3D polygonal models using rotation invariant shape descriptors [C]// Proceedings of IEEE International Conference on Systems, Man, and Cybernetics. Piscataway: IEEE, 2000: 2946-2952.
- [12] 孙挺. 三维模型特征提取技术研究[D]. 西安:西北大学, 2011.
- [13] 邢玉辉. 几种重要的三维模型特征提取方法的实现研究[D]. 长春:吉林大学, 2006.
- [14] 王慧玲. 基于内容的 3D 模型检索概述[J]. 伊犁师范学院学报:自然科学版, 2010(3): 54-57.
- [15] 朱悠悠,赵晓飞,陈钰,等. 一种基于射线投影的球面调和检索算法[J]. 现代计算机:专业版, 2011(10): 28-30.
- [16] 张汝珍,王婉,周雄辉,等. 基于形状分布算法的三维模型相似性研究[J]. 计算机集成制造系统, 2007, 13(10): 1928-1933.
- [17] Performance measures used [EB/OL]. [2012-08-10]. <http://give-lab.cs.uu.nl/SHREC/shrec2007/performanceMeasures.html>.

(上接第 425 页)

- [7] VURAN M C, AKYILDIZ I F. Spatial correlation based collaborative medium access control in wireless sensor networks [J]. IEEE/ACM Transaction on Networking, 2006, 14(2): 316-329.
- [8] 程龙,陈灿峰,马建. 无线传感器网络中多移动 sink 的选择策略[J]. 通信学报, 2008, 29(11): 12-18.
- [9] AKKAYA K, YOUNIS M. A survey on routing protocols for wireless sensor networks [J]. Ad Hoc Networks, 2005, 3(3): 325-349.
- [10] 苏威,林亚平,尤志强,等. 无线传感器网络中一种环状空间相关性模型[J]. 计算机应用研究, 2008, 25(6): 1860-1863.
- [11] SSU K-F, WANG W-T, CHANG W-C. Detecting Sybil attacks in wireless sensor networks using neighboring information [J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2009, 53(18): 3042-3056.
- [12] 冯涛,马建峰. 防御无线传感器网络 Sybil 攻击的新方法[J]. 通

信学报, 2008, 29(6): 13-19.

- [13] ZHENG Y, ZHANG P, VIRTANEN T. Trust evaluation based security solution in Ad Hoc networks [EB/OL]. [2012-04-22]. http://www.citmo.com/library/Trust_Evaluation_Based_Security_Solution_in_Ad_Hoc_Networks.pdf.
- [14] RYUTOV T, NEUMAN C. Trust based approach for improving data reliability in industrial sensor networks [C]// IFIP International Federation for Information Processing Volume, IFIP 238. Boston: Springer-Verlag, 2007: 349-365.
- [15] LAVRATTI F, PINTO A R, BOLZANI L, et al. Evaluating a transmission power self-optimization technique for WSN in EMI environments [C]// 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools. Piscataway: IEEE, 2010: 509-515.