Website: ycyk.brit.com.cn Email: ycyk704@163.com

无线传感器网络中故障节点检测与修复方法综述*

卢晓艳[1,2]，颜培玉[1]，解志斌[1,2]，毛云龙[1,2]，徐 桧[1,2]，刘民东[1,2]
（1 江苏科技大学电子信息学院 镇江 212003
2 镇江市智慧海洋信息感知与传输实验室 镇江 212003）

摘要：无线传感器网络 WSNs（Wireless Sensor Networks）的网络故障节点问题已引起人们的极大关注。针对这个问题，将修复方法分为可连通情境下修复和非连通情境下修复，并将二者进行对比分析，对不同类型的故障节点检测算法进行了归纳，最后对无线传感器网络中故障节点检测与修复的发展进行展望。

关键词：无线传感器网络；故障类型；故障检测；修复

中图分类号：TN92 **文献标识码：**A **文章编号：**CN11-1780(2021)04-0012-08

DOI：10.12347/j.ycyk.20210422001

引用格式：卢晓艳，颜培玉，解志斌，等. 无线传感器网络中故障节点检测与修复方法综述[J/OL]. 遥测遥控, 2021, 42(4): 104–111[20XX-XX-XX]. http://ycyk.brit.com.cn/ycyk/article/abstract/20210422001.

Overview of fault node detection and repair in wireless sensor networks

LU Xiaoyan[1,2], YAN Peiyu[1], XIE Zhibin[1,2], MAO Yunlong[1], XU Hui[1,2], LIU Mindong[1,2]
（1. School of Electronic and Information, Jiangsu University of Science and Technology, Jiangsu 212003, China;
2. Intelligent Marine Information Sensing and Transmission Laboratory, Jiangsu 212003, China）

Abstract: The problem of network node failure in wireless sensor networks (WSNs) has attracted great attention. Aiming at the problem, this paper divides the repair methods into connected and non-connected situations to compare and analyze, and summarize different types detection algorithms of fault node, trying to predict the trends of fault node detection and repair in wireless sensor networks.

Key words: Wireless sensor networks; Types of nodes; Fault detection; Repair

DOI：10.12347/j.ycyk.20210422001

Citation: LU Xiaoyan, YAN Peiyu, XIE Zhibin, et al. Overview of fault node detection and repair in wireless sensor networks [J/OL]. Journal of Telemetry, Tracking and Command, 2021, 42(4): 104–111[20XX-XX-XX]. http://ycyk.brit.com.cn/ycyk/article/abstract/20210422001.

引 言

1996 年，美国加州大学洛杉矶分校 William J Kaiser 教授向美国国防高级研究设计计划局提交“低能耗无线集成微型传感器”研究建议书，自此揭开了现代无线传感器网络 WSNs（Wireless Sensor Networks）的序幕。WSNs 较传统通信网络有其独特优势，一经提出即受到各方强烈关注。由于 WSNs 一般部署于恶劣的环境，在军事上用于检测双方军力、地方部署以及物资等重要军事信息，甚至有些传感器节点负责监控打击目标或者发射目标[1]；在民用中用于检测温度、湿度或者是工作情况[2]。

随着 WSNs 的应用越来越广泛和复杂，网络中节点的数量随之增加，故障节点产生的概率越来越高[3]，能否保障网络正常运行变得越来越重要。一旦发生网络故障，技术人员必须尽快对故障节点进行故障类型检测并实施修复，否则有可能造成更大面积的网络瘫痪，最终对整个网络造成不可挽回的损害。

本文将故障节点的修复工作分为两个主要部分进行归纳和总结，即：可连通情境下修复和非连通情

*基金项目：国家自然科学基金（61871203）；江苏省研究生科研与实践创新计划资助项目（KYCX21_3480）
收稿日期：2021-04-22 收修改稿日期：2021-05-11

境下的修复。

1　可连通情境下修复

在 WSNs 中，有些故障节点仍然处于能与其他节点相互连通的范围内，可将这类型故障节点划分为不良节点、恶意节点、自私节点和失效节点等，如图 1 所示。基于上述不同的故障节点类型，可利用不同的检测方法检测出故障节点类型，再对其进行相应的修复。

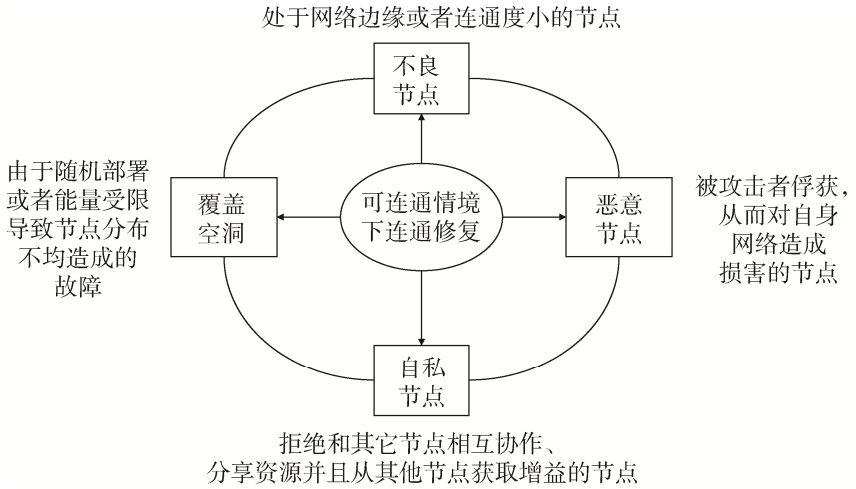

图 1　可连通情境下连通修复类型示意图

Fig. 1　Schematic diagram of connectivity repair types in connectable scenarios

1.1　不良节点的检测与修复

按照节点分布的位置和节点的连通度，可以将位处边缘或连通度小的节点称为不良节点。其中，处于 WSNs 覆盖区域边缘的不良节点，由于网络中可能没有与之邻近连通的节点，而无法进行有效的通信。

根据不良节点的定义常将其分为边缘节点和亚孤立节点。通常把节点满足边界且节点的度小于网络平均连通度的节点标记为边缘节点，其中，边界是指 WSNs 覆盖区域具有最大偏心距的节点组成的集合。当节点的连通度小于网络平均连通度时，将其标记为亚孤立节点[4]。针对边缘节点和亚孤立节点的检测，有很多不一样的检测方法。如 ZHANG Chi 等人[5]基于局部 Voronoi 多边形检测节点是否处于网络边缘位置，通过将节点分为簇群的边缘节点和内部节点，并判断任意节点所属簇群，若不在簇群内则为边缘节点。AHMED N 等人[6]提出了利用右手法则的方法来判断处于边界的节点。XU Lianming 等人[7]提出了基于图论的原理和方法对边缘节点和亚孤立节点进行判断，根据分析节点密度、接收锚节点的范围和方向提出了判断边缘节点和亚孤立节点的方法。DABBA A 等人[8]提出了一种边缘覆盖协议 BCP（Border Coverage Protocol），在协议内容中通过定义一个区域，将没有完全属于这个区域的节点判定为边缘节点。综合上述文献可得，不良节点的检测方法大多都是针对节点所处位置和周围节点密度进行判断，从而确定其是否为不良节点。

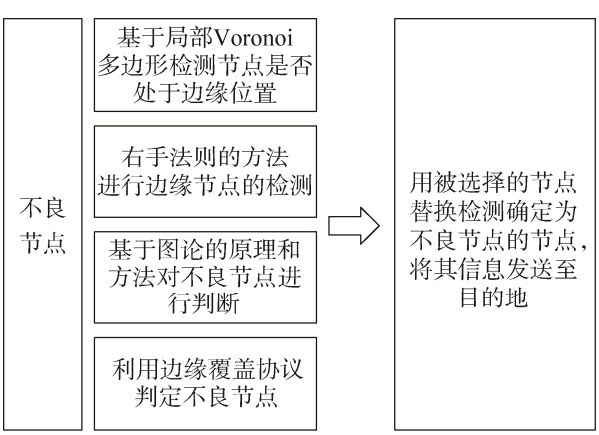

图 2　不良节点检测方法及修复示意图

Fig. 2　Misbehavior nodes detection method and repair schematic diagram

当确定为不良节点并且确定其故障节点所处位置后，在修复过程中，将节点传送的信息分为三种类型，根据节点接收信息的不同可以将节点分为四种状态（监听、被动、主动和退出服务），通过节点接收到的信息检测是否有可能的节点能替换掉原来出现故障的节点，如果可以，则通过其将信息发送至目的节点，以此达到修复不良节点的目的。其中，整体修复流程示意如图 2 所示。实验证明，该方法在修复过程中有关的覆盖率和边界覆盖率均有显著增加。

1.2　恶意节点的检测与修复

恶意节点属于一种被攻击者俘获从而对自身

网络造成损害的节点[9]，这类节点在网络中会被实施窃听、删除或者毁坏数据包[10]等恶意行为。如黑洞攻击和灰洞攻击，会造成 WSNs 的通信安全与通信质量受损。更有甚者，可以通过伪装对网络中节点的信息以及数据进行修改和欺骗[11,12]，以此造成 WSNs 的重大故障和损失。

在开放性部署环境中[13]，内部网络很难阻止外来攻击者的侵入，并有可能被窃取通信密钥。此时可能会出现恶意节点，这些节点会伪装成内部节点进行通信，从而大幅降低了网络的安全性与有效性。在这种情况下，CHO Y 等人[14]提出了用来检测恶意节点的看门狗机制。但是看门狗机制存在明显的限制，诸如，节点传播能力有限时不能发送数据到达目的位置或者在模棱两可的传输情况时不能准确判定异常节点，从而无法检测出行为异常的节点。在文献[15]和文献[16]中，NII E 等人提出了利用协作节点进行恶意节点的识别检测：利用协作节点对发射节点和多跳节点传输的信息进行比较，以此判断该节点是否为恶意节点。实验表明该方法能保持较高的检测率，并能在后期的修复过程中清除所有恶意节点。在文献[17]中 GOMATHI S 等人提出了一种安全数据聚合协议 SDAP（Secure Data Aggregation Protocol），该协议通过以树状拓扑结构的形式提供了一个逻辑组来识别恶意节点。GOMATHY V 等人提出了基于异构聚类的安全路由协议 HCBS（Heterogeneous Cluster Based Secure Routing Protocol），并在此基础上设计了基于信任的安全网络，用于检测网络中的恶意节点[18]。还有其他检测恶意节点的方法，如可以检测任意类型恶意节点的方法[19]和基于信誉投票合作机制的恶意节点检测算法[20]。除此之外，还有人提出了可以提高恶意节点检测效率的方法[21]。文献[14]~文献[21]提供的检测方法都是对于恶意节点的检测，文献[13]提出了对于恶意攻击后产生的安全事件进行检测，此时检测的不只是单个的恶意节点，而是恶意节点攻击后受影响的某个区域。检测方法特点对比见表 1。

表 1　恶意节点检测方法比较

Table 1　Comparison of malicious node detection methods

方法名称	检测恶意伪装节点	检测恶意节点攻击	检测任意类型恶意节点	检测恶意事件	优缺点
看门狗机制	√				能进行伪装检测，但是存在由于恶意节点破坏导致误判
基于异构聚类的安全路由方案	√	√			该检测恶意节点方法准确率高达百分之九十六，能耗低至百分之十
协同节点检测	√				能够检测出相邻恶意节点，或者两跳内恶意节点
安全数据聚合协议	√				安全聚合数据，提高数据聚合率
任意类型恶意节点检测算法	√	√	√		在算法执行过程不会引起任何额外能耗、开销和复杂性
基于信誉投票合作机制的恶意节点检测算法	√				利用基站广播控制信息给所有节点，对所有节点进行检测
恶意事件检测算法		√		√	可以检测和抵御多个被破坏的传感器节点

由于 WSNs 的工作特点，大多数节点部署在开放性环境中，用以监测外在环境或者其它因素，所以极有可能受到外界攻击而形成恶意节点。解决方法可以分为两类：① 经过检测确定为恶意节点，通过逻辑隔离和内部票选的方式将恶意节点进行隔离；② 在恶意节点发生前就进行预防，如利用卷积码生成安全比特的算法[22]。

1.3　自私节点的检测与修复

在 WSNs 中，节点可利用的资源有限，有些节点为了节约自身能量，在网络中不与其它节点相互协作，拒绝分享自身的资源，却从其它节点获取增益，这类节点称之为自私节点亦可称为贪婪节点[23]。

在文献[24]中将自私节点分为四类：① 不发送问候信息；② 不转发问答信息；③ 转发问答信息，但是延时转发；④ 不转发数据包。这四种行为会使其它节点传输数据时为了绕过这些自私节点而更换

为更远的路径，导致了能量和传输带宽的浪费，并使得数据包的传输率降低[25]。有时，自私节点不转发信息或者数据也会导致网络无法进行正常信息传递，故而，自私节点也是一类比较常见并且严重的故障节点。

自私节点在 WSNs 中接收其他节点的信息但不转发信息，以此来为自己保存资源。这类节点行为对系统的性能有很大影响，WU L 等人[26]讨论了不转发问答信息和不转发数据包信息情况下自私节点的检测，并对这两种情况设计了两种算法进行检测，通过计算检测率 $DR = N_{sd}/N_{st}$（N_{sd} 为被检测出的自私节点个数，N_{st} 为总自私节点个数）和错误检测率 $DR = N_{msd}/N_{nt}$（N_{msd} 为被错误检测为自私节点的正常节点个数，N_{nt} 为总的正常节点的个数）来检测出自私节点，该实验显示，当节点移动率较高时，误检率能够降低至 10%[26]。经过总结可以发现，大多数检测方法都是通过建立信任机制对自私节点进行检测，检测侵入信任机制或者获取自私节点的信任值，以此判断节点是否为自私节点[27-30]。根据判断流程进行总结，可得基于信任值的自私节点判定流程，如图 3 所示。

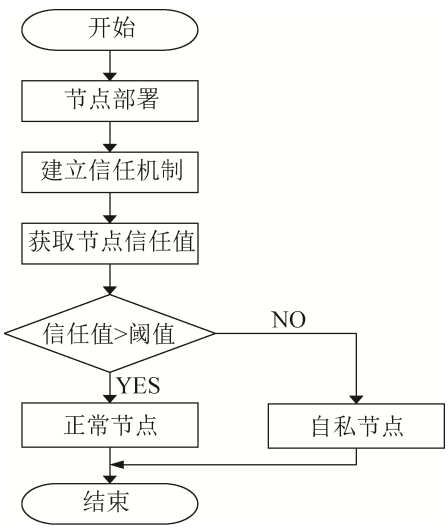

图 3　基于信任值的自私节点判定流程

Fig. 3　Selfish node determination process based on trust value

如果通过检测方法检测出故障节点为自私节点，则可以分为两种方法处理（如大多数方法）：一是直接将其排除出网络；二是将其转化为正常节点，以此增大原本网络的吞吐量。通过将自私节点转变为发送或转发节点重新获取信任值，从而变成正常节点，以此达到修复自私节点故障和提高原有网络吞吐量的目的[31]。

1.4　覆盖空洞的检测与修复

由于 WSNs 的节点大多数是随机部署和能量受限的，因此可能导致网络节点部署不均匀问题，形成网络覆盖空洞。覆盖空洞分为大范围空洞和小范围空洞，二者的区分如图 4 所示。

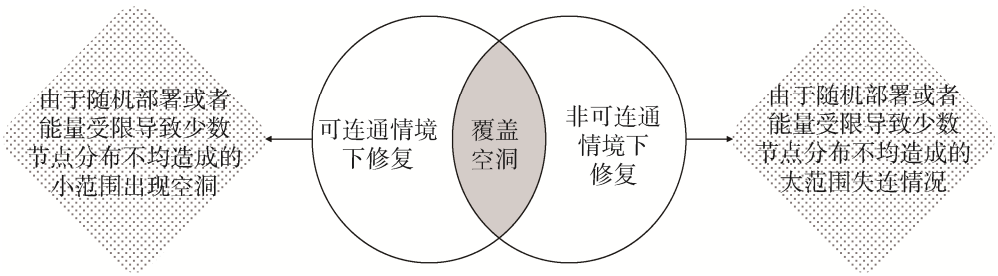

图 4　覆盖空洞区分图

Fig. 4　Comparison chart of coverage hole

已有很多研究者提出了覆盖空洞检测算法，诸如：分布式节点选择算法、分布式覆盖空洞检测算法和基于 WSNs 的简单距离公式计算最小传输信息量的覆盖空洞检测算法等[32-34]。总结可知，覆盖空洞的检测大多采用分布式的检测算法，除此之外，还有一些其他非算法的分布式检测方法，如：基于孔径的检测方法和利用基于孔径管理器的多目标优化算法[35,36]等方法。

如果节点是由于随机部署、能量耗尽提前死亡或者其他环境原因出现的覆盖空洞，可以通过 K 最近邻算法 KNN（K-Nearest Neighbor）选择备份节点，然后对备份节点进行唤醒，以此替换发生故障的节点。实验显示，该方法能够快速修复节点，并且提高传感器网络的容错率[37]。DENG X[38]等人提出了一个最佳匹配节点的策略解决覆盖空洞这类失效节点问题，通过选择最近的不活跃的节点进行激活，然后移动到目的地修复覆盖空洞。在文献[39]中，利用移动节点的移动特性，采用泰森多边形原理判断网络中的边界节点，依据边界圆弧进行覆盖空洞的动态完全修复。总结后可以发现，覆盖空洞的修复可以分

为两个阶段，即：① 进行覆盖空洞区域大小的确定；② 确定最优化部署覆盖空洞的面积。在这两个阶段中都可以进行优化处理，前期处理就是寻求最优覆盖空洞的面积，后期实际上是优化修复面积与最小化重叠面积。当然，还可以采用优化算法进行修复，诸如采用邻居节点介入的快速修复算法[40]。

2　非连通情境下修复

在 WSNs 中，多个节点失效时可能导致分支断裂问题[41]以及大范围空洞的覆盖空洞问题。这些问题将使得原始节点网络中部分网络节点失去连通，从而有可能导致整个网络瘫痪。故而需要进行连通修复，以此减少经济损失。

对于多节点失效导致分支断裂的问题，主要是指网络节点由于受部署地环境等因素影响发生了移动，当网络节点被动移动至超出节点间最大连通范围时，移动后的网络节点将不能与网络进行通信。这类场景多发生在水面部署环境，当网络节点受水流、风力等原因漂移超出连通范围时，会导致网络节点间连通中断，或是损失大量观测数据。

如图 5 所示，为节点受漂移影响失去连通的示意图，部分节点受环境影响从 A 部分脱离并漂移至 B 位置，B 在 A 的连通范围之外。在文献[42]中，作者将类似 B 漂移模型定义为群组移动模型[43-44]，为了使 A 和 B 相互连通起来，在图中所示的可部署区域构建连通路径。通过不同的目标函数可以得到不同的连通路径。诸如，构建最短连通路径 $\min(d_{ij})$，然后计算得出最少的节点数 $N_{\min}$ 为：

$$N_{\min}=\mathrm{ceil}\left[\frac{\min\left(d_{ij}\right)}{r}\right]^{+}-1 \tag{1}$$

其中，ceil 为向上取整函数，r 为节点的最大通信距离，d_{ij} 为第 i 和第 j 个不同位置两个节点间的距离。通过传输数据损耗模型确定传输路径转发数据所消耗的最小总能量为：

$$\min\left(E_{\mathrm{total}}\right)=\left(m+1\right)\cdot k\cdot\alpha_0\cdot\left[\frac{\min\left(d_{ij}\right)}{N_{\min}+1}\right]^2 \tag{2}$$

其中，E_{total} 为传输路径损耗总能量，m 为移动节点，k 是一个常数，α_0 表示传输的数据量。由上式可得最短可选连通路径 b，如图 6 所示。同时，也可基于其它的目标函数得到诸如可选路径 a 和 c 等，从而实现漂移节点与原网络间的再连通部署，修复不可连通故障。

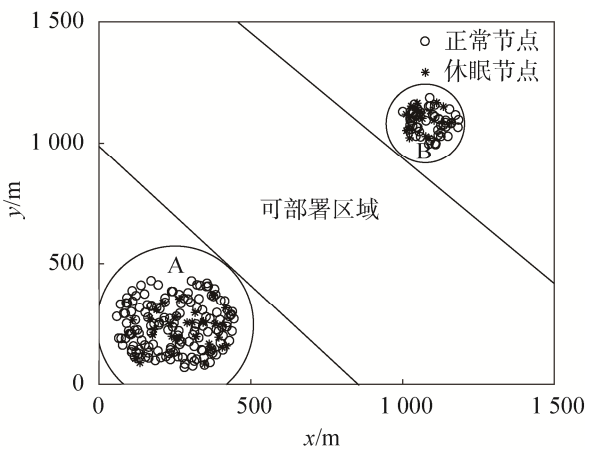

图 5　节点经漂流失去连通图

Fig. 5　Nodes lose the connected graph by drifting

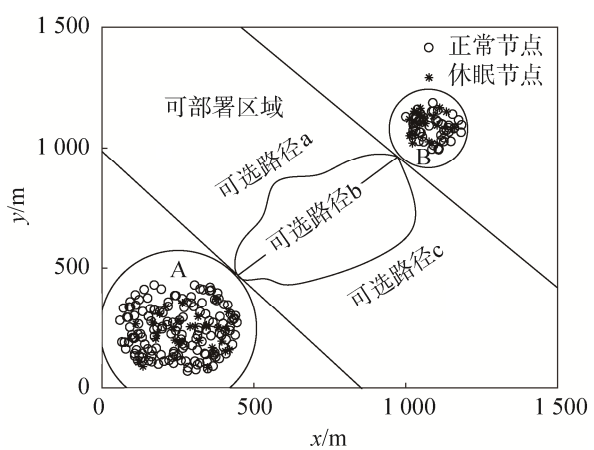

图 6　节点修复后连通图

Fig. 6　Connected graph after node repair

3　结束语

随着 WSNs 在军事和民用方面应用的普及，对其可靠性的要求也越发严苛。WSNs 的节点问题已受到越来越多研究者的关注，总结而言，主要涵盖节点故障类型检测以及故障修复这两个方面。虽然现有

的检测方法准确率很高，但是，修复方案中仍然存在如下一些问题亟待解决：

① 覆盖空洞修复中仍然存在覆盖重叠面积，不能完全消除，浪费资源。

② 恶意节点处理仍然处于隔离处理阶段，依然对原有网络结构和传输路径有影响，甚至导致资源损耗。

③ 失效节点处理过程中建立的连通路径易受环境影响造成二次失效。

为此，在未来工作中，可以依据现有的问题进行进一步的研究，以此提高节点修复的资源利用率和修复后的稳定性，满足实际应用的可靠性需求。

参考文献

[1] 刘志坤, 刘忠, 夏清涛, 等. 基于网格划分的无线传感器网络多重覆盖算法[J]. 火力与指挥控制, 2014, 39(11): 80–83, 88.
LIU Zhikun, LIU Zhong, XIA Qingtao, et al. Multi-coverage algorithm based on grid-plotting in WSN[J]. Fire Control & Command Control, 2014, 39(11): 80–83, 88.

[2] 赵宏程, 王旭阳, 王野, 等. 无线传感器网络的研究现状及发展趋势[J]. 科技广场, 2011(9): 77–80.
ZHAO Hongcheng, WANG Xuyang, WANG Ye, et al. Research status and developing trends of wireless sensor networks[J]. Science Mosaic, 2011(9): 77–80.

[3] ZORGUI M, WANG Z. Centralized multi-node repair in distributed storage[C]. Allerton Conference on Communication. IEEE, 2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, 2016: 617–624.

[4] 于宁, 万江文, 马万兴. 无线传感器网络中不良节点的判断与定位[J]. 高技术通讯, 2009, 19(3): 219–223.
YU Ning, WAN Jiangwen, MA Wanxing, et al. Judgment and location of misbehavior nodes in wireless sensor networks[J]. Chinese High Technology Letters, 2009, 19(3): 219–223.

[5] ZHANG Chi, ZHANG Yanchao, FANG yuguang. Detecting coverage boundary nodes in wireless sensor networks[C]. 2006 IEEE International Conference on Networking, Sensing and Control, Ft. Lauderdale, FL, 2006: 868–873.

[6] AHMED N, KANHERE S S, JHA S. Efficient boundary estimation for practical deployment of mobile sensors in hybrid sensor networks[C]. 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Vancouver, BC, 2006: 662–667.

[7] XU Lianming, RUAN Fengli, DENG Zhongliang, et al. Recognition and localization of boundary and isolated nodes in wireless sensor networks[C]. 2014 IEEE International Conference on Communication Problem-solving, Beijing, 2014: 111–114.

[8] DABBA A, BEGHDAD R. BCP: A border coverage protocol for wireless sensor networks[C]. 2014 Science and Information Conference, London, 2014: 632–640.

[9] 张宗福, 汤霖, 杨国威. 移动网络中恶意节点自动检测研究与仿真[J]. 计算机仿真, 2016, 3(7): 293–296.
ZHANG Zongfu, TANG Lin, YANG Guowei. Mobile network automatically detect malicious nodes in the research and simulation[J]. Computer Simulation, 2016, 3(7): 293–296.

[10] CHELANI P L, BAGDE S T. Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme[C]. 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016: 1–6.

[11] 杨治秋, 陈丽敏, 张丹. 无线传感器网络中基于邻域的恶意节点检测[J]. 湖北农业科学, 2020, 59(5): 142–144, 151.
YANG Zhiqiu, CHEN Limin, ZHANG Dan. Neighbor-based malicious node detection in wireless sensor networks[J]. Hubei Agricultural Sciences, 2020, 59(5): 142–144, 151.

[12] ZHOU Wenxiong, LIN Sui. Malicious node recognition algorithm in wireless sensor networks[J]. Computer Systems and Applications, 2020, 29(2): 175–180.

[13] ILLIANO V P, LUPU E C. Detecting malicious data injections in event detection wireless sensor networks[J]. In IEEE Transactions on Network and Service Management, 2015, 12(3): 496–510.

[14] CHO Y, QU G, WU Y. Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks[C]. 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012: 134–141.

[15] NII E, KITANOUMA T, ADACHI N, et al. Cooperative detection for falsification and isolation of malicious nodes for

wireless sensor networks in open environment[C]. 2017 IEEE Asia Pacific Microwave Conference (APMC), Kuala Lumpar, 2017: 521–524.

[16] KIMURA Y, NII E, TAKIZAWA Y. Cooperative detection for falsification and isolation of malicious nodes through inter-node vote for wireless sensor networks in open environments[C]. 2019 Global Information Infrastructure and Networking Symposium (GIIS), 2019: 1–3.

[17] GOMATHI S, KRISHNAN C G. Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol[J]. Wireless Personal Communications, 2020, 113(5): 1–16.

[18] GOMATHY V, PADHY N, SAMANTA D. Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks[J]. J Ambient Intell Human Computer, 2020, 11(21): 1–7.

[19] ALTHUNIBAT S, ANTONOPOULOS A, KARTSAKLI E. Countering intelligent-dependent malicious nodes in target detection wireless sensor networks[J]. In IEEE Sensors Journal, 2016, 16(23): 8627–8639.

[20] 崔慧, 潘巨龙, 闫丹丹. 无线传感器网络中基于信誉–投票机制的恶意节点检测[J]. 中国计量学院学报, 2013(4): 26–32.
CUI Hui, PAN Julong, YAN Dandan. Malicious node detection algorithm based on reputation with voting mechanism in wireless sensor networks[J]. Journal of China University of Metrology, 2013, (4): 26–32.

[21] YANG H, ZHANG X, CHENG F. A novel algorithm for improving malicious node detection effect in wireless sensor networks[J]. Mobile Networks and Applications, 2020, 25(3): 1–10.

[22] ALGHAMDI T. Convolutional technique for enhancing security in wireless sensor networks against malicious nodes[J]. Human-centric Computing and Information Sciences, 2019, 9(1): 1–10.

[23] 任智, 谭永银, 李季碧. 可靠的机会网络自私节点检测算法[J]. 通信学报, 2016, 37(3): 1–6.
REN Zhi, TAN Yongyin, LI Jibi. Reliable selfish node detection algorithm for opportunistic networks[J]. Journal on Communications, 2016, 37(3): 1–6.

[24] YOKOYAMA S, NAKANE Y, TAKAHASHI O, et al. Evaluation of the impact of selfish nodes in ad hoc networks and detection and countermeasure methods[C]. 7th International Conference on Mobile Data Management(MDM'06), Nara, Japan, 2006: 95–95.

[25] AIFA S, THOMAS Tibin. Review on Different Techniques used in Selfish Node Detection[C]. 2018 IEEE International Conference on Circuits and Systems in Digtal Enterprise Technology. IEEE, 2018: 1–4.

[26] WU L, YU R. A threshold-based method for selfish nodes detection in MANET[C]. 2010 International Computer Symposium (ICS2010), Tainan, 2010: 875–882.

[27] ULLAH Z, KHAN M S, Ahmed I, Javaid N, Khan M. I. Fuzzy-based trust model for detection of selfish nodes in MANETs[C]. 2016 IEEE 30th International Conference on Advanced Information Networking and Applications(AINA), Crans-Montana, 2016: 965–972.

[28] RAMA Abirami, SUMITHRA K, M. G. Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection[J]. Cluster Comput, 2019, 22(6): 13307–13316.

[29] KUMAR S, DUTTA K. Trust based intrusion detection technique to detect selfish nodes in mobile Ad Hoc networks[J]. Wireless Pers Commun, 2018, 101(4): 2029–2052.

[30] 赵建伟, 贾小珠, 裘文娟. Ad Hoc 网络基于信誉机制的自私节点检测[J]. 青岛大学学报: 自然科学版, 2016, 29(4): 64–68.
ZHAO Jianwei, JIA Xiaozhu, XI Wenjuan. The detection of selfish based on reputation mechanism in Ad Hoc networks[J]. Journal of Qingdao University(Natural Science Edition), 2016, 29(4): 64–68.

[31] MEERAN A, PRAVEEN A N, RATHEESH T K. Enhanced system for selfish node revival based on watchdog mechanism[C]. 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 2017: 332–337.

[32] RAFIEI A, ABOLHASAN M, FRANKLIN D, et al. Boundary node selection algorithms in WSNs[C]. 2011 IEEE 36th Conference on Local Computer Networks, Bonn, 2011: 251–254.

[33] LAO H. Y, DING Yi F. Coverage Hole Detection Algorithm Based on HPNs in WSN[C]. 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, 2018: 896–900.

[34] ALIOUANE L, BENCHAÏBA M. Efficient boundary detection of coverage hole in WSNs[C]. 2016 International

Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, 2016: 1–6.

[35] SINGH P, CHEN Y. Sensing coverage hole identification and coverage hole healing methods for wireless sensor networks[J]. Wireless Networks: The Journal of Mobile Communication, 2020, 26 (1): 2223–2239.

[36] JAIN, J K. A coherent approach for dynamic cluster-based routing and coverage hole detection and recovery in bilayered WSN-IoT[J]. Wireless Personal Communications, 2020, 114(1): 519–543.

[37] LI Weihong, SHEN Fanfan, CHENG Xiaohui. Research on node repair mechanisms in wireless sensor networks[C]. 2012 International Conference on Communication and Electronics Systems (ICCES). IEEE, 2012.

[38] DENG X, XU C, ZHAO F, et al. Repair policies of coverage holes based dynamic node activation in wireless sensor networks[C]. 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, 2010: 368–371.

[39] 张生凤, 徐志良, 吴晓蓓. 无线传感器网络覆盖空洞动态完全修复[J]. 南京理工大学学报: 自然科学版, 2013(6): 818–825.
ZHANG Shengfeng, XU Zhiliang, WU Xiaobei. Dynamic full repairing of coverage holes in wireless sensor networks[J]. Journal of Nanjing University of Science and Technology, 2013(6): 818–825.

[40] KHALIFA B, AGHBARI Z Al, KHEDR A. M, et al. Coverage hole repair in wsns using cascaded neighbor intervention[J]. IEEE Sensors Journal, 2017, 17(21): 7209–7216.

[41] 张生凤. 无线传感器网络中节点失效问题的修复策略研究[D]. 南京: 南京理工大学, 2016.

[42] 张生凤, 徐志良, 吴晓蓓. 移动无线传感器网络群组移动的连通性保证[J]. 中国科技论文, 2013, 8(7): 599–606.
ZHANG Shengfeng, XU Zhiliang, Wu Xiaobei. Research on keeping connectivity of group mobility in mobile wireless sensor networks[J]. China Encepaper, 2013, 8(7): 599–606.

[43] DU H, YU Z, YI F, et al. Recognition of group mobility level and group structure with mobile devices[J]. IEEE Transactions on Mobile Computing, 2018, 17(4): 884–897.

[44] NAGUIB K M, ALI A S, MAHMOUD K R. Group mobility-based optimization of cache content in wireless device-to-device networks[C]. 2018 14th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2018: 260–265.

[作者简介]

卢晓艳 1996 生，在读硕士研究生，主要研究方向为无线传感器网络。
颜培玉 1982 生，硕士，助理研究员，主要研究方向为模式识别与智能处理。
解志斌 1981 生，博士，教授，主要研究方向为通信信号处理、无线传感器网络。
毛云龙 1989 生，博士，讲师，主要研究方向为计算电磁学、天线设计。
徐 桧 1998 生，在读硕士研究生，主要研究方向为水下光通信。
刘民东 1996 生，在读硕士研究生，主要研究方向为水下物理层安全。

(本文编辑：潘三英)