

无线传感器网络抗毁性

李文锋 符修文

(武汉理工大学物流工程学院 武汉 430063)

摘 要 无线传感器网络常因能量耗尽、硬件故障或者遭遇入侵等原因导致节点失效,使得原本连通的网络拓扑分割,甚至导致全局网络受损.因此,研究抗毁性对解决无线传感器网络规模化应用瓶颈具有重要的理论价值.目前有关无线传感器网络抗毁性的研究主要关注以下 3 个方面:(1)造成无线传感器网络节点失效与网络受损的原因有哪些;(2)如何准确度量无线传感器网络抗毁性;(3)如何有效提升无线传感器网络抗毁性能.文中有针对性地分别从失效成因、测度、提升策略与故障检测和修复等 4 个方面对有关研究进行归纳和分类,重点分析无线传感器网络抗毁性优化方法,包括路由控制、网络重构和拓扑演化.最后,指出无线传感器网络抗毁性研究未来发展所面临的技术挑战,并就其发展趋势进行探讨.

关键词 无线传感器网络;抗毁性;路由控制;网络重构;拓扑演化;故障检测与修复

中图法分类号 TP393 **DOI号** 10.3724/SP.J.1016.2015.00625

Survey on Invulnerability of Wireless Sensor Networks

LI Wen-Feng FU Xiu-Wen

(School of Logistics Engineering, University of Wuhan Technology, Wuhan 430063)

Abstract The factors such as energy depletion, hardware malfunction and invasion, can lead to the node failure of wireless sensor networks (WSNs), further contributing to the topology partition (or even the paralysis of the entire network). Therefore, invulnerability is the major technical bottleneck that impedes the widespread application of WSNs. The research of the invulnerability of WSNs mainly focuses on following three issues: (1) what are the factors responsible for the node failure and network damage of WSNs; (2) how to measure the invulnerability of WSNs; (3) how to improve the invulnerability of WSNs. In this paper, the study on the causes of failures, invulnerability measurements, improvement strategies, fault detection and recovery are concluded and classified. As the core of the invulnerability research, the methods of invulnerability optimization (e. g. routing control, network reconstruction and topology evolution) are analyzed emphatically. At the end, the future challenges and development tendency of the invulnerability of WSNs are discussed.

Keywords wireless sensor networks; invulnerability; routing control; network construction; topology evolution; fault detection and recovery

1 引 言

“网络抗毁性 (Invulnerability, Survivability,

Robustness, Tolerance, Reliability)”衡量的是系统可持续稳定提供可靠服务的能力^[1-2].如在电力网络运行过程中,少数关键变电设施发生故障,其影响将瞬间波及全网,引发网络瘫痪.在军事后勤保障网

收稿日期:2013-10-08;最终修改稿收到日期:2014-10-17. 本课题得到国家“十二五”科技支撑计划项目(2012BAJ05B07)、国家自然科学基金基金(61305110)、湖北省国际科技合作项目(2011BFA012)和中央高校基本科研业务费专项资金(135118003)资助. 李文锋,男,1966年生,博士,教授,博士生导师,主要研究领域为物联网与机器人技术、无线传感器网络. E-mail: liwf@whut.edu.cn. 符修文,男,1987年生,博士研究生,主要研究方向为无线传感器网络抗毁性、复杂网络理论.

络中,对关键港口或机场展开攻击,将导致整个后勤供给受到威胁,并进而可能影响战争进程^[3].特别是随着人类社会网络化程度的加深,频繁发生的事故引起了人们的广泛思考.我们身边的这些网络的可靠性到底如何?当面对恶意攻击或自然灾害时,网络是否仍能够稳定可靠运行?是否存在潜在事故隐患引发网络崩溃?这些都是研究网络抗毁性所重点关注的问题.

网络抗毁性分为狭义抗毁性与生存性.狭义抗毁性指的是网络应对自然灾害或人为攻击等外在破坏因素时可持续稳定提供服务的能力,衡量的是网络受到外部破坏时的可靠性,最早应用于军事与电力领域^[4].事实上,多数网络如电力网络、物流网络、计算机网络等,只需要破坏少数关键链路或者节点就可以影响整个网络运行进程.网络生存性是指网络应对诸如能量耗尽与软硬件故障等自身内部失效情形时的可靠性.在商用环境中,网络生存性表现为网络中部件(节点和链路)的自然失效^[5].

无线传感器网络(Wireless Sensor Networks, WSNs)通过在环境中布设大量传感器节点,采用无线协作方式,可有效感知与处理各种环境与目标信息.布置在恶意环境中的 WSNs 常会因为人为入侵或自然灾害等外部原因导致节点失效.与此同时, WSNs 中节点通常采用移动电源供电,常因成本受限或部署环境恶劣等原因,导致节点能量快速耗尽或软硬件故障而无法正常工作.失效节点将造成网络连通性与覆盖度下降,并进而导致全局网络受损^[6-8].由于资源有限、规模庞大、传递时延与有向传输等内在因素所产生的非线性网络行为难以预测,研究 WSNs 抗毁性对解决 WSNs 规模化应用瓶颈具有重要的理论价值.

WSNs 抗毁性研究主要关注以下 3 个科学问题:

(1) 造成 WSNs 节点失效与网络受损的原因有哪些?

确定 WSNs 失效原因是研究 WSNs 抗毁性需要首先关注的问题. WSNs 在不同的节点失效作用下,网络受损类型表现出明显的差异性,因此,确定不同 WSNs 任务场景中造成节点失效的起因,分析网络受损类型,是保证后续抗毁性研究成果符合真实场景需要的前提.

(2) 如何度量 WSNs 的抗毁性能?

抗毁性测度是研究 WSNs 抗毁性的前提.需要针对 WSNs 特征,借助概率论、图论等理论与方法,

构建 WSNs 抗毁性解析模型,并建立科学合理的抗毁性能评估方法与体系.

(3) 如何提升 WSNs 的抗毁性能?

该问题是研究 WSNs 抗毁性的目标,需要在抗毁性测度基础上,通过对 WSNs 微观与宏观结构属性、静态与动态行为的分析,研究 WSNs 各种属性与行为对网络抗毁性能的影响,明确 WSNs 应具备的抗毁性要素,为网络抗毁性的设计与优化提供理论依据与指导.

围绕以上 3 个问题,本文就 WSNs 抗毁性的研究现状与进展进行归纳总结,指出当前 WSNs 抗毁性研究中存在的问题与技术挑战,并探讨了未来发展趋势.

2 受损类型与起因

如图 1 所示(图中数字代表采用相关研究参考文献编号),受损类型是指从网络角度,依照网络受损行为发生的概率分布与功能性特征,对网络受损进行类型划分,包含随机性受损、被选择性受损与组织性受损.受损起因是从节点失效角度,考虑个体节点物理属性,分析造成网络受损的起因,包含能耗失效、故障失效与攻击失效.

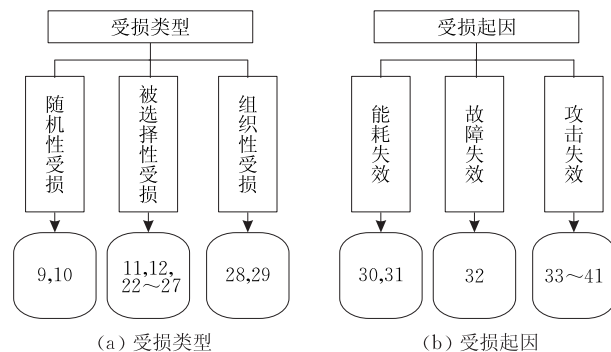


图 1 受损类型与起因分类

2.1 受损类型

2.1.1 随机性受损

在 WSNs 中,随机性受损^[9-10]指的是由人为失误、软件漏洞、硬件故障或者自然环境变化等各种随机因素引起的物理设备损坏或软件故障所导致的网络受损类型.假定 WSNs 含有 N 个节点,从网络中随机移除 $N \times f$ 个节点,其中 f 为所移除节点占网络节点总数比例,这就是我们所谓的随机性受损.

2.1.2 被选择性受损

被选择性受损^[11]是指基于所获取的网络局部

或全部信息,按照节点重要性程度选择受损目标对网络进行破坏.通常情况下,被选择性受损是指由于黑客入侵或恶意破坏所导致的具有明显人为干涉特征的网络受损类型^[12].因此,如何确定节点的重要性程度是研究被选择性受损类型的核心问题.关于节点重要性程度的评估方法有很多,例如度^[13]、紧密度^[14]、介数^[15]、特征向量^[16]等.但最简单也是使用最广泛的节点重要度指标就是节点的度. Albert 等人^[1]研究随机网络(ER 模型)和无标度网络(BA 模型),Guimera 等人^[17]研究交通网络,Opsahl 等人^[18]研究社交网络,Newman 等人^[19]研究电子邮件网络,Cetinkaya 等人^[20]研究 Internet,李勇等人^[21]研究后勤保障网络,他们均将节点的连接度作为确定节点重要性程度的指标.但 WSNs 作为以数据为中心的分布式网络,以往关于广义复杂网络的中心度定义难以对 WSNs 节点的中心化程度给予精确度量.以典型分簇 WSNs 拓扑为例(如图 2 所示),对 WSNs 中心度进行分析(如表 1 所示).

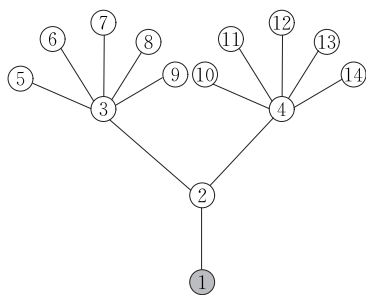


图 2 典型分簇 WSNs 拓扑结构

表 1 不同节点、不同中心化测度比较

节点	度中心度	紧密度中心度	介数中心度	特征向量中心度	WSN 介数中心度
2	0.230	0.565	0.615	0.590	1.000
3,4	0.461	0.520	0.641	0.690	0.500
5~14	0.069	0.351	0	0.255	0.071

如图 2 所示,节点 1 为 Sink 节点,其余节点均为普通传感器节点.如果节点 2 由于某种原因停止工作,则网络中剩余传感器节点都将因通往 Sink 节点的链路缺失而无法正常工作.节点 3 或 4 若无法运行,则网络中仍有 50% 的节点可正常运行.但如果仅仅依靠连接度、紧密度、介数或者特征向量对节点中心化程度进行度量,如表 1 所示,显然不足以反映节点 2 的重要性程度.尽管在紧密度中心化指标上,节点 2 略高于节点 3 和 4,但其幅度并不足以说明节点 2 的中心化程度.因此,作者基于 WSNs 数据传输的有向性给出全新 WSNs 中心化测度——

WSN 介数中心度 $C_c(x)$ ^[22]:

$$C_c(x) = \frac{\sum_{k \in v} g_k(x)/g_k}{n-1} \quad (1)$$

其中, g_k 为节点 k 到达 Sink 节点的最短路径数量. $g_k(x)$ 为节点 k 到达 Sink 节点的所有最短路径中经过节点 x 的条数.显然,对于节点 x ,最极端情形为除自身节点外,网络中其他节点到达 Sink 节点的最短路径均经过节点 x ,此时节点 x 的 WSN 介数中心度 $C_c(x)$ 为 1.

以上关于网络中心度的研究仍是针对网络拓扑,以连通性作为出发点,以网络邻接矩阵作为研究对象,基于图论对网络中心度进行分析,并没有考虑 WSNs 自身的路由特点. WSNs 在早期研究过程中,通常采用对等平面结构,采用功率控制算法进行数据传递^[23].但随着研究深入,分层分簇结构由于传输高效等优点得到广泛研究,如 LEACH^[24]、PEGASIS^[25]等.王良民等人^[26]针对 WSNs 分簇结构,选择簇头节点作为受损目标.在其研究中,簇头节点占所有节点 n 中的比例为 $p(n)$,则入侵节点集中在 $n \times p(n)$ 个簇头上.林力伟等人^[27]在此基础上对选择策略进行扩展,分别设置 3 种选择策略:(1)选择网络中的簇头节点;(2)选择靠近 Sink 节点的传感器节点,但不包含基础设施节点;(3)选择靠近 Sink 节点的传感器节点,且包括基础设施节点.尽管在王和林的选择策略中,考虑了 WSNs 分簇结构,但是其实质仍是依据路由分簇与地理位置信息构建受损对象集合,但集合内节点彼此重要性程度相同,不存在选择优先级,所以仍带有明显的随机性特征.考虑能耗均衡,在绝大多数分簇协议中,由于簇头节点采用定期选举机制,簇头分布具有明显的动态性特征.如何在动态环境下构建受损对象集合仍是有待研究的方向.

2.1.3 组织性受损

组织性受损是将 WSNs 与一般网络区分开来的重要标志. WSNs 作为典型的数据中心网络,其关注的焦点不在于节点自身能否正常工作,而是节点能否将自身所采集的数据发送至 Sink 节点.因此,即使传感器节点自身物理属性健全,但若因与 Sink 节点有效链路中断而无法进行数据传递,则可合理认定该节点无法正常工作^[28].因此,组织性受损是指网络因移除节点而导致通往 Sink 节点有效链路缺失所引发的网络受损类型.值得注意的是,组织性受损不能作为单一网络受损类型存在,其出现必然

伴随随机性受损或被选择性受损的发生. 在随机布设及不考虑 WSNs 能耗属性的前提下, 本文作者在文献[29]中通过仿真验证, 对于一般 WSNs, 仅需随机移除 40% 的传感器节点, 就可破坏剩余节点通往 Sink 节点的绝大多数通讯链路, 并进而验证了组织性受损是造成 WSNs 抗毁性能下降的主要受损类型. 在 WSNs 大规模部署情形下, 节点中心化程度分布不均, 少数关键节点失效将导致大规模剩余传感器节点通讯链路受损. 因此, 若依照节点中心化程度对网络展开攻击, 则组织性受损对网络性能的影响更为明显.

2.2 受损起因

2.2.1 能耗失效

WSNs 作为能量受限网络, 因电池耗尽所引起的节点失效是网络受损的重要原因之一. WSNs 能耗通常包括通讯能耗与监听能耗. 文献[30]定义网络空间内传感器节点均具有初始能量 E_0 . 每单位时间间隔 Δt 内, 节点因监听消耗能量 E_w . 针对通讯能耗, 设定每单位时间间隔 Δt 内, 网络中任意节点依照概率 P_M 产生消息包 Msg, 并沿最短路径到达 Sink 节点. 消息传递过程中所产生的能耗采用经典 First-order Radio^[31] 无线通信能耗模型. 需要说明的是, 与其他两种失效成因不同, 能耗作为 WSNs 自身固有物理属性, 网络在运作过程中将不可避免地产生能量消耗, 并导致能耗失效. 因此, 对提升 WSNs 抗毁性而言, 研究能耗失效的目的在于提升网络抗毁性能的同时, 如何将网络能耗降至最低.

2.2.2 故障失效

在 WSNs 中, 一般将故障失效设定为基于随机概率分布确定失效对象. 事实上, 由于 WSNs 拓扑异质性的存在, 中心节点所承担通讯负载远大于普通节点, 造成其故障发生概率远高于普通节点. 以最为常见的 WSNs 分簇结构为例, 簇头节点除自身感知任务外, 仍需要收集、处理与转发簇内成员节点数据, 使得簇头节点所承担任务量远大于普通成员节点, 导致其故障发生概率远高于一般节点. 基于该考虑, 在文献[32]中, 故障发生概率与节点度成指数变化关系.

2.2.3 攻击失效

对于攻击失效, 目前多数文献^[1,5,9-12,26-27] 均简单将攻击策略设定为依据节点中心化程度, 从高至低依次对网络展开攻击. 由于被选择性受损是节点攻击失效发生后网络受损类型的主要表现形式, 有关节点中心度的确定可参照 2.1.2 节有关选择性受损的表述. 在对攻击失效进行具体建模时, 需要对攻击

方式做出具体参数设定, 通常包含攻击视野、攻击范围与攻击强度.

(1) 攻击视野

攻击视野是指攻击者在制定网络攻击策略时, 对网络的熟知程度. 在多数文献^[1,5,9-12,26-28,32] 中, 都将攻击失效的前提设置为破坏者了解全网信息, 从而能够以最具杀伤力的方式对网络展开攻击. 但在很多情况下, 攻击者显然只能掌握网络局部信息, 并根据局部信息展开攻击. 如在军事领域, 甲方只能在已渗透区域对乙方的网络基础设施展开攻击, 而无法对未到达区域展开攻击. 因此, 制定攻击策略时, 需要根据任务场景的不同, 具体设定攻击视野. 攻击视野的选择可归纳为典型的不完全信息条件下的区域信息确定性问题^[33]. 设定网络中节点 v_i 的中心度为 I_i . 所有节点依照中心度 I_i 进行排序, 可获得节点 v_i 的排列序号为 r_i . 节点 v_i 的信息获取状态用 δ_i 表示. 若 v_i 的中心度 I_i 已知, 则 $\delta_i = 1$, 否则 $\delta_i = 0$. 称所有信息状态公开的节点所构成集合为“已知区域 Ω ”, 即 $\Omega = \{v_i | \delta_i = 1, v_i \in V\}$. 称所有信息状态未知的节点所构成集合为“未知区域 Ω^* ”, 即 $\Omega^* = \{v_i | \delta_i = 0, v_i \in V\}$. Xiao 等人^[34] 基于局域信息提出一种基于路由表的攻击策略, 攻击者不需要掌握网络全局信息, 仅依据所持有邻域路由信息对邻居节点展开攻击. Xia 等人^[35] 则根据已掌握网络局部度信息 (Partial Degree Information) 对全局网络拓扑进行合理估计, 并以此为依据制定攻击策略. Holme 等人^[36] 按照网络信息的更新程度, 将网络攻击者分为仅掌握初始网络拓扑信息和实时掌握网络拓扑信息两类, 并分别选取度和介数构建攻击策略, 主要有

① ID (Initial Degree) 攻击策略: 依照初始网络中节点度的大小移除节点;

② IB (Initial Betweenness) 攻击策略: 依照初始网络中节点介数的大小移除节点;

③ RD (Recalculated Degree) 攻击策略: 移除当前时刻网络中度最大的节点;

④ RB (Recalculated Betweenness) 攻击策略: 移除当前时刻网络中介数最大的节点.

(2) 攻击范围

攻击范围是指执行单次攻击行为时所波及的范围大小, 一般包含单点攻击与区域攻击. 多数研究均将攻击范围设定为单点攻击, 即每次攻击行为仅破坏单个节点或单条链路. 但事实上, 在多数真实场景中 (如火灾、地震等), 攻击行为多为区域攻击, 具备

典型的空间相关性特征,即攻击对象往往为某一中心点及其相邻地理区域.我们通常将该类攻击失效情形定义为地理空间关联失效(Geographically Correlated Failures)^[37].Azimi 等人^[38]最早对地理空间关联失效展开研究,并将攻击范围的形状分别设置为三角形与正方形.Liu 等人^[39]在此基础上对其进行扩展,提出 PRF(Probabilistic Region Failure)失效模型.该模型将攻击范围的形状设定为圆形,且离圆心较近的节点失效概率明显高于距离较远的节点.考虑如爆破、地震等具备典型震源辐射特征的真实场景,PRF 模型较 Azimi 等人所提模型更为接近真实情形.不论是 Azimi 等人还是 Liu 等人的研究成果均将失效对象限制为网络所覆盖单一区域内的节点同时失效,Sen 等人^[40]将该类模型归纳为单一区域失效模型 SRFM(Single Region Fault Model),并对其进行了扩展,给出多区域失效模型 MRFM(Multiple Region Fault Model).由于在 MRFM 模型中,仅简单将多个失效区域设定为覆盖范围与形状均相同,且地理位置服从随机分布,具有明显局限性.基于该考虑,Rahnamay-Naeimi 等人^[41]对网络负载进行度量,并基于泊松分布,确定多个失效区域中心位置.若该区域载荷越重,则被选择攻击的概率越高.

(3) 攻击强度

攻击强度是指执行单次攻击行为对攻击对象的破坏程度.在多数场景中,均将移除点或边作为单次攻击失效的实现方式.但在某些特殊场景,网络攻击仅会导致节点或边性能的衰减.考虑该情形,Ágoston 等人^[42]提出“弱攻击(Weak Attack)”概念,即网络中边均被赋予权值,当两端节点受到攻击时,对应边权值随之衰减,若降为 0,则边失效.Yin 等人^[43]则在此基础上,引入权系数 $\omega \in [1, \infty)$ 对攻击强度进行定义.攻击强度随权系数的增加而单调递增.当权系数为 1 时,等同于节点或边未遭受攻击.当权系数趋近于 ∞ ,则被攻击的点或边从网络拓扑中直接移除.

值得注意的是,在研究个体节点失效行为时,常常基于以下假设:当节点失效行为发生,该失效为永久失效且不可逆转.显然,对于能耗失效而言,若不考虑能量补充,该失效模式为永久失效.但在其他情形下,节点失效后仍有可能恢复到正常工作状态.以故障失效为例,考虑节点信道占用,短时间内节点无法接收数据.若信道被释放,则节点恢复正常.考虑

攻击失效,若节点内设有硬件或软件冗余机制,节点在经历短时间工作停摆后,即可恢复工作.基于以上考虑,Masoum 等人^[44]考虑短时失效,基于离散时间马尔可夫链(Discrete Time Markov Chain)构建节点失效模型,即传感器节点分别被划分为状态 ON 与 OFF.当节点状态为 ON 时,在下一时刻,节点以概率 a 切换为状态 OFF,反之,以概率 $1-a$ 保持状态 ON 不变.同理,当节点处于 OFF 状态时,则遵循概率 b 进行状态切换.Parvin 等人^[45]则在此基础上对短时失效故障模型进行细分,分别引入妥协状态(Compromised State)与回馈状态(Response State).对于未发生故障节点,当簇内可用节点比例超过阈值 k 时,则认定节点处于健康状态(Healthy State),当簇内可用节点比例低于阈值 k 时,则节点切换为妥协状态.处于妥协状态的节点以概率 μ 转换为故障节点,以概率 λ_r 进入回馈状态.在回馈状态,节点可通过重启(Rebooting)等方式以概率 μ 返回健康状态,若回馈失败,则节点以概率 λ 转化为故障节点.在 Masoum 等人与 Parvin 等人的研究中,均将节点故障的发生与恢复视为简单概率事件.但在真实情形下,发生故障的时长与频率和节点通讯密切相关.

尽管当前有关 WSNs 受损类型与成因的研究众多,但现有节点失效模型与真实情形差异明显.因此,如何提出一种综合节点失效模型,能够涵盖攻击策略与方式选择、能耗与故障失效及时间域选择等,保证所构建网络能够对随机受损、被选择性受损与组织性受损等多种网络受损类型作出准确响应,将是未来研究工作的重点.

3 抗毁性测度

当研究网络抗毁性时,我们需要针对不同节点的失效情形与网络受损类型对网络抗毁性能的影响做出准确评估.当利用网络构造方法提升网络抗毁性能时,我们需要对提升效用的好坏给出评价.网络抗毁性测度作为衡量网络抗毁性能优劣的具体量化指标,一直是复杂网络抗毁性研究领域的热点^[46],而 WSNs 抗毁性测度研究可被视为复杂网络抗毁性测度研究应用的拓展.因此,本节首先对复杂网络的抗毁性测度研究展开简要介绍,并在此基础上,归纳 WSNs 抗毁性测度现有研究成果.

网络抗毁性测度研究文献众多,根据网络覆盖

范围的不同,网络抗毁性测度可分为局部抗毁性测度与全局抗毁性测度^[47-48],根据网络拓扑模型的不同,网络抗毁性测度可分为非赋权抗毁性测度与赋权抗毁性测度^[49].从与网络拓扑的关联性程度的角度,本文将抗毁性测度分为非拓扑性测度与拓扑性测度.

3.1 非拓扑性测度

非拓扑性测度的核心思想是选取与网络拓扑无关的网络简单属性作为衡量网络抗毁能力的测度指标.常用网络属性包括剩余可用节点数量^[50]、覆盖面积^[51]、网络寿命^[52]等.这些网络属性简单易得,因此,在许多文献中往往采用一种或几种网络属性作为抗毁性测度的指标.但是网络属性难以全面准确反映网络抗毁性能.以 WSNs 中剩余可用节点数量为例,当网络遭受攻击,若剩余可用节点数量较多,说明该网络的节点冗余度较高.但若剩余生存节点全部局限于特定区域,显然难以满足以覆盖面积为服务质量(Quality of Service, QoS)标准的抗毁性要求.

3.2 拓扑性测度

与仅以单一点或边为特征提取对象的非拓扑抗毁性测度相比,基于网络拓扑的抗毁性测度以网络连通性为对象,以邻接矩阵为提取特征来源,选择图论及概率统计学等作为理论工具,能够更为全面地度量网络抗毁性能.在 Albert 等人^[1]2000 年发表在《Nature》上的关于随机网络(ER 模型)与无标度网络(BA 模型)的抗毁性经典论述中,就选取不同攻击条件下的网络最大连通簇(Giant Component)尺寸与网络规模之比 S 、最大连通簇平均最短路径 l 与节点移除比例 f 的关系作为网络抗毁性测度,并在此基础上,得到在选择性攻击下,随机网络较无标度网络抗毁性更优,而无标度网络抵御随机攻击能力更强这一经典结论.但吴俊等人^[2]发现,对于一般复杂网络而言,随着网络破坏程度的加剧,最大连通簇规模呈单调递减趋势,而平均最短路径却是先增大后减小,这种非单调性给评估网络抗毁性能带来诸多不便.1970 年 Frank 等人^[53]提出的“连接度(Node Connectivity)”和“粘聚度(Link Connectivity)”被证明具有良好的抗毁性表征性能.连接度是指使网络不连通所需移除的最少节点个数,而粘聚度是指使网络不连通所需删除的最少链路数.后续有诸多学者在此基础上对连接度及粘聚度概念进行扩展,但由于在复杂网络中,特别是无标度网络中普遍存在大量度数很小的节点,而连通度与粘聚度必须小于

最小节点度数,导致在许多网络中连接度与粘聚度失去测度意义.基于该考虑,谭跃进等人^[54]首次引入“收缩”概念,综合考虑节点连接度以及经过该节点最短路径的数目,重新定义粘聚度.在此基础上,郭虹等人^[55]通过计算 Ad Hoc 网络中任意节点收缩前后的网络粘聚度,评估节点中心化程度,并通过构建面向网络中心度分布的网络抗毁性熵评估网络抗毁性能.其他抗毁性测度还包括跳面节点法^[56]、基于全网平均等效最短路径数的方法^[57]、基于自然连通度的评估方法^[58]、基于拓扑不相交路径的评估方法^[59]和基于连通分支数的评估方法^[60]等.尽管有关抗毁性研究众多,但这些测度各有侧重点.对于不同类型网络而言,均带有一定局限性.

3.3 WSNs 抗毁性测度

对于 WSNs,尽管有关复杂网络的抗毁性测度研究,一定程度上能够反映网络抗毁性能的优劣,但在实际运用过程中,仍存在一定局限:(1)未考虑 WSNs 有效连通性;(2)未考虑能耗敏感.以文献^[60]所提网络连通系数为基础,林力伟等人^[27]考虑 WSNs 汇聚特征,引入有效连通度概念,提出面向 WSNs 的抗毁性测度.何明等人^[61]从网络连通性覆盖度出发,提出满足 k -覆盖与 k -连通的 WSNs 抗毁性评估模型.该模型整合了以往基于连通度的网络抗毁性与表明 QoS 的覆盖率,但没有考虑 WSNs 的典型分簇结构.Xing 等人^[62]通过评估基本簇单元的连通性与覆盖度来测量具有多级簇结构的 WSNs 的抗毁性能,具有更好的场景适用性.文献^[63]提出了基于删除节点后最短路径变化的评估方法,该方法只在移除节点后考量剩余网络是否仍然连通,并没有考虑移除节点可能造成剩余节点之间最短距离变大这一特殊情况.Aboelfotoh 等人^[64]观测到一个或多个节点的失效可能导致源节点与 Sink 节点之间链路中断,或者链路长度增加,加剧信息传递延迟.作者通过构建预期信息延迟和最大信息延迟测度,测量网络抗毁性.与之前面向连通性的 WSNs 抗毁性测度相比,Aboelfotoh 等人所提测度可涵盖消息传递延时等 QoS 指标,对抗毁性能表征更为全面.

WSNs 与其他网络的最大差别在于缺乏能量持续供给,因此,在研究 WSNs 抗毁性时,不应忽略节点剩余能量的影响.齐小刚等人^[65]提出一种考虑节点剩余能量与拓扑贡献度的 WSNs 抗毁性测度.在该测度中,以个体节点的抗毁性能作为输入,求解均

值与方差用来表征全局网络的抗毁性能, 但该测度并未就如何确定节点剩余能量与网络拓扑在测度中所占权重给予具体说明. Cai 等人^[66]基于网络平均寿命与 k -覆盖率提出抗毁性测度. 网络平均寿命的定义为从网络中随机移除数个传感器节点, 当 k -覆盖率降低至阈值 θ 时, 所移除节点数量占全局网络节点总数的比例, 即为网络平均寿命. 与之对应, 若将随机移除策略替换为依照连接度从高到低依序移除, 则移除节点数目与全网节点总数的比值定义为平均抗毁性. 该测度准确与否依赖于 k 值的选取. 由于不同规模网络对覆盖率要求具有明显差异性, k 值的选取面临难题. 段谟意^[67]针对网络抗毁性提出了一种新的度量方法, 该方法通过建立节点最大流量模型, 并借助元胞蚁群算法进行求解, 评估网络抗

毁性能. 但在该测度中, 仅将最大流量视为节点间链路可靠性的评价指标, 忽视了冗余链路对抗毁性能的提升效果, 使得测度评估结果带有明显局限性. 为说明现有抗毁性测度的性能, 如表 2 所示, 对其进行比较分析.

4 抗毁性策略

如图 3 所示, 抗毁性策略按照实施手段可分为路由控制、网络重构和拓扑演化, 其中路由控制可划归为“软优化”, 即不需要硬件改动或升级, 通过路由优化提升网络抗毁性能. 与之相反, 网络重构与拓扑演化可归纳为“硬优化”, 即需要通过提升网络异质性或规模达到抗毁性优化的目的.

表 2 网络抗毁性测度比较分析

抗毁性测度	网络对象	能耗敏感	随机性 受损类型	被选择性 受损类型	组织性 受损类型	测量 单调性	计算 复杂度	研究方法
剩余可用节点数量 ^[50]	一般网络	不可测量	可测量	可测量	不可测量	单调	低	仿真比较
覆盖面积 ^[51]	一般网络	不可测量	可测量	可测量	不可测量	单调	低	仿真比较
网络寿命 ^[52]	一般网络	可测量	不可测量	不可测量	不可测量	单调	低	仿真比较
最大连通簇尺寸 ^[1]	一般网络	不可测量	可测量	可测量	不可测量	单调	中	仿真比较
最大连通簇平均最短路径 ^[1]	一般网络	不可测量	可测量	可测量	不可测量	非单调	中	理论推导
连接度与凝聚度 ^[53]	一般网络	不可测量	可测量	可测量	不可测量	单调	高	仿真比较
收缩凝聚度 ^[54]	一般网络	不可测量	可测量	可测量	不可测量	单调	高	理论推导
网络抗毁性熵 ^[55]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	高	理论推导
跳面节点法 ^[56]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	高	理论推导
全网平均等效最短路径数 ^[57]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	中	理论推导
自然连通度 ^[58]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	高	理论推导
拓扑不相交路径 ^[59]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	高	理论推导
连通分支数 ^[60]	Ad Hoc	不可测量	可测量	可测量	不可测量	单调	低	仿真比较
拓扑有效连通分支 ^[27]	WSNs	不可测量	可测量	可测量	不可测量	单调	中	仿真比较
k -连通与 k -覆盖 ^[61]	WSNs	不可测量	可测量	可测量	不可测量	单调	高	仿真比较
基本簇单元 ^[62]	WSNs	不可测量	可测量	可测量	不可测量	单调	中	仿真比较
最短路径变化 ^[63]	WSNs	不可测量	可测量	可测量	可测量	单调	中	仿真比较
信息传递延迟 ^[64]	WSNs	不可测量	可测量	可测量	不可测量	单调	高	仿真比较
节点剩余能量与拓扑贡献度 ^[65]	WSNs	可测量	可测量	可测量	可测量	单调	高	仿真比较
网络平均寿命与拓扑贡献度 ^[66]	WSNs	可测量	可测量	可测量	可测量	单调	高	仿真比较
基于元胞蚁群算法的节点最大流量估计 ^[67]	WSNs	不可测量	可测量	可测量	不可测量	单调	高	仿真比较

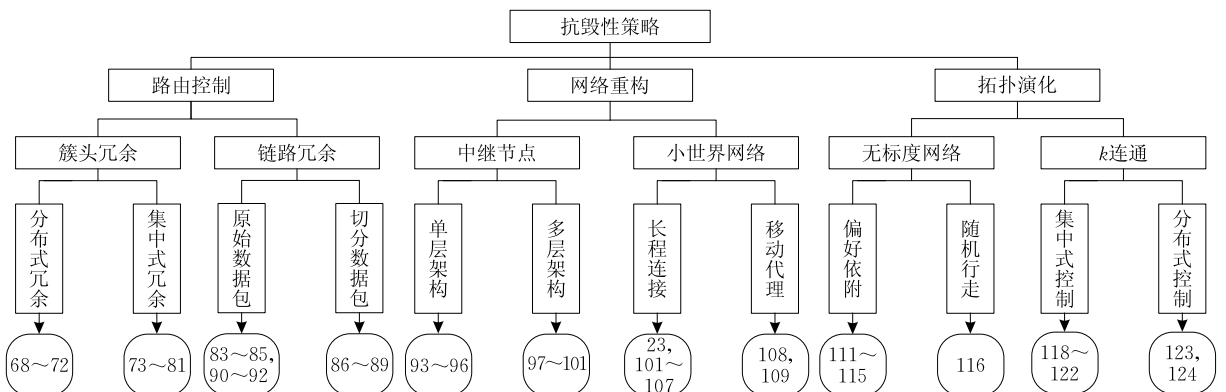


图 3 抗毁性策略分类

4.1 路由控制

在多数 WSNs 任务场景中,通常需要大规模部署低成本的传感器节点,因此在网络中存在许多冗余节点与链路. 这为利用冗余机制提升网络抗毁性能提供了可能. 路由控制的核心思想就是利用网络冗余特性,引入备份机制提升网络抗毁性能. 按照控制对象的不同,冗余机制可分为簇头冗余与链路冗余.

4.1.1 冗余簇头

簇头冗余策略是通过在每个簇单元内设置多个簇头. 当前簇头发生故障或能量耗尽时,由备份簇头与簇内成员节点建立通信,执行簇内数据采集、处理与转发任务. 根据簇头维护机制的不同,可将现有簇头冗余策略分为两类:(1)分布式簇头冗余策略,如 EEUC^[68] (Energy-efficient Unequal Clustering), HEED^[69] (Hybrid Energy-Efficient Distributed clustering), REED^[70] (Robust Energy Efficient Distributed clustering) 均属于此类策略,其特点是由簇内节点共同维护当前簇头与备份簇头的能量与路由信息,并对簇头轮换做出决定. 如在 REED 路由协议中,网络预先设定 k 个独立簇集合,且每个集合内均预设多个簇头节点. 当前簇头节点发生故障时,簇内节点通过路由信息交换,从备份簇头节点中选取簇内连通性最优的节点作为执行簇头. 该路由的运行依赖于所在簇内成员节点需要同时维持 k 个簇头节点路由信息,导致簇内节点间路由由数据交换能耗巨大,影响网络寿命. 基于该考虑,蔡海滨等人^[71]通过建立相邻节点间剩余能量预测模型 REP (Redundant Energy Prediction),降低簇内节点间因路由维护所产生的通讯能耗. 上述情况均将簇头间状态切换视为理想情形. 但显然在真实情况下,当前簇头与备份簇头发生状态切换时,可能由于

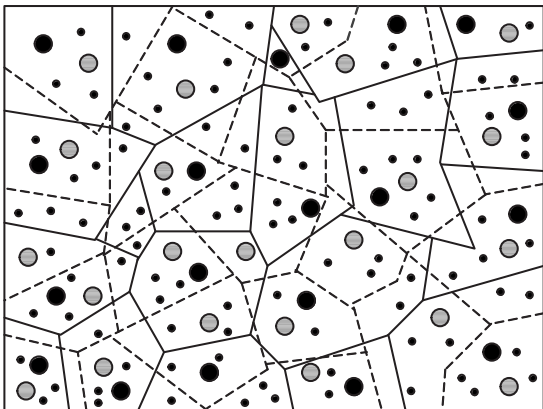


图 4 簇头冗余

噪声干扰或信道冲突等原因导致切换失败, Hashmi 等人^[72]通过额外设置除工作状态与备选状态外的失效状态,基于非齐次马尔可夫链 (Non-homogeneous Markov Chain) 对簇头切换状态进行概率建模,从而保证了当簇头切换指令执行失败时,当前簇头节点能够有效感知,并再次发送轮换请求,从而最终保证路由可靠性;(2)集中式簇头冗余策略. 典型算法包括 K -means^[73]、FT-DSC (Fault Tolerant Dynamic Clustering Protocol)^[74] 等,其特征是由当前簇头根据自身情况主动选择备份簇头进行轮换. 如在冯东芹等人^[75]所提集中式分簇路由算法中,当工作簇头能量不足时,主动向备份簇头发送轮换请求. 除此之外,工作簇头定期向备份簇头发送冗余测试报文,若设定时长内备份簇头未接收到该报文,则认定工作簇头发生故障,由备份簇头主动接替簇头管理职能. 尽管该机制运行简单,但由于备份簇头节点仍需对簇内路由及能量信息进行实时同步更新,因此,在运行过程中,其能量消耗仍较为明显. 基于能耗考虑, Gupta 等人^[74]通过对当前簇头节点与备用簇头节点重新进行分工定义,由当前簇头节点负责簇内信息转发,而备用簇头节点负责簇内路由与剩余能量信息维护以及簇头故障检测. 与冯东芹等人所提冗余分簇路由相比, Gupta 所提 FT-DSC 路由能够有效降低簇头节点通讯及运算造成的负担.

总体而言,集中式策略要求簇头实时获取和计算冗余簇头的能量与路由信息. 对于规模较小,特别是簇内拓扑为星形结构的网络而言,执行效率较高,可靠性优势明显. 但当网络规模较大时,仅依靠当前簇头对所在簇进行管理,受制于缓存及能耗限制,现实中存在实现困难. 而分布式路由依赖节点间协作,具有较强的复杂事务处理能力,因而场景适应能力较强. 但分布式路由需要依赖簇内节点不断交互信息,与集中式相比,将明显加剧网络通信负载,并占用额外通信带宽. 特别是当网络拥塞或突发故障时,网络响应较慢,无法做到实时快速处理.

值得注意的是,在 WSNs 分簇路由协议中,簇头除了采集、处理与传递簇内数据外,还需中继传输来自其他簇的过路数据,使得离 Sink 节点越近的簇头将承担越多的过路数据转发任务,从而引发网络负载失衡的“热点 (Hot-spot) 效应^[76]”(如图 5 所示). 该效应使接近 Sink 节点的簇头比其他节点更快耗尽电量,并进而引发“能量空洞 (Energy Hole)^[77]”,造成网络拓扑分割与数据传输链路中断. 除此之外,由簇头失效所引发的簇重组过程往往需要消耗大

量能量,并明显加剧服务延时.因此,针对该问题,Bagci 等人^[78]提出 EAUCF(Energy Aware Unequal Clustering with Fuzzy)算法将邻近 Sink 节点的区域分成许多规模较小的簇,使簇间负载均衡.但该算法仅将簇内节点连通性作为备份簇头的选举依据,而诸如剩余能量等关键影响因子未被考虑在内.苏金树等人^[79]提出一种基于节点剩余能量与保证簇头 2-连通性的容错分簇算法.其考虑大规模网络部署情形下,获取最优簇头集合为典型 NP-Hard 问题.因此,采用自适应的离散粒子群算法对问题进行求解.张擎等人^[80]提出一种综合考虑节点地理位置约束与节点能量的不等规模分簇算法,通过动态调节分簇半径,实时有效处理拥塞和簇头故障,减少消耗巨大的重新分簇过程.曾志文等人^[81]在动态调节分簇半径基础上,通过让能耗低的节点以较高的数据发送率,能耗高的节点以较低的数据发送率传递数据,进一步均衡网络能耗且延迟不增加.

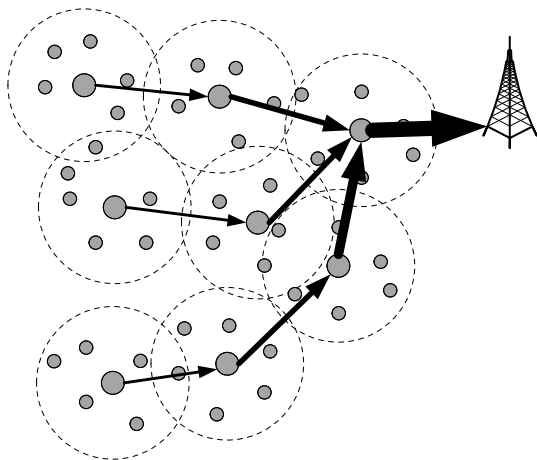


图 5 网络热点效应

4.1.2 冗余链路

冗余链路通过在源节点与 Sink 节点间构建多条链路的方式,避免节点通讯过度依赖单一链路的情况,从而保证当前通讯链路失效时,数据仍可传递至 Sink 节点.冗余链路等价于多路径路由问题.多路径路由按照数据包是否切分可以分为:(1)原始数据包发送方式;(2)切分数据包发送方式^[82].在原始数据包发送方式中,源节点将数据包拷贝多份,并将原始数据包及其拷贝沿多路径传递至目标节点.如 MMSPEED^[83](Multi-path and Multi-SPEED)、MCMP^[84](Multi-Constrained and Multi-path)均属于此类方式.例如 Ren 等人^[85]基于动态源路由协议 DSR(Dynamic Source Routing)提出了考虑信息流的多路径构造算法 TADR(Traffic-aware Dynamic

Routing).该算法首先根据深度场(Depth Field)确定源信息至目标信息最短路径,并基于势场(Potential Field)对次优路径进行排序.如果最优路径因节点失效导致链路中断,则次优路径依次递补.而在切分数据包发送方式中,源节点对数据包进行重新编码,并将其切分为若干数量的独立数据包,在完成拷贝复制后,沿多路径发送至目标节点.典型路由包括 DCAR^[86](Distributed Coding-Aware Routing)、SCAR(Self-Coding-Aware Routing)^[87]和 NC-RMR^[88](Network Coding based Reliable disjoint and braided Multipath Routing).例如 Lai 等人^[89]依据路径数目对所发送数据进行切分,利用冗余发送方式沿多路径进行传递.目标节点将所接收数据包进行重组,即可还原得到原始数据.与原始数据发送方式相比,切分数据发送方式由于传输数据包单位体积较小且数量冗余,避免网络中数据传输过分依赖单一链路或数据包,从而提高网络的抗毁性能.但数据包编码与切分过程对节点运算性能要求较高,且路由设计相对复杂.

多路径路由根据多路径间是否相交可分为:(1)不相交点多路径;(2)不相交边多路径;(3)局部相交多路径.其中,不相交点多路径指的是已确定路径集合内,彼此间不存在相交节点.显然,不相交点多路径由于路径间彼此独立,移除单一点或边至多导致一条链路失效.与不相交点多路径类似,不相交边多路径在其已确定路径集合内,不存在重复边.在不考虑节点失效情况下,对因通信失效而导致的边失效情形具有较强抗毁性.但在实际布置中,寻找理想数量的不相交点/边多路径存在现实困难,而局部相交多路径介于上述两种路径选择策略之间,在具有较强场景适应性的同时,对点失效与边失效情形均具有一定抗毁性.在其路径规划过程中,往往遵循 2 度分离原则,即至少存在两条及两条以上不相交点路径.方效林等人^[90]基于广度优先搜索提出 2-不相交路径路由算法,该算法对网络规模扩大具有较强适应性,并可用于多 Sink 网络.但由于算法复杂度为 $O(|L|)$,其中 $|L|$ 为网络存在边数.显然,如果网络中通讯链路分布密集,则搜索范围急剧扩大,算法收敛速度将受到明显影响.于磊磊等人^[91]针对工业传感器网络拓扑稳定且 Sink 节点功能相对强大等特性,提出一种中心化计算的 2-不相交路径路由算法,该算法由掌握全网路由信息的 Sink 节点计算近似最优 2-节点/链路不相交路径.较分布式多路径路由算法,该算法能够有效减轻网络通讯负载.以

上研究,均理想假设若节点间链路建立,则链路可靠且不存在时延,与真实场景具有明显差异.因此,王小明等人^[92]考虑信号衰减、干扰与时延等通信环境下不确定因素,引入模糊随机过程理论和模糊随机规划方法,对无线链路时延与可靠性进行模糊性与随机性建模,提出了一种模糊随机多约束多路径路由,能够更真实地反映 WSNs 链路特征.

路由控制在不需要硬件改动或升级的前提下,能够借助路由优化提升网络抗毁性能,因而在网络构建成本方面,具有明显优势.但抗毁性能的提升是以通讯性能的下降与路由复杂度的上升作为代价.基于该考虑,网络重构与拓扑演化等“硬优化”方法因其构建方法简单与网络综合性能良好等优势得到越来越多学者的重视.

4.2 网络重构

网络重构是在已布设网络基础上,通过在网络中引入新的基础设施,提升网络异质性,并进而改善网络的抗毁性能.当前网络重构方法主要包含引入中继节点与构建小世界网络.引入中继节点的实质是通过引入比普通节点更为强大的中继节点提升网络中节点的异质性.与之对应,小世界网络则是借助长程连接或移动代理,构建比原有链路更为可靠的通讯链路,从而提升网络中链路的异质性.

4.2.1 中继节点

由于 WSNs 能耗是传输距离的非线性函数,长距离通信对于传感器节点耗能巨大.与普通传感器节点相比,中继节点在通讯与计算性能、能量储备及可靠性上表现更优.通过设置中继节点,能够有效均衡网络通讯负载,改善网络能耗表现,提升网络冗余度与连通度,使得传感器节点至 Sink 节点可能存在多条独立的通信路径,并最终达到提升网络抗毁性能的目的.目前多数中继节点布局算法均是研究如何通过布设最少数量的中继节点使网络具备 k -连通性,从而保证网络具有较好的容错性能.因此一般情况下,中继节点布局算法包含两种评价指标:(1)使用的中继节点数量最少;(2)完成布设后通信路径最短.

1999 年, Lin 等人^[93]在保证网络最小连通前提下,证明最少中继节点布设问题是一个 NP-Hard 问题,并基于最小生成树原理给出 5-逼近算法.在此基础上, Chen 等人^[94]和 Cheng 等人^[95]对算法提出改进,分别提出时间多项式为 3 和 2 的逼近算法,算法精度及收敛速度得到明显改善.但单连通 WSNs 面对失效/攻击,网络性能衰减明显.因此,现有关于中

继节点的研究的主要对象为 k -连通网络($k \geq 2$). Lloyd 等人^[96]提出了两种在网络中布设中继节点的策略:FFRP(Full Fault-tolerance Relay Placement)与 PFRP(Partial Fault-tolerance Relay Placement).在 FFRP 中,网络中任意一对中继节点与普通节点之间均至少存在 k 条独立的通信链路.而在 PFRP 中,仅每对普通节点之间存在 k 条独立的通信链路.尽管中继节点的加入可改善网络连通性,提升网络抗毁性能,但网络自身仍为单层(Single-tiered)网络(如图 6(a)所示),即中继节点仍基于现有路由协议参与网络通讯,因而加剧了网络路由负载失衡.基于该考虑, Han 等人^[97]通过构造双层(Double-tiered)网络平衡网络路由负载(如图 6(b)所示).在下层中,中继节点与邻近传感器节点构成分簇,中继节点负责接收及转发簇内其他节点数据.而在上层,所有中继节点组成骨干网络,用来簇间通讯.由于双层架构易于管理,且具有良好的可扩展性,成为目前中继节点研究的热点.在 Han 等人的研究中,其目标为构造 2-连通骨干网络,并未考虑中继节点对簇内节点的覆盖度,带有明显局限性. Yang 等人^[98]将 2-连通问题扩展为 2-连通/覆盖(2-connected Double Cover)问题,即网络中任意节点均至少被两个中继节点覆盖,且中继节点与 Sink 节点所组建的骨干网络连通度至少为 2.该算法容错性能优异,但算法近似比为 $O(\ln n)$,造成所需中继节点数目较大,网络构造成本上升明显.

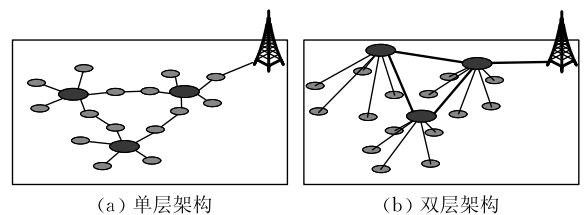


图 6 中继节点布局架构

在现实条件下,中继节点的布设往往受到环境、节点密度等条件限制.基于该考虑, Misra 等人^[99]考虑地理位置约束与节点间因避免通讯干扰而引入的最小距离约束,首先提出了中继节点备选位置集合的概念.王翥等人^[100]对约束条件进一步扩展,引入中继节点通讯容量约束与后期运行实际功耗约束,提出基于枚举法与贪婪寻优法结合的中继节点布局算法.随后,王翥等人^[101]通过引入最小网络距离因子评价标准,进一步改善中继节点布局算法性能.

4.2.2 小世界网络

小世界网络(Small-world Network)因具有良

好的拓扑属性,一直是复杂网络研究领域的热点.在小世界网络中,绝大多数节点并不直接相连.但由于有长程连接的存在,网络中多数节点仅需经过少数几个节点即可与网络中其他任意节点建立链路.因而,小世界网络具有较大的聚类系数与较小的平均路径长度.对于能量受限的 WSNs 而言,降低传感器节点与 Sink 节点之间的通讯链路长度是提升网络性能的关键.因此,如果能构建具有小世界网络特征的 WSNs 拓扑,则可使网络连通性较好且功耗较低.

Helmy 等人^[102-103]通过在 WSNs 中引入逻辑链路,首先证明了小世界网络同样适用于具有空间属性的 WSNs(如图 7 所示).研究表明,通过随机化加边的方式,网络平均路径长度下降明显.与此同时,所添加的逻辑链路长度仅需达到网络直径的 25%~40%,即可明显提升网络性能.对于由 1000 个随机分布的传感器节点所构成的 WSN.若 Sink 节点布设在区域中心位置,则仅需添加 5~24 条链路,网络平均路径长度降幅最高可达 60%~70%.Sharma 等人^[104]则进一步论证了通过在网络中添加少数随机连接,能够明显改善网络能耗均衡.Hawick 等人^[105]也采用类似方法,研究 WSNs 覆盖、容错与能耗问题.研究表明,将小世界网络特征引入 WSNs,不仅可以有效降低网络平均路径长度,而且网络中孤立簇的出现概率也明显下降,WSNs 的整体覆盖效果与寿命均得到大幅改善.以上研究均选取随机布局策略衡量长程连接的性能提升效果,但显然随机布局的提升效果并非最优.因此,对于布设 WSNs 长程连接而言,其核心问题为如何设置长程连接,使提升效果达到全局最优.Guidoni 等人^[106-107]提出了全新的构建 WSNs 小世界网络特征的 DAS(Directed Angulation towards the Sink)方案和 SSD(Sink node as Source/Destination)方案.但 DAS 与 SSD 方案的核心是随机选取起始端节点,并与 Sink 节点连线,选取固定夹角,以该连线作为中心线,确定夹角覆盖范围,并在该范围内随机选取终端节点,构建长程连接.尽管两种方案均可以保证长程连接在一定角误差范围内指向 Sink 节点,但选取过程仍带有明显随机性.本文作者基于 WSN 介数中心度提出一种面向抗毁性的长程连接布局策略^[23],通过计算全网中心度分布,选取中心度最高节点在通往 Sink 节点最短路径的上游与下游分别选取端点构建长程连接.该策略使得面对单一网络有且仅有一种布局策略使抗毁性能提升效果达到最优,从而排除了随机性因素对网络性能的影响.

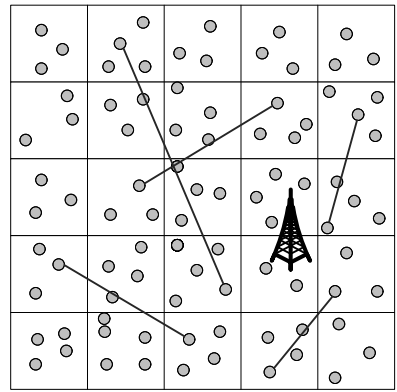


图 7 面向 WSNs 的小世界网络构型

一般情况下长程连接主要适用于静态网络拓扑环境,一旦布置好便不能移动,且易受地理位置约束.Shah 等人^[108]基于容迟网络特征,提出利用移动代理 data mules 模拟小世界网络中的长程连接,构建具备小世界网络特征的 WSNs 拓扑结构.而动态网络环境下的长程连接是由 data mules 在数据传输过程中借助移动轨迹所建立的.仿真结果表明, data mules 数量的上升能够有效降低网络平均路径长度,使网络表现出明显的小世界网络特征.考虑到移动代理访问传感器节点的顺序及数量对路由效率、网络寿命等有着重大影响,周四望等人^[109]提出了一种基于数据融合的移动代理曲线动态路由算法.该算法通过求解移动代理迁移过程中的静态最优路由节点序列,将移动代理路由问题转化为动态路径规划问题.

4.3 拓扑演化

拓扑演化是指通过配置硬件参数或扩大网络规模的方式,促使现有网络拓扑向抗毁性较优的方向演化.与网络重构方法所获网络拓扑具备典型异质性特征不同,拓扑演化所得网络拓扑均为同质网络,即节点与链路间彼此不存在明显差异.当前拓扑演化方法主要包含无标度网络生长与构建 k -连通网络.无标度网络生长的实质是通过引入新增节点,借助“偏好依附(Preferential Attachment)”机制,实现网络生长,从而保证生成网络拓扑具备无标度网络特征. k -连通网络则是通过调节节点发射功率,改善网络连通性能,使网络拓扑具有较好的抗毁性能.

4.3.1 无标度网络

无标度网络节点度分布 $p(k)$ 符合幂率分布,这就决定了网络中少数节点占用了绝大部分连接,而网络中绝大部分节点度数较低.因此,对于随机失效而言,占网络多数的度数较低的边缘末端节点的失

效概率明显高于少数度数较高的中心节点. 但度数较低的边缘末端节点的失效对网络整体通讯性能影响并不明显. 显然, 构建具有无标度网络特征的 WSNs 拓扑能够具有较好的容错性能.

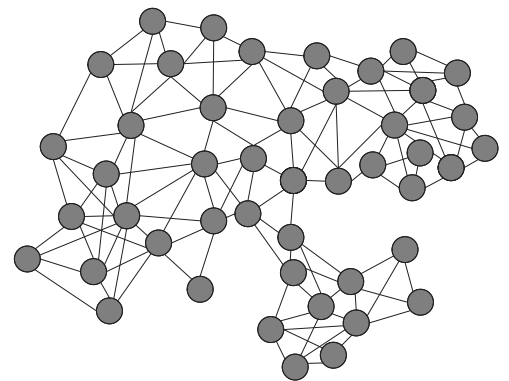
2003 年, Ishizuka 等人^[110] 针对 WSNs 提出一种节点度服从 $p(k) = k^{2/(\alpha-1)}$ 幂率分布的随机部署 (Stochastic Placement) 模型, 并验证当 $\alpha = 0.1$ 时, 网络容错能力最强. 但随机部署模型仅适用于大规模节点部署情形, 具有明显的应用局限性. Sarshar 等人^[111] 和 Kong 等人^[112] 分别通过在 Ad Hoc 网络中引入节点删除与链路补偿机制, 使网络在初始拓扑固定情形下, 通过动态演化, 具备无标度特征. 该研究为后续关于无标度 WSNs 拓扑演化研究提供了有益借鉴. 在此基础上, Zhu 等人^[113] 基于局域世界 (Local World) 模型, 分别提出两种面向无标度网络特征的 WSNs 演化模型: EAEM (Energy-Aware Evolution Model) 与 EBEM (Energy-Balanced Evolution Model). 在 EAEM 中, 新节点优先连接剩余能量较高的节点. 而在 EBEM 中, 除考虑节点剩余能量外, 新节点优先加入连接度较高的节点. 实验表明, EBEM 在能耗及容错性上明显优于 EAEM. 除此之外, 通过在生长机制中, 加入“有限支撑 (Finite Support)”约束, 限制单个节点拥有过多连边, 避免“赢者通吃 (Winner Takes All)”现象. 但在 EAEM 与 EBEM 模型中, 未考虑 WSNs 异质性特征, 即网络中簇头与 Sink 节点地位高于一般节点. 基于该考虑, Li 等人^[114] 提出一种异质 WSNs 演化模型, 新节点加入网络时, 优先选择簇头与 Sink 节点. 该模型在保持无标度网络特征的同时, 能够有效提升网络通讯效率, 降低后期路由设计复杂度. 上述演化模型均假设节点间通信采用最大功率传输半径, 但这种假设使得无标度 WSNs 局部通信链路过于密集, 从而造成网络通讯性能的下降. Qi 等人^[115] 所提 TEBAS (Topology Evolution Based on Adaptive Scale-free networks) 模型通过在决定节点优先选择的适用度函数 (Fitness Function) 中引入通讯半径参数, 使新节点加入网络时, 可根据加入结果, 动态调整通讯半径, 避免通讯干涉行为的发生.

现有关于 WSNs 无标度网络模型的研究大多数采用 BA 模型, 即通过遵循“偏好依附”原则的网络生长机制, 使网络节点度分布服从幂率分布. 陈力军等人^[116] 基于随机行走模型^[117], 提出一种全新的 WSNs 无标度网络模型 TERW (Topology Evolution

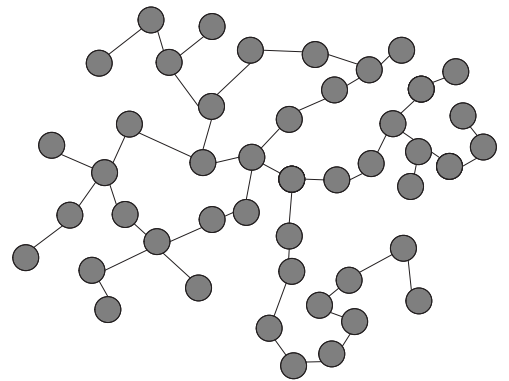
Random Walker), 尽管在文中未就 BA 模型进行性能比较, 但为后续研究提供了宝贵思路.

4.3.2 k -连通网络

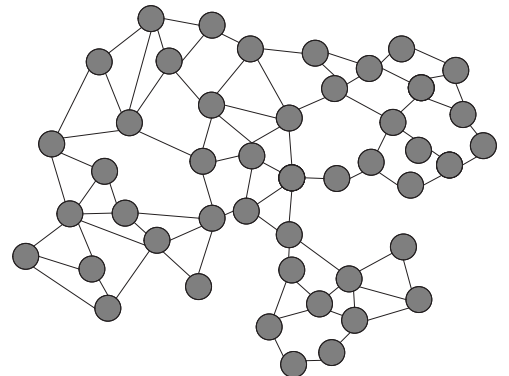
对于 WSNs 而言, 当节点均以最大传输功率进行通信时, 网络连通度最高. 以 k -连通图为例, 此时 k 值取其上限 (如图 8(a) 所示). 但这也将导致: (1) 节点能量快速消耗, 缩短网络工作寿命; (2) 加剧节点信号冲突与信道占用, 并最终影响通信质量. 尽管在 k -连通图中, $k-1$ 条链路的缺失, 不会改变图的连通性, 但如果仅仅依靠最小功率控制实现 WSNs 最小连通 (如图 8(b) 所示), 由于能量耗尽、节点故障等原因所导致的节点失效极易造成网络



(a) 采用最大功率的网络拓扑



(b) 最小功率控制的网络拓扑



(c) 2-连通的网络拓扑

图 8 不同控制条件下的网络拓扑情形

拓扑分割,网络抗毁性能较差.因此,功率控制的目标是在保证网络合理生命周期的前提下,生成一个优化的网络拓扑结构,提升 WSNs 抗毁性.功率控制方法在确保网络最小 k -连通的前提下,通过调节节点通信距离,降低网络中边的数量,达到优化网络拓扑结构的目的,以 $k=2$ 为例,如图 8(c) 所示. Kirousis 等人^[118]首先将功率控制问题简化为节点通信范围分配问题,即 TRA(Transmission Range Assignment)问题. TRA 问题的实质是在满足网络 k -连通的前提下最小化节点通信半径. 1 维空间下 TRA 问题的算法复杂度为 $O(n^4)$, 2 维和 3 维空间下 TRA 问题被证明是 NP-Hard. 因此,与中继节点布设问题类似,基于 k -连通的功率控制方法偏向于在合理算法复杂度前提下,寻找保持网络 k -连通的趋向最优近似解. Jia 等人^[119]提出一种基于 K -means 聚类近似常数的拓扑控制算法,生成具有较低能耗的 k -连通网络,并给出严格理论推导. 在假定传感器节点具备角度识别功能前提下, Li 等人^[120]提出 YAO 算法,生成 k -连通网络,但对传感器节点硬件配置具有较高要求. 类似算法还包括 CTC(Configurable Topology Control)^[121]、FLSS(Fault-tolerant Local Spanning Subgraph)^[122]等. 以上拓扑控制算法均假设全局网络信息已知,采用集中式控制,但对于大规模 WSNs 而言,以上假设通常不成立. 时锐等人^[123]基于邻居集合提出分布式功率控制算法 LKINDP(Localized K Internal Node Disjoint Paths).

在该算法中,网络拓扑能够保证最小化节点通信半径,但算法证明前提仍为集中式. 在 LKINDP 算法基础上,徐强等人^[124]分别基于全局信息与局部信息给出分布式功率控制算法 GDTPC(Global Knowledge based Distributed Transmit Power Control)和 LDTPC(Localized Distributed Transmit Power Control). 算法通过从初始网络拓扑中删除长程通讯链路,获得可靠拓扑结构,但这将有可能导致网络中存在不对称链路.

4.4 抗毁性策略性能比较

由表 3 可知,基于冗余机制(簇头冗余、链路冗余)的抗毁性策略对任务场景具有较强适应性,无需花费额外成本. 这是由于簇头冗余与链路冗余策略均充分利用了 WSNs 节点冗余度较高这一特有属性. 但节点间通信路径的增加与通信频率的上升加重了网络负担,导致节点故障发生概率上升与网络通讯性能下降. 中继节点策略通过在网络中引入功能更为强大的节点分担普通节点的通信负载,能够有效提升网络性能,但是中继节点一旦部署,位置很难改变,因此,对于拓扑动态变化的 WSNs,中继节点策略具有明显局限性. 除此之外,在网络中添加中继节点也将导致网络硬件成本的上升. 考虑到攻击者在制订网络攻击策略时,为最大程度降低网络性能,会优先攻击中继节点. 因此,中继节点策略应对被选择性受损类型时,网络抗毁性表现较差.

表 3 网络抗毁性策略比较分析

策略	网络时延	网络生存周期	网络建设成本	场景适应性	可应对网络受损类型
簇头冗余	无明显影响	显著降低	无明显影响	较强	随机性受损、被选择性受损、组织性受损
链路冗余	无明显影响	显著降低	无明显影响	较强	随机性受损、被选择性受损、组织性受损
中继节点	显著降低	显著上升	增加	一般	随机性受损、组织性受损
长程连接	显著降低	显著上升	增加	较差	随机性受损、组织性受损
移动代理	显著上升	显著上升	增加	较强	随机性受损、被选择性受损、组织性受损
无标度网络	无明显影响	无明显影响	无明显影响	较强	被选择性受损、组织性受损
k -连通	无明显影响	显著降低	无明显影响	较强	随机性受损、被选择性受损、组织性受损

基于复杂网络理论的移动代理和长程连接策略可显著提升网络的生命周期,这是由于这两种策略所构建的网络拓扑具有明显的小世界网络特征. 传感器节点至 Sink 节点的平均路径明显缩短,因而网络整体能耗与单个节点的通信负载显著下降. 但二者对网络时延影响差异明显. 移动代理策略的传递时延取决于代理节点的移动速度,但代理节点的移动速度明显低于信号的传播速度,因而传递时延更为明显. 长程连接策略利用线缆方式的长程连接代替代理节点,能够显著降低传递时延. 移动代理和长

程连接策略均需要在初始网络中引入额外的基础设施,因而网络硬件成本均有显著上升. 在移动代理策略中,移动代理运动轨迹可跟据网络拓扑结构的动态变化实时调整,而在长程连接策略中,长程连接一旦部署很难改变其位置,因此,移动代理策略的场景适应性远高于长程连接策略. 在面对选择性攻击时,由于长程连接静态布设,因而更容易遭受攻击. 与之相比,在移动代理策略中,代理节点可自由移动且运动轨迹通常依照网络拓扑的变化而发生改变,更加难以捕捉. 当面临被选择性受损类型时,网络抗毁性

能表现更优.

基于 k -连通的抗毁性策略采用功率控制提升网络连通性. 在该策略中, 抗毁性能高低取决于 k 值大小. 在维持抗毁性较优的同时, k 值增大将会导致网络生存周期的明显下降. 无标度网络的拓扑演化策略基于“偏好依附”原则, 构建网络生长机制. 与其他策略相比, 未引起网络额外开销且具有较强适应性, 性能较优. 网络中少数中心节点占据了绝大部分连接, 这保证了网络具有较强容错能力. 但在应对中心节点受到攻击情形时, 易造成网络性能的急剧下降. 因此, 在应对被选择性受损类型时, 网络抗毁性能表现较差.

5 故障检测与修复

提升网络抗毁性能可被视为保障网络可持续稳定提供服务的“预防”措施. 这也是本文的研究重点. 但显然, 当网络受损而导致服务能力下降时, 如何快速有效地发现失效节点并采取合理措施修复网络, 对于提升网络抗毁性能同样具有十分重要的理论与应用价值. 如图 9 所示, 故障检测根据任务执行主体的不同可分为集中式检测和分布式检测. 故障修复按照执行手段的不同可分为冗余节点替换与移动节点部署.

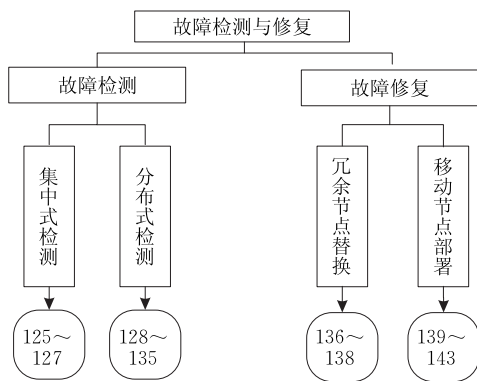


图 9 故障检测与修复研究内容分类

5.1 故障检测

5.1.1 集中式检测

集中式检测由中心管理节点负责对网络进行监控, 追踪失效节点. 集中式方法主要采用周期性主动轮询方式进行检测. 在集中式检测中, 通常由 Sink 节点通过定期轮询获取网络内所有传感器节点的状态信息, 并对获取信息进行比对分析, 确定节点失效行为是否发生. Ruiz 等人^[125]提出集中式 WSNs 故障管理架构 MANNA. 框架定期选取剩余能量较高

的节点作为管理节点负责采集网络节点状态信息, 并以此作为故障检测依据. 在此基础上, Ramanathan 等人^[126]利用 Sink 节点能量不受限这一特征, 通过设置传感器节点定期向 Sink 节点传递故障检测数据包, 由 Sink 节点将故障检测数据与环境监测数据进行整合, 并基于事件内容的时空相关性, 检测节点失效行为. Lee 等人^[127]提出另一种集中式架构 WinMS. 架构中包含本地网络管理方案与中心网络管理方案, 其中本地网络管理方案负责节点自身管理, 中心网络管理方案用于获取网络状态信息并进行故障管理. 尽管 WinMS 由于采用树形结构, 具备一定分布式特征. 但因为故障检测等复杂任务仍由单一中心管理节点完成, 所以仍属于典型集中式架构.

总体而言, 与其他 WSNs 集中式管理方法类似, 集中式检测由于将所有的检测任务均集中在单一中心节点, 导致中心节点工作负担过重, 而且由于大量原始数据在网络上传输, 造成大量额外通信开销, 对网络寿命及工作效率造成影响.

5.1.2 分布式检测

与集中式检测相比, 分布式检测通过节点协作实现故障检测, 能够将复杂的故障检测任务平滑地分配至各个节点. 显然, 传感器节点自身所承担的决策任务越多, 网络负载则越轻. 曹晓梅等人^[128]在构建简单高效的独立流量预测模型基础上, 提出一种基于流量预测的异常检测方案. 若传感器节点实时观测到流量与预期流量差异明显, 则判定异常发生. 该方案优势在于节点无需特殊硬件支持, 且实时性较优. 但方案涉及分组到达速率等四组特征阈值, 阈值设定合适与否将直接影响检测精度. 文献^[129]所提的检测方法考虑 WSNs 典型分簇结构, 将故障检测任务分散至各个单元簇内完成. 簇内由簇头节点通过定期广播检测并定位故障节点, 而簇头节点的故障检测则可通过与邻居簇头节点的定期数据交换来实现. 但显然, 若簇内成员节点众多, 则簇头节点所承担负载依旧较重. Sheth 等人^[130]给出了网络平面结构下的故障检测方法, 其核心思想为将节点所获故障信息与邻居节点获得的故障信息进行比较, 在得到确认后, 才将最终故障信息发送至 Sink 节点, 避免误报警事件的发生. 与文献^[129]相比, 网络因故障检测所产生的能耗分布更加均匀, 且检测精度有明显上升. 与之类似, Ding 等人^[131]也提出了一种分布式检测方法, 用于识别可疑或故障节点. 如果传感器节点所感知数据与其邻居节点差异明显, 则将

该节点诊断为故障节点. 但显然, 如果网络的失效形式为区域关联失效或该节点周边有超过一半邻居节点为失效节点, 则该算法无法有效监测节点失效行为发生. 基于该考虑, Chen 等人^[132]对此进行改进, 选择网络中健康节点进行比较, 并将已诊断健康节点数据传播到整个网络, 从而以此为参照物, 诊断其他待检测节点状态. 该算法在一半邻居节点故障等极端情况下, 依旧能够识别故障节点. 但在 Chen 等人所提算法中, 仅通过判断待检测节点与健康节点的观测数据差值是否处于门限值范围内来判断节点状态, 检测结果仍存在明显误差. Choi 等人^[133]则引入了置信度概念. 通过分析邻居节点的历史数据来计算邻居节点的置信度, 并以此为依据选择健康节点与待检测节点进行比对. 上述研究均采用单跳范围内的邻域节点作为样本, 进行数据比对. 但事实上, 即使在单跳范围内, 节点间彼此地理位置的差异, 也将造成检测数据的明显不同. 基于该考虑, Guo 等人^[134]所提的 FIND 算法, 通过将所接收监测数据进行排序, 并与单跳邻居节点的地理位置序列进行对比, 若序列间顺序差异明显, 则认定节点失效. 与之前相关研究相比, FIND 算法考虑地理位置信息融合, 监测精度有明显提升. 考虑在多数场景下, 受制于硬件成本限制, 传感器节点无法获取自身与周边节点的地理位置信息. 因此, 黄庭培等人^[135]提出一种基于监督学习理论的故障识别算法, 将 RSSI (Received Signal Strength Indicator) 与 LQI (Link Quality Indicator) 所组成的特征向量作为输入, 替代原有地理位置输入, 通过离线训练与检验, 实现故障快速检测与识别. 该方法在保证检测精度的同时, 具有较强的场景适用性.

5.2 故障修复

5.2.1 冗余节点替换

冗余节点替换的核心思想是若某个传感器节点发生故障, 则通过唤醒故障节点周边处于休眠状态的冗余节点, 使其代替故障节点继续工作. 在文献^[136-138]等相关文献中, 往往通过设置大量的额外监控节点实现网络的故障修复. 当监控节点感知周边传感器节点发生故障, 则替代故障节点进行工作. 但该类方法对节点冗余度要求较高, 部署代价花费明显. WSNs 作为以数据为中心的任务驱动型网络, 其关注的重点是整个监测区域的数据采集与覆盖情况, 并不关注单个节点状态与所获取的数据. 基于该考虑, 在设置冗余节点时, 针对关键节点如簇头等采取备份机制, 网络修复效果更为显著. 相关研究

成果已在 4.1.1 节有关簇头冗余的研究现状描述中给予详细介绍, 在此不再赘述. 尽管冗余节点替换对网络故障响应速度较快, 但是在目前的研究工作中, 仍存在明显技术瓶颈, 如对于稀疏覆盖的区域, 一旦节点发生故障, 周围可供其使用的冗余节点往往难以满足故障恢复的要求.

5.2.2 移动节点部署

移动节点部署是通过在网络中设置可移动节点动态调整网络拓扑. 当传感器节点发生故障时, 移动节点前往故障节点所在区域, 负责维持网络继续连通. 特别是随着传感器与执行器网络 (Wireless Sensor and Actor Networks, WSNs) 的研究深入, 通过移动节点部署进行故障修复得到了广泛的研究. Abbasi 等人^[139]首先于 2009 年提出的 DARA (Distributed Actor Recovery Algorithm) 的连接恢复策略, 将节点的移动距离作为评价指标, 通过构建最小移动节点集合, 采用分布式自主决策方式, 修复因节点故障所引发的连接中断问题. 针对网络最小连通度要求, Abbasi 等人分别提出了满足 1-连通与 2-连通的 DARA-1C 和 DARA-2C 策略. 但 DARA 策略中并未涉及 k -连通 ($k > 2$) 问题. 基于该考虑, Wang 等人^[140]与 Imran 等人^[141]分别对 DARA 策略进行补充, 从而使移动节点仅需要通过局部移动就可以填补网络因节点故障所产生的监测盲区. 但上述 3 种方法均优先考虑选取移动距离与节点度最小的节点前往到故障节点位置, 从而可能引发级联移动问题, 并最终造成其他移动节点伴随产生移动, 导致过度能量消耗. 当前有关利用移动节点部署对 WSN 进行修复的研究成果众多, 文献^[142-143]都对相关研究现状作了较好归纳. 总体而言, 由于移动节点部署对不同网络应用场景具有较强适应性, 且可随时根据故障类型更改修复策略, 具有广阔的研究与应用前景.

6 技术挑战

最早与 WSNs 抗毁性相关的论文成果可追溯至 1998 年^[144], 尽管目前有越来越多的学者针对 WSNs 抗毁性及其相关问题展开研究并取得一定成果. 但总体上, 抗毁性研究仍处于探索阶段, 且成果仍以理论研究为主, 相关应用转化成果较少. 特别是在考虑 WSNs 实际特征的综合失效模型及选取合适 WSNs 抗毁性测度等方面仍面临诸多技术挑战, 已有研究成果仍有待改善的空间, 如表 4 所示.

表 4 WSNs 抗毁性研究所面临的技术挑战

受损类型	网络随机性受损与被选择性受损等受损类型均可通过数学建模予以准确表述,但组织性受损依照初始网络拓扑不同,存在明显差异,且具备明显的动态性特征. 针对组织性受损建模是网络受损建模的主要技术挑战.	
受损起因	在真实场景下,网络受损是多种节点失效情形共同作用的结果,但各个失效情形对网络受损所施加的影响各不相同,存在主次之分. 如何在复杂的网络受损环境下,确定引起网络受损的主要起因,是有针对性构建抗毁性提升方法的前提.	
受损成因与情况	<p>短时故障失效</p> <p>综合建模</p>	<p>现有短时故障失效研究仅简单将故障发生与恢复设定为依照简单概率事件触发. 但在真实场景下,故障发生时长和频率与节点通讯关联密切. 如何采用数学模型,准确表述二者之间的有机关联,使其符合真实场景,将是未来研究短时故障失效所需要面对的主要技术挑战.</p> <p>现有相关节点失效研究,往往简单假设节点仅存在单一失效情形,与真实场景差异明显. 为保证所构建节点失效模型尽可能贴近真实应用场景,需要综合考虑多种节点失效情形. 因此,在构建过程中,应针对攻击失效,选择合适的攻击策略,针对能耗与故障失效,构建节点实际能耗与故障失效模型,并在此基础上,考虑真实节点失效情形,引入时间域选择,实现短时与长时失效行为之间的状态转换.</p>
分簇结构相关	现有与分簇结构相关抗毁性测度研究均简单假定网络拓扑结构固定. 但在多数分簇协议中,网络分簇结构动态变化. 如何在动态网络环境下,提取基本簇单元并评估全网抗毁性能是与分簇结构相关抗毁性测度研究的主要技术挑战.	
抗毁性测度	<p>剩余能量相关</p> <p>分层抗毁性测度</p> <p>算法复杂度</p>	<p>现有剩余能量相关的抗毁性测度研究通过赋予剩余能量权重使评估结果更为全面,但如何确定剩余能量因子与其他影响因子的权重分配是抗毁性测度评估是否准确的核心关键问题.</p> <p>现有测度研究往往就单一网络类型或网络单一性能表现进行评估,具有明显局限性. 建立分层抗毁性测度能够避免现有测度在多维度及局部测量上的短板,构建分层抗毁性测度方法是未来抗毁性测度研究的主要趋势.</p> <p>现有多数测度均采用介数、平均路径或连通度作为抗毁性测度的关键影响因子,但对于大规模网络而言,获取介数等因子计算量巨大,存在现实困难. 因此,如何合理控制测度复杂度是提升抗毁性测度实用性的关键.</p>
路由控制	基于冗余策略的路由控制方法以牺牲网络路由性能及增加能耗作为代价换取网络抗毁性能的提升,因此,如何在提升抗毁性能的同时,降低对网络性能影响是路由算法设计过程中的主要技术挑战.	
抗毁性提升方法	<p>网络重构</p> <p>拓扑演化</p>	<p>网络重构实质是以强化节点与链路性能提升网络抗毁性. 现有研究主要从拓扑角度提升网络抗毁性能. 但实际在改造或引入网络基础设施的同时,路由复杂度上升明显. 如何有针对性的构建高效路由是亟待解决的关键问题.</p> <p>拓扑演化借助发射频率与网络生长控制,提升网络抗毁性能. 通过功率控制实现网络 k-连通作为 NP-Hard 问题,借助启发式算法寻找最优解是研究的重点方向. 而网络生长机制则应通过引入地理位置与节点密度等相关约束条件,使生长结果更加贴近于真实网络.</p>
故障检测与修复	<p>故障检测</p> <p>移动节点部署</p>	<p>在传统 Internet 中,若网络发生故障,能够快速凭借内在故障检测机制确定故障发生位置,并确定故障来源. 与之相比,现有 WSNs 故障检测研究,往往仅能就节点或网络是否发生故障及基本故障类型给出大致判断,对于故障精确诊断及故障来源分析的研究较为匮乏,为后续有针对性采取故障修复手段造成技术挑战.</p> <p>现有相关研究工作主要针对如何确保移动节点沿最优路径到达故障地点,避免过度能耗. 但在多数场景下,WSNs 网络受损往往不仅仅是由单一的节点失效引起的,往往需要多个移动节点通过协同合作的方式完成修复任务. 因此,如何对网络受损状况进行评估,并进行任务分割与分配,从而保证多个移动节点协同完成复杂修复任务,将是通过移动节点部署实现故障修复所面临的主要技术挑战.</p>

(2) 级联失效研究

当前 WSNs 抗毁性研究主要从静态角度,研究移除点或边对网络拓扑的影响,并未考虑网络的动态性过程. 但在现实 WSNs 中,网络拓扑结构的改变会导致网络数据流的重新分配,进而引发网络通讯负载的动态变化. 受制于硬件成本,传感器节点往往链路带宽受限. 当实时通讯负载高于节点额定载荷,将导致节点因链路堵塞而引发过载失效. 而节点失效的发生将导致网络负载再次分配,进而可能造成其他节点因过载而失效,从而引发新一轮的负载分配,并最终导致网络大规模级联失效的发生. 当前针对 WSNs 级联失效的研究依旧较为匮乏. 如何将已有静态抗毁性研究中的理论与方法推广至具有动态网络特征的级联失效抗毁性研究,或者建立新的理论与方法,是下一步 WSNs 抗毁性研究需要关注的重点.

7 展 望

抗毁性作为制约 WSNs 规模应用的关键瓶颈之一,针对 WSNs 的抗毁性研究将会不断升温. 多学科理论与方法的渗入及面向应用需求的深入研究将是该领域发展的必然趋势.

(1) 真实世界情形下网络抗毁性建模

在现有关于 WSNs 抗毁性研究中,往往仅将节点与边对网络的拓扑约束及能耗约束作为网络约束条件. 但是在真实网络情形下,除上述约束条件外,节点能否正常工作仍受自身缓存大小影响,而边则受地理位置约束. 除此之外,网络间信息传递仍存在信号干扰与信道冲突等问题. 因此,全面考虑各种因素影响,有助于建立更贴近真实场景的 WSNs 抗毁性模型.

(3) 微观机理研究

真实网络中普遍存在的群聚属性(Clusters)、社会属性(Social Attributes)等为研究真实网络微观结构提供了宝贵思路,但对于 WSNs 抗毁性研究而言,现有研究成果的立足点仍是从全局网络入手分析网络抗毁性能.对规模网络下的微观或局部结构缺乏深入认识.如何从微观角度对网络失效行为的时空演化规律进行分析将是提升 WSNs 抗毁性研究水平的重要理论研究方向.

(4) 复杂网络理论应用

尽管小世界网络与无标度网络等经典复杂网络理论为 WSNs 抗毁性研究提供了良好借鉴,但由于在传统复杂网络研究中,通常以对等网络为研究对象,网络中点与边并没有被赋权.而 WSNs 信息流动具有明显汇聚特征,且往往因典型分簇结构而带有明显异质特征.因此,以往面向单层网络模型的复杂网络研究成果对于 WSNs 而言,带有明显局限性.我们需要以 WSNs 与一般关系网络的“共性”角度入手,探索 WSNs 的“特殊性”,以实际网络为背景,对其抗毁性进行建模、分析、优化与控制.

(5) 信息安全机制研究

对于 WSNs 而言,当攻击者掌握网络全局或局部信息,就可以采取对己方最为有利的攻击策略对网络展开攻击.虽然 WSNs 抗毁性研究是以网络拓扑为对象,提升网络在应对点或边移除等情况下可持续提供服务的能力.但保障网络信息安全,可以有效避免因信息泄露使攻击者制订精确攻击策略.因此,如何运用数据加密、安全检测、节点认证和数据一致性校验等方法保证网络信息安全,并将相关研究与现有 WSNs 抗毁性研究成果相结合,是全面提升 WSNs 抗毁性的重要研究方向.

8 结束语

结构决定功能,抗毁性作为 WSNs 规模化应用的关键瓶颈,其研究具有重要的理论及应用价值.围绕 WSNs 抗毁性研究需要解决的 3 个科学问题,本文总结了国内外相关领域学者在 WSNs 抗毁性研究方面取得的进展,分析了其面临的技术挑战和发展趋势.尽管 WSNs 抗毁性研究在过去几年取得了重大进展,但绝大多数研究成果仍为理论研究,而 WSNs 技术的快速发展与推广为抗毁性研究提供了丰富的应用平台,可以预见随着抗毁性技术的不断成熟,相关研究成果将逐步走向应用,并推动 WSNs 技术的发展.

致谢 审稿专家与编辑为本文提供了宝贵的修改意见和建议,作者在此表示最诚挚的感谢!

参 考 文 献

- [1] Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks. *Nature*, 2000, 406(6794): 378-382
- [2] Tan Yue-Jin, Wu Jun, Deng Hong-Zhong, et al. Invulnerability of complex networks: A survey. *Systems Engineering*, 2006, 24(10): 1-5(in Chinese)
(谭跃进, 吴俊, 邓宏钟等. 复杂网络抗毁性研究综述. *系统工程学报*, 2006, 24(10): 1-5)
- [3] Zheng B, Huang D, Li D, et al. Some scale-free networks could be robust under selective node attacks. *Europhysics Letters*, 2011, 94(2): 28010
- [4] Tan Yue-Jin, Wu Jun, Deng Hong-Zhong. Progress in invulnerability of complex networks. *Journal of University of Shanghai Science and Technology*, 2011, 33(6): 653-668(in Chinese)
(谭跃进, 吴俊, 邓宏钟. 复杂网络抗毁性研究进展. *上海理工大学学报*, 2011, 33(6): 653-668)
- [5] Chen C, Wang Y. The invulnerability of emergency logistics network based on complex Network//Luo J ed. *Affective Computing and Intelligent Interaction*. Berlin Heidelberg: Springer, 2012: 789-797
- [6] Anastasi G, Conti M, Di Francesco M, et al. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 2009, 7(3): 537-568
- [7] Mottola L, Picco G P. Programming wireless sensor networks: Fundamental concepts and state of the art. *ACM Computing Surveys (CSUR)*, 2011, 43(3): 19
- [8] Fu X, Li W, Yang L. Design and implementation of fire-alarming system for indoor environment based on wireless sensor networks//Proceedings of the 2013 Chinese Intelligent Automation Conference. Yangzhou, China, 2013: 457-468
- [9] Mishkovski I, Biey M, Kocarev L. Vulnerability of complex networks. *Communications in Nonlinear Science and Numerical Simulation*, 2011, 16(1): 341-349
- [10] Paul G, Sreenivasan S, Stanley H E. Resilience of complex networks to random breakdown. *Physical Review E(Statistical, Nonlinear, and Soft Matter Physics)*, 2005, 72(5): 056130. 1-056130. 6
- [11] Criado R, Flores J, Hernández-Bermejo B, et al. Effective measurement of network vulnerability under random and intentional attacks. *Journal of Mathematical Modelling and Algorithms*, 2005, 4(3): 307-316
- [12] Cohen R, Erez K, Ben-Avraham D, et al. Breakdown of the Internet under intentional attack. *Physical Review Letters*, 2001, 86(16): 3682
- [13] Wasserman S. *Social Network Analysis: Methods and Applications*. UK: Cambridge University Press, 1994
- [14] Okamoto K, Chen W, Li X Y. Ranking of closeness centrality for large-scale social networks//Preparata F P. *Frontiers in Algorithmics*. Berlin Heidelberg: Springer, 2008: 186-195

- [15] Newman M E J. A measure of betweenness centrality based on random walks. *Social Networks*, 2005, 27(1): 39-54
- [16] Bonacich P. Some unique properties of eigenvector centrality. *Social Networks*, 2007, 29(4): 555-564
- [17] Guimera R, Mossa A, Turttschi A, et al. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *National Academy Sciences*, 2005, 102(22): 7794-7799
- [18] Opsahl T, Agneessens F, Skvoretz J. Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, 2010, 32(3): 245-251
- [19] Newman M E J, Forrest S, Balthrop J. Email networks and the spread of computer viruses. *Physical Review E*, 2002, 66(3): 035101
- [20] Cetinkaya E K, Broyles D, Dandekar A, et al. Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach. *Telecommunication Systems*, 2011, 52(2): 751-766
- [21] Li Yong, Wu Jun, Tan Yue-Jin. Critical invulnerability study for cascading failure of tactical logistics networks. *Journal of System Simulation*, 2012, 24(5): 1030-1034 (in Chinese)
(李勇, 吴俊, 谭跃进. 物流保障网络级联失效临界抗毁性. 系统仿真学报, 2012, 24(5): 1030-1034)
- [22] Fu X, Li W, Fortino G. Empowering the invulnerability of wireless sensor networks through super wires and super nodes//Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). Delft, Netherlands, 2013: 561-568
- [23] Li Fang-Min, Xu Wen-Jun, Liu Wen-Hua. Power control for wireless sensor networks. *Journal of Software*, 2008, 19(3): 716-732 (in Chinese)
(李方敏, 徐文君, 刘新华. 无线传感器网络功率控制技术. 软件学报, 2008, 19(3): 716-732)
- [24] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks//Proceedings of the 33rd Annual International Conference on System Sciences. Hawaii, USA, 2000: 1-10
- [25] Lindsey S, Raghavendra C S. PEGASIS: Power-efficient gathering in sensor information systems//Proceedings of the IEEE Aerospace conference. Los Angeles, USA, 2002: 1125-1130
- [26] Wang Liang-Min, Ma Jian-Feng, Wang Chao. Degree of fault-tolerance and intrusion-tolerance for topologies of wireless sensor networks. *Acta Electronica Sinica*, 2006, 34(8): 1446-1451 (in Chinese)
(王良民, 马建峰, 王超. 无线传感器网络拓扑的容错度与容侵度. 电子学报, 2006, 34(8): 1446-1451)
- [27] Lin Li-Wei, Xu Li, Ye Xiu-Cai. A novel method and its simulation to evaluate the invulnerability of wireless sensor networks. *Computer System & Applications*, 2010, 19(4): 32-36 (in Chinese)
(林力伟, 许力, 叶秀彩. 一种新型 WSN 抗毁性评价方法及其仿真实现. 计算机系统应用, 2010, 19(4): 32-36)
- [28] Fu Xiu-Wen, Li Wen-Feng, Yang Lin, et al. Analysis of invulnerability of wireless sensor networks based on cellular automata. *Computer Engineering and Applications*, 2014, 50(8): 1-6 (in Chinese)
(符修文, 李文锋, 杨林等. 基于元胞自动机无线传感器网络抗毁性分析. 计算机工程与应用, 2014, 50(8): 1-6)
- [29] Fu Xiu-Wen, Li Wen-Feng. Analysis of invulnerability of wireless fire-alarming network and methods of improving it. *China Safety Science Journal*, 2014, 24(1): 41-47 (in Chinese)
(符修文, 李文锋. 无线消防报警网络抗毁性分析与提升方法. 中国安全科学学报, 2014, 24(1): 41-47)
- [30] Ren Xiu-Li, Deng Cai-Li. Topology control algorithm of wireless sensor network based on cellular automata. *Journal of Computer Applications*, 2012, 32(6): 1495-1498 (in Chinese)
(任秀丽, 邓彩丽. 基于元胞自动机的无线传感网络拓扑控制算法. 计算机应用, 2012, 32(6): 1495-1498)
- [31] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 2002, 1(4): 660-670
- [32] Yin Rong-Rong, Liu Bin, Liu Hao-Ran, et al. The fault-tolerant topology control approach in wireless sensor networks based on integrated fault model of node. *Journal of Electronics & Information Technology*, 2012, 34(10): 2375-2381 (in Chinese)
(尹荣荣, 刘彬, 刘浩然等. 基于节点综合故障模型的无线传感器网络容错拓扑控制方法. 电子与信息学报, 2012, 34(10): 2375-2381)
- [33] Wu J, Deng H Z, Tan Y J, et al. Vulnerability of complex networks under intentional attack with incomplete information. *Journal of Physics A: Mathematical and Theoretical*, 2007, 40(11): 2665
- [34] Xiao S, Xiao G. On intentional attacks and protections in complex communication networks//Proceedings of the Global Telecommunications Conference. San Francisco, USA, 2006: 1-5
- [35] Xia Y X, Jin F. Efficient attack strategy to communication networks with partial degree information//Proceedings of the IEEE International Symposium Circuits and Systems (ISCAS). Rio de Janeiro, Brazil, 2011: 1588-1591
- [36] Holme P, Kim B J, Yoon C N, et al. Attack vulnerability of complex networks. *Physical Review E*, 2002, 65(5): 056109
- [37] Pezoa J E. Optimizing mission allocation in wireless sensor networks under geographically correlated failures//Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems. New York, USA, 2013: 57-63
- [38] Azimi N H, Gupta H, Hou X, et al. Data preservation under spatial failures in sensor network//Proceedings of the 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York, USA, 2010: 171-180

- [39] Liu J, Jiang X, Nishiyama H, et al. Reliability assessment for wireless mesh networks under probabilistic region failure model. *IEEE Transactions on Vehicular Technology*, 2011, 60(5): 2253-2264
- [40] Sen A, Murthy S, Banerjee S. Region-based connectivity — A new paradigm for design of fault-tolerant networks// *Proceedings of the 2009 IEEE International Conference on High Performance Switching and Routing*. Paris, France, 2009: 1-7
- [41] Rahnamay-Naeini M, Pezoa J E, Azar G, et al. Modeling stochastic correlated failures and their effects on network reliability// *Proceedings of the 20th IEEE International Conference on Computer Communications and Networks*. Hawaii, USA, 2011: 1-6
- [42] Ágoston V, Csermely P, Pongor S. Multiple weak hits confuse complex systems; A transcriptional regulatory network as an example. *Physical Review E*, 2005, 71(5): 051909
- [43] Yin Y P, Zhang D M, Tan J, et al. Continuous weight attack on complex network. *Communications in Theoretical Physics*, 2008, 49(3): 797-800
- [44] Masoum A, Jahangir A H, Taghikhaki Z. Survivability analysis of wireless sensor network with transient fault// *Proceedings of the International Conference on Computational Intelligence for Modelling Control & Automation*. Vienna, Austria, 2008: 975-980
- [45] Parvin S, Hussain F K, Park J S, et al. A survivability model in wireless sensor networks. *Computers & Mathematics with Applications*, 2012, 64(12): 3666-3682
- [46] Tan Yue-Jin, Zhao Juan, Wu Jun, Deng Hong-Zhong, et al. Review on the network reliability based on paths. *System Engineering-Theory & Practice*, 2012, 32(12): 2724-2730 (in Chinese)
(谭跃进, 赵娟, 吴俊, 邓宏钟等. 基于路径的网络可靠性研究综述. *系统工程理论与实践*, 2012, 32(12): 2724-2730)
- [47] Newman M E J. The structure and function of complex networks. *SIAM Review*, 2003, 45(2): 167-256
- [48] Yazdani A, Jeffrey P. A complex network approach to robustness and vulnerability of spatially organized water distribution networks. *Physics and Society*, 2010, 15(2): 1-18
- [49] Ma Run-Nian, Wen Gang, Shao Ming-Zhi, et al. Evaluation method of invulnerability of weighted network based on measurements of invulnerability. *Application Research of Computers*, 2013, 30(6): 1802-1804 (in Chinese)
(马润年, 文刚, 邵明志等. 基于抗毁性测度的赋权网络抗毁性评估方法. *计算机应用研究*, 2013, 30(6): 1802-1804)
- [50] Chiang M W, Zilic Z, Radecka K, et al. Architectures of increased availability wireless sensor network nodes// *Proceedings of the 2004 International Test Conference of IEEE Computer Society*. Montreal, Canada, 2004: 1232-1241
- [51] Zhu C, Zheng C L, Shu L, et al. A survey on coverage and connectivity issues in wireless sensor networks. *Journal of Network and Computer Applications*, 2012, 35(2): 619-632
- [52] Mustapha R S, Abdelhamid M, Hadj S, et al. Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols. *Journal of Networks and Computer Applications*, 2012, 35(4): 1317-1328
- [53] Frank H, Frisch I. Analysis and design of survivable networks. *IEEE Transactions on Communication Technology*, 1970, 18(5): 501-519
- [54] Tan Yue-Jin, Wu Jun, Deng Hong-Zhong. Evaluation method for node importance based on node contraction in complex networks. *System Engineering-Theory & Practice*, 2006, 26(11): 79-83 (in Chinese)
(谭跃进, 吴俊, 邓宏钟. 复杂网络中节点重要度评估的节点收缩方法. *系统工程理论与实践*, 2006, 26(11): 79-83)
- [55] Guo Hong, Lan Ju-Long, Liu Luo-Kun. Research of metrics of Ad Hoc networks invulnerability considering node importance assessment. *Journal of Chinese Computer Systems*, 2010, 31(6): 1063-1066 (in Chinese)
(郭虹, 兰巨龙, 刘洛琨. 考虑节点重要度的 Ad Hoc 网络抗毁性测度研究. *小型微型计算机系统*, 2010, 31(6): 1063-1066)
- [56] Guo Wei. Reliability evaluating method of tactical commutation network. *Acta Electronica Sinica*, 2000, 28(1): 3-6 (in Chinese)
(郭伟. 野战地域通信网可靠性的评价方法. *电子学报*, 2000, 28(1): 3-6)
- [57] Rao Yu-Ping, Lin Jing-Yu, Hou De-Ting. Evaluation method for network invulnerability based on shortest route number. *Journal on Communications*, 2009, 30(4): 113-117 (in Chinese)
(饶育萍, 林竞羽, 侯德亭. 基于最短路径数的网络抗毁评价方法. *通信学报*, 2009, 30(4): 113-117)
- [58] Wu Jun, Tan Suo-Yi, Tan Yue-Jin, et al. Analysis of invulnerability in complex networks. *Complex Systems and Complexity Science*, 2014, 11(1): 78-86 (in Chinese)
(吴俊, 谭索怡, 谭跃进等. 基于自然连通度的复杂网络抗毁性分析. *复杂系统与复杂性科学*, 2014, 11(1): 78-86)
- [59] Bao Xue-Cai, Dai Fu-Sheng, Han Wei-Zhan. Evaluation method of network invulnerability based on disjoint paths in topology. *System Engineering and Electronics*, 2012, 34(1): 168-174 (in Chinese)
(包学才, 戴伏生, 韩卫占. 基于拓扑的不相交路径抗毁性评估方法. *系统工程与电子技术*, 2012, 34(1): 168-174)
- [60] Wu Jun, Tan Yue-Jin. Study on measure of complex network invulnerability. *Journal of System Engineering*, 2005, 20(2): 128-131 (in Chinese)
(吴俊, 谭跃进. 复杂网络抗毁性测度研究. *系统工程学报*, 2005, 20(2): 128-131)
- [61] He Ming, Dong Qiang, Yuan Li-Miao, et al. Model for evaluating reliability of wireless sensor networks. *Journal of PLA University of Science and Technology (Nature Science Edition)*, 2010, 11(4): 393-396 (in Chinese)
(何明, 董强, 袁黎苗等. 无线传感器网络的可靠性评估模型. *解放军理工大学学报(自然科学版)*, 2010, 11(4): 393-396)

- [62] Xing L, Shrestha A. QoS reliability of hierarchical clustered wireless sensor networks//Proceedings of the 25th IEEE International Conference on Performance, Computing, and Communications. Phoenix, USA, 2006: 641-646
- [63] Li Peng-Xiang, Ren Yu-Qing, Xi You-Min. An importance measure of actors (set) within a network. *System Engineering*, 2004, 22(4): 13-20(in Chinese)
(李鹏翔, 任玉晴, 席酉民. 网络节点(集)重要性的一种度量指标. *系统工程*, 2004, 22(4): 13-20)
- [64] Aboelfotoh H M F, Iyengar S S, Chakrabarty K. Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. *IEEE Transactions on Reliability*, 2005, 54(1): 145-155
- [65] Qi Xiao-Gang, Zhang Cheng-Cai, Liu Li-Fang. Study on node importance and network invulnerability analysis of wireless sensor networks. *System Engineering-Theory & Practice*, 2011, 31(2): 33-37(in Chinese)
(齐小刚, 张成才, 刘立芳. WSN 节点重要性和网络抗毁性的分析方法. *系统工程理论与实践*, 2011, 31(2): 33-37)
- [66] Cai W, Jin X, Zhang Y, et al. Research on reliability model of large-scale wireless sensor networks//Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing. Wuhan, China, 2006: 1-4
- [67] Duan Mo-Yi. A novel measurement method for network invulnerability. *Journal of Chinese Computer Systems*, 2012, 33(12): 2729-2732(in Chinese)
(段谟意. 一种新的网络抗毁性的度量方法. *小型微型计算机系统*, 2012, 33(12): 2729-2732)
- [68] Li C, Ye M, Chen G, et al. An energy-efficient unequal clustering mechanism for wireless sensor networks//Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Washington, USA, 2005: 588-604
- [69] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing*, 2004, 3(4): 366-379
- [70] Younis O, Fahmy S, Santi P. Robust communications for sensor networks in hostile environments//Proceedings of the 12th IEEE International Workshop on Quality of Service. Montreal, Canada, 2004: 10-19
- [71] Cai Hai-Bin, Ju Xiao-Ming, Cao Qi-Ying. Energy prediction and reliable clustering routing protocol for multilevel energy heterogeneous wireless sensor networks. *Journal of Chinese Computers*, 2009, 32(12): 2393-2402(in Chinese)
(蔡海滨, 琚小明, 曹奇英. 多级能量异构无线传感器网络的能量预测和可靠簇路由协议. *计算机学报*, 2009, 32(12): 2393-2402)
- [72] Hashmi S U, Rahman S M M, Mouftah H T, et al. Reliability model for extending cluster lifetime using backup cluster heads in cluster-based wireless sensor networks//Proceedings of the 6th International Conference on Wireless and Mobile Computing, Networking and Communications. Niagara, USA, 2010: 479-485
- [73] Zhang Hai-Yan, Liu Hong. Balanced energy consumption routing algorithm based on K-means for WSN. *Chinese Journal of Sensors and Actuators*, 2011, 24(11): 1639-1643(in Chinese)
(张海燕, 刘虹. 基于 K-means 聚类的 WSN 能耗均衡路由算法. *传感技术学报*, 2011, 24(11): 1639-1643)
- [74] Feng Dong-Qin, Li Guang-Hui, Quan Jian-Min, et al. Reliability of wireless sensor networks based on redundancy of cluster-heads. *Journal of Zhejiang University (Engineering Science)*, 2009, 43(5): 849-854(in Chinese)
(冯冬芹, 李光辉, 全剑敏等. 基于簇头冗余的无线传感器网络可靠性研究. *浙江大学学报(工学版)*, 2009, 43(5): 849-854)
- [75] Gupta C, Sharma R, Agarwal N, et al. Fault tolerant event detection in distributed WSN via pivotal messaging. *International Journal of Computers & Technology*, 2013, 7(1): 463-472
- [76] Kumar P, Chaturvedi A. An energy efficient algorithm to avoid hot spot effects in wireless sensor networks//Proceedings of the International Conference on Signal Processing Image Processing & Pattern Recognition. Coimbatore, India, 2013: 117-121
- [77] Wu Xiao-Bing, Chen Gui-Hai. The energy hole problem of nonuniform node distribution in wireless sensor networks. *Chinese Journal of Computers*, 2008, 31(2): 253-261(in Chinese)
(吴小兵, 陈贵海. 无线传感器网络中节点非均匀分布的能量空洞问题. *计算机学报*, 2008, 31(2): 253-261)
- [78] Bagci H, Yazici A. An energy aware fuzzy approach to unequal clustering in wireless sensor networks. *Applied Soft Computing*, 2013, 13(4): 1741-1749
- [79] Su Jin-Shu, Guo Wen-Zhong, Yu Chao-Long, et al. Fault-tolerance clustering algorithm with load-balance aware in wireless sensor network. *Chinese Journal of Computers*, 2014, 37(2): 445-456(in Chinese)
(苏金树, 郭文忠, 余朝龙等. 负载均衡感知的无线传感器网络容错分簇算法. *计算机学报*, 2014, 37(2): 445-456)
- [80] Zhang Qing, Chai Qiao-Lin. Unequal scaled clustering routing for WSN based on redundancy of cluster headers. *Computer Engineering*, 2011, 37(14): 27-30(in Chinese)
(张擎, 柴乔林. 基于簇头冗余的 WSN 不等规模分簇路由. *计算机工程*, 2011, 37(14): 27-30)
- [81] Zeng Zhi-Wen, Chen Zhi-Gang, Liu An-Feng. Energy-hole avoidance for WSN based on adjust transmission power. *Chinese Journal of Computers*, 2010, 33(1): 12-22(in Chinese)
(曾志文, 陈志刚, 刘安丰. 无线传感器网络中基于可调发射功率的能量空洞避免. *计算机学报*, 2010, 33(1): 12-22)
- [82] Stavrou E, Pitsillides A. A survey on secure multipath routing protocols in WSNs. *Computer Networks*, 2010, 54(13): 2215-2238
- [83] Felemban E, Lee C G, Ekici E. MMSPEED: Multipath Multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 2006, 5(6): 738-754

- [84] Huang X, Fang Y. Multi-constrained QoS multipath routing in wireless sensor networks. *Wireless Networks*, 2008, 14(4): 465-478
- [85] Ren F, He T, Das S K, et al. Traffic-aware dynamic routing to alleviate congestion in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(9): 1585-1599
- [86] Le J, Lui J C S, Chiu D M. DCAR: Distributed coding-aware routing in wireless networks. *IEEE Transactions on Mobile Computing*, 2010, 9(4): 596-608
- [87] Wang J, Zhu C, Guo Q, et al. SCAR: A dynamic coding-aware routing protocol//*Proceedings of the 6th International Conference on Signal Processing and Communication Systems*. Golden Coast, USA, 2012: 1-5
- [88] Yang Y, Zhong C, Sun Y, et al. Network coding based reliable disjoint and braided multipath routing for sensor networks. *Journal of Network and Computer Applications*, 2010, 33(4): 422-432
- [89] Lai Y, Chen H. Energy-efficient fault-tolerant mechanism for clustered wireless sensor networks//*Proceedings of the 16th International Conference on Computer Communications and Networks*. Honolulu, USA, 2007: 272-277
- [90] Fang Xiao-Lin, Shi Sheng-Fei, Li Jian-Zhong. A disjoint multi-path routing algorithm in wireless sensor network. *Journal of Computer Research and Development*, 2009, 46(12): 2053-2061(in Chinese)
(方效林, 石胜飞, 李建中. 无线传感器网络一种不相交路径路由算法. *计算机研究与发展*, 2009, 46(12): 2053-2061)
- [91] Yu Lei-Lei, Chen Dong-Yan, Liu Yue-Mei, et al. Centralized-calculating-based 2-disjoint multipath routing algorithm for wireless sensor networks. *Journal of Computer Research and Development*, 2013, 50(3): 517-523(in Chinese)
(于磊磊, 陈冬岩, 刘月美等. 中心计算的无线传感器网络 2-不相交路径路由算法. *计算机研究与发展*, 2013, 50(3): 517-523)
- [92] Wang Xiao-Ming, Lu Jun-Ling, Li Ying-Shu, et al. Multi-constrained multipath routing for wireless sensor networks in the fuzzy random environment. *Chinese Journal of Computers*, 2011, 34(5): 779-791(in Chinese)
(王小明, 卢俊岭, 李英妹等. 模糊随机环境下的无线传感器网络多约束多路径路由. *计算机学报*, 2011, 34(5): 779-791)
- [93] Lin G H, Xue G. Steiner tree problem with minimum number of Steiner points and bounded edge-length. *Information Processing Letters*, 1999, 69(2): 53-57
- [94] Chen D, Du D Z, Hu X D, et al. Approximations for Steiner trees with minimum number of Steiner points. *Journal of Global Optimization*, 2000, 18(1): 17-33
- [95] Cheng X, Du D Z, Wang L, et al. Relay sensor placement in wireless sensor networks. *Wireless Networks*, 2008, 14(3): 347-355
- [96] Lloyd E L, Xue G. Relay node placement in wireless sensor networks. *IEEE Transactions on Computers*, 2007, 56(1): 134-138
- [97] Han X, Cao X, Lloyd E L, et al. Fault-tolerant relay node placement in heterogeneous wireless sensor networks. *IEEE Transactions on Mobile Computing*, 2010, 9(5): 643-656
- [98] Yang D, Misra S, Fang X, et al. Two-tiered constrained relay node placement in wireless sensor networks: Efficient approximations. *IEEE Transactions on Mobile Computing*, 2012, 11(8): 1399-1411
- [99] Misra S, Hong S D, Xue G, et al. Constrained relay node placement in wireless sensor networks: Formulation and approximations. *IEEE/ACM Transactions on Networking*, 2010, 18(2): 434-447
- [100] Wang Zhu, Wang Qi. Research on multi-restricted fault-tolerant relay node placement algorithm in wireless sensor networks. *Acta Electronica Sinica*, 2011, 39(3): 116-120(in Chinese)
(王翥, 王祁. 多约束容错性 WSN 中继节点布局算法的研究. *电子学报*, 2011, 39(3): 116-120)
- [101] Wang Zhu, Wang Qi, Wei De-Bao, Wang Ling. Relay node placement and addition algorithms in wireless sensor networks. *Acta Physica Sinica*, 2012, 61(12): 95-104(in Chinese)
(王翥, 王祁, 魏德宝, 王玲. 无线传感器网络中继节点布局算法的研究. *物理学报*, 2012, 61(12): 95-104)
- [102] Helmy A. Small worlds in wireless networks. *IEEE Communications Letters*, 2003, 7(10): 490-492
- [103] Chitradurga R, Helmy A. Analysis of wired short cuts in wireless sensor networks//*Proceedings of the IEEE/ACS International Conference on Pervasive Services*. Los Angeles, USA, 2004: 167-177
- [104] Sharma G, Mazumdar R. Hybrid sensor networks: A small world//*Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. Illinois, USA, 2005: 366-377
- [105] Hawick K A, James H A. Small-world effects in wireless agent sensor networks. *International Journal of Wireless and Mobile Computing*, 2010, 4(3): 155-164
- [106] Guidoni D L, Mini R A F, Loureiro A A F. On the design of resilient heterogeneous wireless sensor networks based on small world concepts. *Computer Networks*, 2010, 54(8): 1266-1281
- [107] Guidoni D L, Boukerche A, Villas L A, et al. A tree-based approach to design heterogeneous sensor networks based on small world concepts//*Proceedings of the 36th Conference on Local Computer Networks*. Bonn, Germany, 2011: 666-672
- [108] Shah R C, Roy S, Jain S, et al. Data mules: Modeling and analysis of a three-tier architecture for sparse sensor networks. *Ad Hoc Networks*, 2003, 1(2): 215-233
- [109] Zhou Si-Wang, Lin Ya-Ping, Nie Ya-Lin, et al. A study of trajectory-based mobile agent dynamic routes algorithm for data fusion in wireless sensor networks. *Chinese Journal of Computers*, 2007, 30(6): 894-904(in Chinese)
(周四望, 林亚平, 聂雅琳等. 无线传感器网络中基于数据融合的移动代理曲线动态路由算法研究. *计算机学报*, 2007, 30(6): 894-904)

- [110] Ishizuka M, Masaki A. The reliability performance of wireless sensor networks configured by power-law and other forms of stochastic node placement. *IEICE Transactions on Communications*, 2004, 87(9): 2511-2520
- [111] Sarshar N, Roychowdhury V. Scale-free and stable structures in complex ad hoc networks. *Physical Review E*, 2004, 69(2): 026101
- [112] Kong J S, Roychowdhury V P. Preferential survival in models of complex ad hoc networks. *Physica A: Statistical Mechanics and Its Applications*, 2008, 387(13): 3335-3347
- [113] Zhu H, Luo H, Peng H, et al. Complex networks-based energy-efficient evolution model for wireless sensor networks. *Chaos, Solitons & Fractals*, 2009, 41(4): 1828-1835
- [114] Li S, Li L, Yang Y. A local-world heterogeneous model of wireless sensor networks with node and link diversity. *Physica A: Statistical Mechanics and Its Applications*, 2011, 390(6): 1182-1191
- [115] Qi X Q, Ma S, Zheng G Z. Topology evolution of wireless sensor networks based on adaptive free-scale networks. *Journal of Information and Computational Science*, 2011, 8(3): 467-475
- [116] Chen Li-Jun, Liu Ming, Chen Dao-Xu, et al. Topology evolution of wireless sensor networks among cluster heads by random walkers. *Chinese Journal of Computers*, 2009, 32(1): 69-76(in Chinese)
(陈力军, 刘明, 陈道蓄等. 基于随机行走的无线传感器网络簇间拓扑演化. *计算机学报*, 2009, 32(1): 69-76)
- [117] Saramäki J, Kaski K. Scale-free networks generated by random walkers. *Physica A: Statistical Mechanics and its Applications*, 2004, 341: 80-86
- [118] Kirousis L M, Kranakis E, Krizanc D, et al. Power consumption in packet radio networks. *Theoretical Computer Science*, 2000, 243(1): 289-305
- [119] Jia X, Kim D, Makki S, et al. Power assignment for k -connectivity in wireless ad hoc networks. *Journal of Combinatorial Optimization*, 2005, 9(2): 213-222
- [120] Li X Y, Wan P J, Wang Y, et al. Fault tolerant deployment and topology control in wireless ad hoc networks. *Wireless Communications and Mobile Computing*, 2004, 4(1): 109-125
- [121] Xing G, Lu C, Jia X, et al. Localized and configurable topology control in lossy wireless sensor networks. *Ad Hoc Networks*, 2011, 11(4): 1345-1358
- [122] Li N, Hou J C. FLSS: A fault-tolerant topology control algorithm for wireless networks//*Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*. Illinois, USA, 2004: 275-286
- [123] Shi Rui, Liu Hong-Wei, Dong Jian, Yang Xiao-Zong. Fault-tolerant topology control in Ad Hoc networks. *Acta Electronica Sinica*, 2005, 33(11): 60-64(in Chinese)
(时锐, 刘宏伟, 董剑, 杨孝宗. 自组网容错拓扑控制的研究. *电子学报*, 2005, 33(11): 60-64)
- [124] Xu Qiang, Chen Jian. Application study of transmit power control technology in reliably connected wireless sensor network. *Acta Electronica Sinica*, 2008, 36(7): 1451-1455 (in Chinese)
(徐强, 陈健. 功率控制技术在可靠连通无线传感器网络中的应用研究. *电子学报*, 2008, 36(7): 1451-1455)
- [125] Ruiz L B, Nogueira J M, et al. MANNA: A management architecture for wireless sensor networks. *IEEE Transactions on Communication Magazine*, 2003, 41(2): 116-125
- [126] Ramanathan N, Kohler E, Estrin D. Towards a debugging system for sensor networks. *International Journal of Network Management*, 2005, 15(4): 223-234
- [127] Lee W L, Datta A, et al. WinMS: Wireless sensor network management system, an adaptive policy-based management for wireless sensor networks. The University of Western Australia, Australia Perth; CSSE Technical Report UWA-CSSE-06-001, 2006
- [128] Cao Xiao-Mei, Han Zhi-Jie, Chen Gui-Hai. Dos attack detection scheme for sensor networks based on traffic prediction. *Chinese Journal of Computers*, 2007, 30(10): 1798-1805(in Chinese)
(曹晓梅, 韩志杰, 陈贵海. 基于流量预测的传感器网络拒绝服务攻击检测方案. *计算机学报*, 2007, 30(10): 1798-1805)
- [129] Tai A T, Tso K S, Sanders W H. Cluster-based failure detection service for large-scale ad hoc wireless network applications//*Proceedings of the 2004 IEEE International Conference on Dependable Systems and Networks*. Los Angeles, USA, 2004: 805-814
- [130] Sheth A, Hartung C, Han R. A decentralized fault diagnosis system for wireless sensor networks//*Proceedings of the 2005 IEEE International Conference on Mobile Ad hoc and Sensor Systems*. Washington, USA, 2005: 191-194
- [131] Ding M, Chen D, Xing K, et al. Localized fault-tolerant event boundary detection in sensor networks//*Proceedings of the 24th International Conference of IEEE Computer and Communications Societies*. Miami, USA, 2005: 902-913
- [132] Chen J, Kher S, Somani A. Distributed fault detection of wireless sensor networks//*Proceedings of the 2006 ACM Workshop on Dependability Issues in Wireless Ad hoc Networks and Sensor Networks*. Los Angeles, USA, 2006: 65-72
- [133] Choi J Y, Yim S J, Huh Y J, et al. A distributed adaptive scheme for detecting faults in wireless sensor networks. *WSEAS Transactions on Communications*, 2009, 8(2): 269-278
- [134] Guo S, Zhong Z, He T. FIND: Faulty node detection for wireless sensor networks//*Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*. Berkeley, USA, 2009: 253-266
- [135] Huang Ting-Pei, Chen Hai-Ming, Zhang Zhao-Liang, et al. EasiPLED: An approach to discriminate the causes of packet losses and errors for wireless sensor networks based on supervised learning theory. *Chinese Journal of Computers*, 2013, 36(3): 471-484(in Chinese)

- (黄庭培, 陈海明, 张招亮等. EasiPLED: 一种基于监督学习理论的无线传感网络分组丢失和错误原因识别方法. 计算机学报, 2013, 36(3): 471-484)
- [136] Chen X, Kim Y A, Wang B, et al. Fault-tolerant monitor placement for out-of-band wireless sensor network monitoring. *Ad Hoc Networks*, 2012, 10(1): 62-74
- [137] Bari A, Jaekel A, Jiang J, et al. Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements. *Computer Communications*, 2012, 35(3): 320-333
- [138] Ma C, Liu H W, Zhou H Y, et al. A fault-tolerant algorithm of wireless sensor network based on recoverable nodes. *Intelligent Automation & Soft Computing*, 2011, 17(6): 737-747
- [139] Abbasi A A, Younis M, Akkaya K. Movement-assisted connectivity restoration in wireless sensor and actor networks. *IEEE Transactions on Parallel and Distributed Systems*, 2009, 20(9): 1366-1379
- [140] Wang S G, Mao X F, Tang S J, et al. Movement-assisted connectivity restoration in wireless sensor and actor networks. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(4): 687-694
- [141] Imran M, Younis M, Md Said A, et al. Localized motion-based connectivity restoration algorithms for wireless sensor and actor networks. *Journal of Network and Computer Applications*, 2012, 35(2): 844-856
- [142] Tao Dan, Ma Hua-Dong. Coverage control algorithms for directional sensor networks. *Journal of Software*, 2011, 22(10): 2317-2334(in Chinese)
(陶丹, 马华东. 有向传感器网络覆盖控制算法. 软件学报, 2011, 22(10): 2317-2334)
- [143] Wu C, Chen H, Liu J. A survey of connectivity restoration in wireless sensor networks//*Proceedings of the 3rd International Conference on Consumer Electronics, Communications and Networks*. Xianning, China, 2013: 65-67
- [144] Chuprun S, Bergstrom C S. Wireless multiple access networks for survivable battlefield communications//*Proceedings of the IEEE Military Communications Conference*. Boston, USA, 1998, 3: 898-902



LI Wen-Feng, born in 1966, Ph. D., professor, Ph. D. supervisor. His main research interests include the technologies of Internet of Things and robots, and wireless sensor networks.

FU Xiu-Wen, born in 1987, Ph. D. candidate. His main research interests include the invulnerability of wireless sensor networks and the theory of complex networks.

Background

Wireless sensor networks (WSNs) as a newly emerging technology, has received significant research attention. However, most of the research related to WSNs remains at its research stage, one of the causes responsible for this is the invulnerability of the WSNs fails to meet the strict demand of the practical application. The unique characterizes of WSNs (e. g. energy-sensitivity and data-convergence) make the network more vulnerable to the situations such as energy depletion, hardware malfunction and invasion. Although there have already been many studies focused on the invulnerability of WSN, no one has yet integrated the findings of these studies. So our work summarizes and classifies the former related work of invulnerability of WSNs. This work is supported by National Science & Technology R&D Program (2012BAJ0507), the National Natural Science Foundation of China (61305110), International Cooperation

Project Funded by Hubei Province (2011BFA012) and Fundamental Research Funds for the Central University (135118003). The aims of these projects are to acquire the environmental data in a highly effective way and exert continuing control on the mobile objects in the environment, which have high requirement for the WSN equipped with the ability for offering sustainable service. Especially, in many scenarios, the deployment environments of WSNs are complex and unpredictable. Some small but vital factors might lead to the failure of the entire network. Therefore, the performance of WSNs on invulnerability is one of the key factors influencing the research progress of these projects. We expect to summary the state of art in WSNs invulnerability to help relevant researchers better understand the invulnerability of WSNs, which in turn help them select the reasonable theories or methods to resolve the problems met during their researches.