

基于不等簇半径和动态簇头的 WSN 能量空洞攻击抑制模型研究

周伟伟, 郁滨

(信息工程大学三院, 河南 郑州 450002)

摘 要: 针对无线传感器网络通信中易遭受能量空洞攻击导致部分节点失效问题, 提出一种动态簇头最优路径的攻击抑制模型。该模型利用不等簇半径和数据流量监测对网络建模, 保证各簇头能量消耗均衡。通过节点的环形截面投影求解数据发送的欧几里得距离, 从而配置动态簇头的初始能量。在此基础上, 当单个圆环和多个圆环区域遭受攻击时, 给出了基于簇头最小生命周期和流量阈值的能量空洞攻击检测抑制算法。实验结果表明, 该算法在 WSN 能量空洞攻击抑制方面有明显优势。

关键词: 无线传感器网络; 能量空洞攻击; 簇半径; 能量耗尽; 簇头生命周期

中图分类号: TP309.1

文献标识码: A

Suppression model of energy sink-hole attack in WSN based on the unequal cluster radius and mobile cluster head

ZHOU Wei-wei, YU Bin

(The Third College, Information Engineering University, Zhengzhou 450002, China)

Abstract: To overcome the problem that partial cluster heads were drastically exhausted by the energy sink-hole attack in wireless sensor network, a novel suppression model based on the optimal path of mobile cluster heads was proposed, which was shown to balance the energy consumption in each cluster head. With the adoption of unequal cluster radius and data traffic monitoring explicitly, the inhibition mechanism was modeled as multivariate linear equations. Furthermore, toroidal projection was adopted to calculate the Euclidean distance, based on which the initial energy of mobile cluster head was configured correspondingly. On this basis, an algorithm based on the minimum cluster lifetime and throughput threshold was provided to achieve the detection and suppression of energy sink-hole attack. The experimental results show that the developed algorithm can suppress energy sink-hole attack evidently and efficiently and is suitable to the resource constrained WSN.

Key words: wireless sensor network, energy sink-hole attack, cluster radius, power depletion, cluster lifetime

1 引言

无线传感网 (WSN, wireless sensor network) 具有节点容量大、分布范围广、部署速度快的特点, 使其在智能交通、战场环境监测、态势感知等领域有着广泛的应用前景^[1]。但是, 无线信道的开放性使其面临着能量空洞攻击、中间人攻击、同频攻击等诸多安全威胁^[2-4]。能量空洞攻击指非法节点向网络中发送大量数据耗尽关键簇头能量, 导致网络

拓扑发生改变或部分功能缺失的一种攻击形式。目前, 针对能量空洞攻击的抑制技术主要分为静态抑制和动态抑制。其中, 静态抑制是指通过调整网络协议规则及各项参数来抵御能量空洞攻击; 动态能量空洞攻击抑制则利用动态节点在网络中收集数据实现能量空洞攻击抑制。

能量空洞攻击的静态抑制技术主要有 3 种。第 1 种是对网络中数据处理方式和拓扑结构进行调整, 针对多对一网络传输中的层次结构特点, Li 等^[5]建立

收稿日期: 2017-02-06; 修回日期: 2017-08-10

基金项目: 信息保障重点实验室开放基金资助项目 (No.KJ-15-104); 河南省科技攻关基金资助项目 (No.132102210003)

Foundation Items: The National Science Key Lab Fund (No.KJ-15-104), The Project of Henan Provincial Key Scientific and Technological Research (No.132102210003)

了攻击模型，提出了分层路径优化和数据压缩方案，该方案将网络划分为不同的圆环区域并依据流量分析重新生成路径，最大限度地保证网络数据均衡，使簇头的生命周期达到最优，但路由路径的规划和更新是建立在数据流量已知的基础上，该方案并不适用于存在未知非法节点的网络环境。第 2 种是分析圆环区域环径与簇头生命周期之间的关系，利用关系模型以及协调器的传输半径确定各环径取值，该方案在非法节点引入数据流量较小的情况下有效，但当数据流量较大时对能量空洞攻击的抑制效果不明显^[6]。第 3 种是利用节点单跳和多跳路由策略将簇头生命周期最优转化为线性规划问题^[7~9]，但该方法仅考虑各节点同时耗尽能量，并未对能量的数据转发效率进行分析。基于此，Heinzelman 等^[10]探讨了增加数据长链对簇头生命周期的影响，提出了基于小世界理论的不等簇轮换方案，但并未解决网络自身存在的能量不均衡问题。

能量空洞攻击的动态抑制主要包括基于动态搜索的协调器和动态簇头的抑制技术^[11,12]。动态数据收集可以依据网络中非法节点的数量和数据流量实时更新数据转发策略，对非法节点发起的能量空洞攻击有较好的抑制作用^[13]。文献[14]提出了针对不同区域节点数据量、能量消耗以及延迟的搜索算法，通过动态调整协调器在网络中的位置，避免控制中心周围区域形成能量空洞，但并未对网络中能量分布不均衡问题进行研究，而且在整个区域内频繁移动协调器也是不现实的。在动态搜索协调器策略的基础上，引入动态簇头可以及时收集非法节点在各圆环区域发送的干扰数据^[15]，但并未给出动态簇头在网络中采集数据的移动路径。文献[16]提出了一种能量均衡的路由算法，依据节点的能耗情况自适应切换路由路径和簇头位置，但该方案在实际应用中不易实现。

综上所述，无论是能量空洞攻击静态抑制还是动态抑制均是在星形和树形网络拓扑结构中解决了节点布局或非法节点入侵引起的能量消耗不均衡问题，并未考虑簇形网络中各环径的取值以及依据非法节点攻击程度的能量空洞攻击抑制策略，影响了簇头生命周期的提高。

本文结合能量分析模型和 WSN 拓扑结构的自身特点，提出了一种基于不等簇半径和动态簇头思想的能量空洞攻击抑制方案，求解了网络布局中各环径的取值和动态簇头的移动路径。最后，实验对

比了本文方案与其他能量空洞攻击抑制方案的抗能量空洞攻击性能。

2 能量空洞攻击抑制模型

无线传感网由协调器、簇头和终端节点构成。假设协调器的能量是无限的，且各节点具备相同的初始能量。终端仅负责数据采集和发送任务，与簇头相比，终端的生命周期相对较长。因此，能量分析模型主要研究簇头数据收发过程中的能耗。

模型中的符号及其含义如表 1 所示。

表 1 所用符号含义

符号	含义
Cor	协调器
c_i	第 i 个圆环区域
R	网络区域半径
R_1, R_2, \dots, R_n	圆环宽度
R_0	以 Cor 为中心的圆半径
$\frac{R_i}{2}$	第 i 个圆环内的簇半径
N	整个网络中的簇头数量
N_1, N_2, \dots, N_n	各圆环中的簇头数量
λ	单位面积采集到的数据量
δ	第 i 个圆环内动态簇头采集数据的半径
E_{elec}	发送一个字节消耗的能量
T	簇头生命周期
ε	信号放大系数
T_{min}	最小簇头生命周期
d_{size}^{attack}	非法节点引入的数据量
d_{size}^{move}	动态簇头采集的数据量
Q	遭受攻击的圆环个数
a	电波路径损失指数
mc	动态簇头
$c_{i,1}, c_{i,2}$	动态簇头轨迹分别与 c_i 内环、外环构成的区域
d_{total}^i	第 i 个圆环内单个簇头接收到的数据量
$N_{i,1}, N_{i,2}$	$c_{i,1}, c_{i,2}$ 内的簇头数量

簇头布局不合理和非法节点能量空洞攻击破坏了原有数据流量均匀分布规律，使部分簇头过早失效，导致协调器无法采集相应区域的数据。通过分析不同区域数据传递流程，同时利用能量分析模型和数据收发特性实现对区域环径的求解。基于此，结合无线传感网数据处理特点设计能量空洞攻击抑制算法。

2.1 模型构建

WSN 汇聚式网络通常利用飞机等工具在采集数据区域上空均匀地播撒簇头和终端节点，形成近似圆形的区域，中心位置部署一个与控制台链接的协调器节点，与其他能量空洞攻击模型^[6-8]相似，本文假设所有节点分布在一个半径为 R 的圆形区域。

由于 WSN 路由采用最短路径原则，外部簇头向协调器中继数据时采用层层传递的形式，圆形区域被自然划分为多个环形区域。假设圆环 C_i 中的簇头将收集到的终端节点数据传递给 C_{i-1} 中的簇头，数据传递需要多跳才能完成。环 C_{i-1} 内的簇头不仅需要传递自身收集到的终端节点数据，还要传递 C_i 到 C_{i-1} 的数据。同一个终端节点连接有多个传感器，终端对各传感器采集到的数据进行数据融合后发送到簇头。终端、簇头以及协调器之间的数据传递不存在数据融合操作。网络结构如图 1 所示。

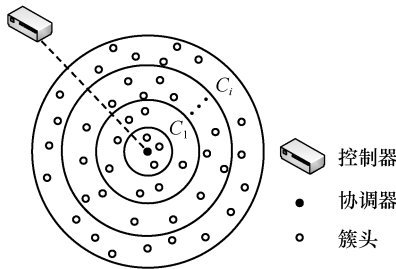


图 1 网络模型

如图 2 所示，以协调器为圆心，以各圆环内簇直径为环的宽度划分环形区域，数据由外向内依次中继到协调器。 r_i 为第 i 个圆环内簇头与第 $i-1$ 个圆环内簇头之间的距离， R_i 为第 i 个圆环的宽度，圆环宽度与网络区域半径满足 $R = R_0 + R_1 + \dots + R_n$ 。

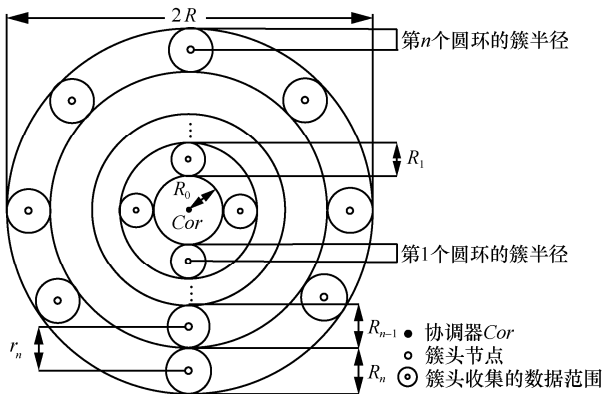


图 2 簇头部署示意

实际应用中簇头和终端节点以一定比例混合均匀后通过飞机等设备向预定地面区域抛洒，簇头和终端节点在圆环中近似均匀分布，且有 $R_0 = R_1$ 。由于部署中各圆环中簇头覆盖区域有重叠和缺漏情况，引入重叠和缺漏程度的关系因子 k_0 ，为分析计算方便，取 $k_0 \approx 1$ ，第 n 个圆环内的簇头个数可表示为

$$N_n = k_0 \frac{\pi(R_0 + R_1 + \dots + R_n)^2 - \pi(R_0 + R_1 + \dots + R_{n-1})^2}{\frac{\pi R_n^2}{4}} \approx \frac{\pi(R_0 + R_1 + \dots + R_n)^2 - \pi(R_0 + R_1 + \dots + R_{n-1})^2}{\frac{\pi R_n^2}{4}} \quad (1)$$

当整个网络中的簇头节点个数为 N 时，满足关系 $N = N_1 + N_2 + \dots + N_n$ 。

第 $i+1$ 个圆环内簇头采集到的数据要通过第 i 个圆环的簇头中继，因此，第 i 个圆环的簇头处理的数据包括本区域内采集到的数据和所有外部圆环簇头传递过来的数据。

由此，第 i 个圆环外部传递过来的数据量为

$$\sum_{j=i+1}^n \lambda \left\{ \pi(R_0 + R_1 + \dots + R_j)^2 - \pi(R_0 + R_1 + \dots + R_{j-1})^2 \right\} \quad (2)$$

第 i 个圆环单个簇头接收到的外部数据量为

$$d_o^i = \frac{\sum_{j=i+1}^n \lambda \left\{ \pi(R_0 + R_1 + \dots + R_j)^2 - \pi(R_0 + R_1 + \dots + R_{j-1})^2 \right\}}{N_i} \quad (3)$$

当网络区域终端节点均匀分布时，第 i 个圆环内部单个簇头接收到当前圆环内产生的数据量为

$$d_i^i = \frac{\pi \lambda R_i^2}{4}$$

将其代入式(3)，则第 i 个圆环内单个簇头接收到的数据量为

$$d_{total}^i = d_o^i + d_i^i = \frac{\pi R_i^2 \sum_{j=i+1}^n \lambda \left\{ (R_0 + R_1 + \dots + R_j)^2 - (R_0 + R_1 + \dots + R_{j-1})^2 \right\}}{4 \left[(R_0 + R_1 + \dots + R_i)^2 - (R_0 + R_1 + \dots + R_{i-1})^2 \right]} + \frac{\lambda \pi R_i^2}{4} \quad (4)$$

第 i 个圆环与第 $i-1$ 个圆环数据发送的距离为

$$r_i = \frac{(R_i + R_{i-1})}{2}, i \in \{1, 2, \dots, n\}。$$

节点的能量消耗主要是在数据发送、接收和簇头移动过程中产生的。采用典型的能量分析模型^[12]，在距离为 d 的 2 个节点之间发送和接收长度为 k bit 的数据时的能量消耗分别如式(5)和式(6)所示。

$$E_{tr}(d) = k(\varepsilon d^a + E_{elec}) \quad (5)$$

$$E_{rec} = kE_{elec} \quad (6)$$

当节点间数据的传输距离小于阈值 φ 时， $a=2$ ；当数据传输距离大于阈值 φ 时， $a=4$ 。

动态簇头在协调器和终端节点之间进行数据转发过程中，移动距离 d_{move} 所产生的能量消耗为 $E_{move}(d_{move}) = e_{move} d_{move}$ 。动态簇头完成一次数据转发所产生的总的能量消耗为

$$\begin{aligned} E_{total}^{move} &= E_{tr}(d) + E_{rec} + E_{move}(d_{move}) \\ &= k(\varepsilon d^a + 2E_{elec}) + e_{move} d_{move} \end{aligned} \quad (7)$$

由式(5)和式(6)可得第 i 个圆环簇头发送和接收数据的总能量消耗为

$$\begin{aligned} E_{total}^{static}(r_i) &= d_{total}^i [E_{tr}(r_i) + E_{rec}] \\ &= m d_{total}^i (\varepsilon r_i^a + 2E_{elec}) \end{aligned} \quad (8)$$

当圆形区域某个或某几个圆环内存在非法节点向网络中发送数据时，会破坏网络能量消耗均衡和原有的拓扑结构，导致部分节点过快失效从而影响网络正常运行。引入动态簇头收集非法节点增加的数据量，使网络重新达到平衡。

整个网络达到平衡时，各静态簇头的能量消耗相等，这样可以保证整个网络节点不会出现能量空洞现象，即 $E_{total}^{static}(r_1) = E_{total}^{static}(r_2) = \dots = E_{total}^{static}(r_n)$ 。

保证网络避免能量空洞攻击的问题转化为采取策略使所有簇头的实际生命周期达到最大。网络满足的攻击抑制模型方程组为

$$\begin{cases} d_{size}^{move} = d_{size}^{attack} = \sum_{i=1}^n d_{size_i}^{attack}, \min(N) \\ N = N_1 + N_2 + \dots + N_n \\ R = R_0 + R_1 + \dots + R_n \\ E_{total}^{static}(r_1) = E_{total}^{static}(r_2) = \dots = E_{total}^{static}(r_n) \\ T \geq 1.1T_{min} \\ T = \frac{E}{E_{total}^{static}(r_1)} \end{cases} \quad (9)$$

2.2 能量空洞攻击抑制算法

依据式(9)所示的约束条件将簇头部署到相应位置。第 $i-1$ 个圆环区域的簇头实时监测第 i 个圆

环区域传送过来的数据流量。协调器利用第 $i-1$ 个圆环区域中各簇头采集到的数据流量总和求均值作为第 i 个圆环区域传送过来的数据流量 v_i^1 。第 i 个圆环区域中的簇头传送的数据流量理论值为 v_i^0 。由于簇头生命周期 $T \geq 1.1T_{min}$ 且实际部署中容易出现局部数据传输不均衡现象，设置阈值为 $0.1v_i^0$ 。以周期 T_0 对各圆环区域数据流量进行监测，当 $\frac{v_i^1 - v_i^0}{v_i^0} \leq 0.1$ 时，圆环区域内的簇头生命周期仍满足 T_{min} ，该圆形区域未遭受能量空洞攻击；当 $\frac{v_i^1 - v_i^0}{v_i^0} > 0.1$ 时，该圆环区域遭受能量空洞攻击，执行相应的防御策略。具体的检测及抑制算法如下所示。

算法 1 系统输入网络覆盖半径为 R ，网络最小生命周期 T_{min} 且满足 $T \geq T_{min}$ ，未受到能量空洞攻击时各簇头满足关系 $E_{total}^{static}(r_1) = E_{total}^{static}(r_2) = \dots = E_{total}^{static}(r_n)$ 。输出结果满足 $d_{size}^{move} = d_{size}^{attack}$ ， $\max(T) = \min_{0 < i \leq n}(E_i)$ ， $\min(N)$ 。

Step1 设置网络初始 R_0 以及簇头采集数据的速率，由式(9)计算环径 R_1, R_2, \dots, R_n 、 T 和 N 。

Step2 当 $R_0, R_1, R_2, \dots, R_n$ 、 T 、 N 以及簇头采集数据的速率确定时，向各环形区域部署簇头。部署完成后，在周期 T_0 结束时，若 $\frac{v_i^1 - v_i^0}{v_i^0} \leq 0.1$ ，系

统判定该圆环区域内未遭受攻击；若 $\frac{v_i^1 - v_i^0}{v_i^0} > 0.1$ ，该圆环区域 i 内遭受攻击，对所有圆环区域进行遍历，确定遭受攻击的圆环区域个数 Q 并计算动态簇头在圆环 i 中移动轨迹长度 L_i 。

Step 3 当 $Q=0$ 时，跳转到 Step 4；当 $Q=1$ 时，在下一个周期 T_0 内执行单圆环区域动态簇头路径优化策略，配置动态簇头的初始能量为 $E_{avg}^{total}(x)$ ，以数据收集速率 $d_c^i = d_{size}^{attack} \frac{v}{L_i}$ 将上一个周期攻击引入的数据量 d_{size}^{attack} 直接传送到协调器；当 $Q>1$ 时，执行多圆环区域动态簇头路径优化策略，配置动态簇头的初始能量为 $\frac{E_{avg}^{total}(x)}{m}$ ，以数据收集速率 $d_c^i = d_{size_i}^{attack} \frac{v}{mL_i}$ 将上一个周期攻击在圆环 i 引入的数

据量 $d_{size_i}^{attack}$ 直接传送到协调器。其中， $L_i = \frac{\pi \delta^2}{m}$ ， m

的取值必须满足 mc 在多圆环区域动态簇头路径优化策略中运行一次的时间不超过 T_0 。

Step 4 若周期 T_0 未超时, 执行 Step 2; 若周期 T_0 超时且未达到网络系统运行总时间, 跳转到 Step 3; 若达到系统运行总时间, 跳转到 Step 5。 T_0 的取值与检测节点的初始能量成反比, 与网络规模成正比。

Step 5 结束。

3 能量空洞攻击抑制模型的求解

WSN 中簇头的能量收发半径是有限的, 即从一个有限的数据集 $\{1, 2, \dots, l\}$ 。利用各簇头能量消耗相等及初始半径 R_0 可以将 R_1, R_2, \dots, R_n 分别表示为 R_0 的一元多项式。网络节点对能量空洞攻击进行实时监测, 当遭受攻击时, 移动簇头将相应区域内非法节点引入的数据量直接传送到协调器, 因此, 在静态簇头的实际部署中不考虑能量空洞攻击的影响。在 $\{1, 2, \dots, l\}$ 中逐个选取元素作为 R_0 , 利用不同的 R_0 可以计算相应的 T 及环径 R_1, R_2, \dots, R_n , 利用式(9)筛选符合要求的 R_0 、 T 以及 N 。

基于以上分析, 下面具体对选定的 R_0 求解相应的 R_1, R_2, \dots, R_n 、 T 和 N 。

$$\begin{cases} a = \lambda m \pi \varepsilon (R^2 - \eta^2), b = 2 \lambda m \pi \varepsilon R_{i-1} \\ c = [2 \lambda m \pi E_{\text{elec}} (R^2 - \eta^2) + \lambda m \pi \varepsilon (R^2 - \eta^2) R_{i-1}^2 - 16B] \\ d = -8B\eta, p = \frac{3ac - b^2}{3a^2}, q = \frac{27a^2d - 9abc + 2b^3}{27a^3} \\ R_i = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \frac{b}{3a}, \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \geq 0, \\ R_i = \frac{2}{3} \sqrt{-3p} \cos\left(\frac{1}{3} \arccos \frac{-3q\sqrt{-3p}}{2p^2}\right) - \frac{b}{3a}, \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0, \end{cases} \quad (13)$$

当 R_0 确定时, 可以利用式(13)求解相应的 R_1 , 依次递推出所有的环径。在此基础上, 结合 $T = \frac{E}{E_{\text{total}}^{\text{static}}(r_i)}$ 与式(1), 求解得到最优的 T 和 N 。

2) 当相邻圆环之间的距离大于阈值 φ 时, 取 $a = 4$, 则第 i 个圆环内簇头的能量消耗可表示为 $E_{\text{total}}^{\text{static}}(r_i) = md_{\text{total}}^i (\varepsilon r_i^a + 2E_{\text{elec}})$

$$= \lambda m \pi R_i^2 \left\{ \frac{R^2 - (\eta + R_i)^2}{4R_i^2 + 8\eta R_i} + \frac{1}{4} \right\} \left\{ \varepsilon \left(\frac{R_i + R_{i-1}}{2} \right)^2 + 2E_{\text{elec}} \right\} \quad (14)$$

将式(11)代入式(14)并化简得

1) 当相邻圆环之间的距离小于阈值 φ 时, 取 $a = 2$, 设定各圆环内的单位面积采集到的数据均匀分布, 令 $\eta = R_0 + R_1 + \dots + R_{i-1}$, 此时第 i 个圆环内簇头的能量消耗可表示为

$$\begin{aligned} E_{\text{total}}^{\text{static}}(r_i) &= md_{\text{total}}^i (\varepsilon r_i^a + 2E_{\text{elec}}) \\ &= \lambda m \pi R_i^2 \left\{ \frac{R^2 - (\eta + R_i)^2}{4R_i^2 + 8\eta R_i} + \frac{1}{4} \right\} \\ &\quad \left\{ \varepsilon \left(\frac{R_i + R_{i-1}}{2} \right)^2 + 2E_{\text{elec}} \right\} \quad (10) \end{aligned}$$

R_0 是已知的, 则以协调器为中心的第一个圆环区域内节点的能量消耗为

$$E_{\text{total}}^{\text{static}}(r_1) = \lambda m \pi \left[\frac{R^2 - 4R_0^2}{12R_0^2} + \frac{R_0^2}{4} \right] \left[2E_{\text{elec}} + \varepsilon \left(\frac{3}{2} R_0 \right)^2 \right] = B \quad (11)$$

各簇头的能量消耗相同, 因此, 将式(11)代入式(10)化简后得

$$\lambda m \pi \varepsilon (R^2 - \eta^2) R_i^3 + 2 \lambda m \pi \varepsilon R_{i-1} R_i^2 + [2 \lambda m \pi E_{\text{elec}} (R^2 - \eta^2) + \lambda m \pi \varepsilon (R^2 - \eta^2) R_{i-1}^2 - 16B] R_i - 8B\eta = 0 \quad (12)$$

式(12)是一个与未知变量 R_i 相关的一元三次方程, 该方程的解如式(13)所示。

$$\lambda m \pi \varepsilon (R^2 - \eta^2) R_i (R_i + R_{i-1})^4 + 32 \lambda m \pi (R^2 - \eta^2) E_{\text{elec}} R_i - 64 B R_i - 128 B \eta = 0 \quad (15)$$

式(15)是与 R_i 相关的一元五次方程, 当 R_0 选定时, 同样可以递推得到所有的环径值。利用选定的 R_0 可以得到一组 R_1, R_2, \dots, R_n 、 T 和 N 。通过对比得到最优的 T 、 N 和 $R_0, R_1, R_2, \dots, R_n$ 。

4 动态簇头路径的优化策略

当网络遭受能量空洞攻击时, 为了避免出现节点能量耗尽, 需要对动态簇头的移动路径和策略进行分析, 快速高效地收集和转发由非法节点引入的

数据量。

4.1 网络参数分析

定理 1 设 $\beta = R_0 + R_1 + \dots + R_{i-1}$ ，则动态簇头在第 i 个圆环内采集数据的轨迹半径为 $\delta = \frac{1}{2}\sqrt{4\beta^2 + 2R_i^2 + 4R_i\beta}$ 。

证明 当检测到存在攻击的圆环区域时，动态簇头移动到该区域收集数据并直接转发到 Cor 。如图 3 所示，设动态簇头距离圆环的内壁距离为 x ，则中心与动态簇头之间的距离为 $\beta + x$ 。

由式(1)可得

$$N_{i,1} = \frac{\pi(\beta + x)^2 - \pi\beta^2}{\frac{\pi R_i^2}{4}} \quad (16)$$

$$N_{i,2} = \frac{\pi(\beta + R_i)^2 - \pi(\beta + x)^2}{\frac{\pi R_i^2}{4}} \quad (17)$$

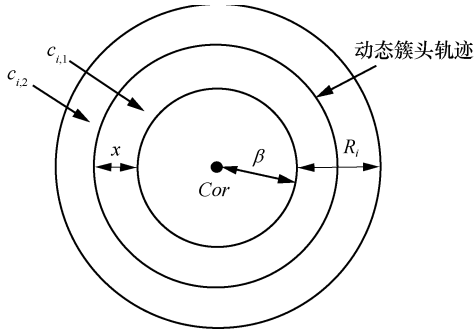


图 3 动态簇头轨迹示意

当动态簇头移动时，两侧的簇头密度相等时针对能量空洞攻击的抑制效果最好，即有 $N_{i,1} = N_{i,2}$ 。

将式(16)和式(17)代入化简得

$$x = \frac{1}{2}\sqrt{2R_i^2 + 4\beta R_i + 4\beta^2} - \beta$$

因此，动态簇头移动轨迹半径 $\delta = \beta + x =$

$$\frac{1}{2}\sqrt{4\beta^2 + 2R_i^2 + 4R_i\beta}。$$

证毕。

定理 2 若动态簇头 mc_1 沿半径为 δ 的圆弧轨迹收集数据，则 $c_{i,1}$ 内节点发送数据的欧几里得距离

为 $d_{avg,i,1} = \frac{1}{3}x$ ， $c_{i,2}$ 内节点发送数据的欧几里得距离

为 $d_{avg,i,2} = \frac{1}{3}(R_i - x)$ 。

证明 非法节点在环形区域 $c_{i,1}$ 内均匀分布并向网络发送大量恶意数据， mc_1 的坐标为 $(0, x)$ ，将

环形区域展开，则非法节点全部投影在纵坐标为 $[0, x]$ 的区间内。

如图 4 所示，设某一非法节点 A 的坐标为 $m = (0, x_1)$ ， mc_1 的坐标为 $n = (0, x)$ ，则非法节点与 mc_1

的欧几里得距离 $d_{avg,i,1} = \frac{\int_{[0,x]} \int_{[0,x]} |m-n| dmdn}{\int_{[0,x]} \int_{[0,x]} dmdn}$ ，而

$$\int_{[0,x]} \int_{[0,x]} dmdn = \int_0^x \int_0^n dmdn = \frac{1}{2}x^2 \quad (18)$$

由于 $n = (0, x)$ ，且有 $0 \leq x_1 \leq x$ ，则 $|m-n| = n-m$ ，因此，可得

$$\int_{[0,x]} \int_{[0,x]} |m-n| dmdn = \int_0^x \int_0^n (n-m) dmdn = \frac{1}{6}x^3 \quad (19)$$

把式(18)和式(19)代入欧几里得距离公式中可以得到 $c_{i,1}$ 内节点与 mc_1 的欧几里得距离为

$d_{avg,i,1} = \frac{1}{3}x$ 。同理， $c_{i,2}$ 内节点与 mc_1 的欧几里得距

离为 $d_{avg,i,2} = \frac{1}{3}(R_i - x)$ 。

证毕。

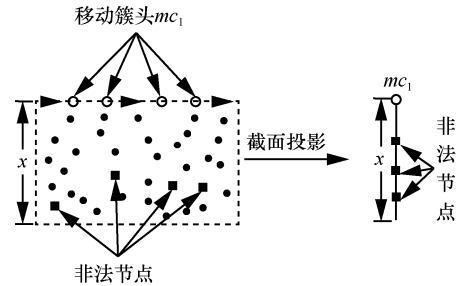


图 4 环形区域平面映射示意

4.2 策略优化

$E_{avg,i,1}(x)$ 为 $c_{i,1}$ 内非法节点引入数据量的能量消耗， $E_{avg,i,2}(x)$ 为 $c_{i,2}$ 内非法节点引入数据量的能量消耗，当网络中仅有一个圆环区域存在非法节点时，执行单圆环区域动态簇头抑制策略，即单个圆环区域遭受攻击时，由一个动态簇头进行数据转发。动态簇头的运动轨迹如图 3 所示，则 $c_{i,1}$ 内数据收发的能量消耗为

$$E_{avg,i,1}(x) = \frac{2\beta x + x^2}{2\beta R_i + R_i^2} d_{size}^{attack} \left[\varepsilon \left(\frac{x}{3} \right)^a + 2E_{elec} \right]$$

$c_{i,2}$ 内数据收发的能量消耗为

$$E_{avg,i,2}(x) = \frac{R_i^2 + 2\beta R_i - 2\beta x - x^2}{2\beta R_i + R_i^2} d_{size}^{attack} \left[\varepsilon \left(\frac{x}{3} \right)^a + 2E_{elec} \right]$$

因此，圆环区域内数据量为 d_{size}^{attack} 的收发能耗为

$$E_{avg,i}(x) = \frac{2\beta x + x^2}{2\beta R_i + R_i^2} d_{size}^{attack} \left[\varepsilon \left(\frac{x}{3} \right)^a + 2E_{elec} \right] + \frac{R_i^2 + 2\beta R_i - 2\beta x - x^2}{2\beta R_i + R_i^2} d_{size}^{attack} \left[\varepsilon \left(\frac{x}{3} \right)^a + 2E_{elec} \right] \quad (20)$$

mc_1 以半径为 $(\beta + x)$ 在 c_i 内采集数据，则簇头移动所消耗的能量为

$$E_{move,i}(x) = e_{move} 2\pi(\beta + x) \quad (21)$$

mc_1 移动到协调器的能量为

$$E_{move,i,1}(x) = e_{move} (\beta + x) \quad (22)$$

由式(20)~式(22)可得非法节点引入的能量消耗为

$$E_{avg}^{total}(x) = E_{avg,i}(x) + E_{move,i}(x) + E_{move,i,1}(x) \quad (23)$$

如图 5 所示，设圆形区域内有 n 个圆环区域，当网络中有多个圆环区域内存在非法节点时，执行多圆环区域动态簇头抑制策略，即在多个圆环区域遭受攻击时，由 m 个动态簇头进行数据转发。圆形区域均分为 m 个扇形，每个扇形的圆心角为 $\frac{2\pi}{m}$ ，扇形区域 ∇_j 的边与动态簇头的轨迹交点依次为 l_n 、 p_n 、 p_{n-1} 和 q_{n-1} 。每个扇形区域对应一个动态簇头，这 m 个扇形区域对应的动态簇头分别为 mc_1, mc_2, \dots, mc_m 。

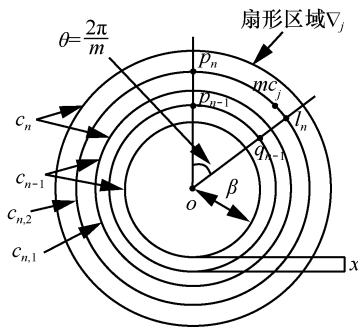


图 5 多圆环动态簇头抑制策略示意

由定理 1 可知， mc_j 在 ∇_j 中数据采集的轨迹是沿半径 $\delta = \beta + x$ 进行的，其中， β 为 mc_j 所在环形区域内壁与圆心 o 之间的距离。 mc_j 在扇形区域中首先沿圆弧 $arc(l_n, p_n)$ 移动，采集 c_n 内的数据，然后沿 $[p_n, p_{n-1}]$ 移动至 p_{n-1} ，在 $arc(p_{n-1}, q_{n-1})$ 上采集 c_{n-1} 内的数据。由此， mc_j 在 ∇_j 中的移动路径为 $arc(l_n, p_n)$ 、 $[p_n, p_{n-1}]$ 、 $arc(p_{n-1}, q_{n-1})$ 、 \dots 、 $[q_1, o]$ 。

$c_i(\nabla_j)$ 为第 i 个圆环区域被 ∇_j 分割的部分， mc_j 将 $c_i(\nabla_j)$ 分为 $c_{i,1}(\nabla_j)$ 和 $c_{i,2}(\nabla_j)$ ， $N_{i,1}(\nabla_j)$ 和 $N_{i,2}(\nabla_j)$ 分别是 $c_{i,1}(\nabla_j)$ 与 $c_{i,2}(\nabla_j)$ 的簇头数量。则有

$$N_{i,1}(\nabla_j) = \frac{1}{m} \frac{\pi(\beta + x)^2 - \pi\beta^2}{\frac{\pi R_i^2}{4}} = \frac{1}{m} \frac{\pi x^2 - 2\pi\beta x}{\frac{\pi R_i^2}{4}}$$

$$N_{i,2}(\nabla_j) = \frac{1}{m} \frac{\pi R_i^2 - \pi x^2 + 2\pi\beta R_i - 2\pi\beta x}{\frac{\pi R_i^2}{4}}$$

$E_{avg,i,\nabla_j}(\beta, R_i, x, m)$ 为 $c_i(\nabla_j)$ 中收发数据的能量消耗总量，可得

$$E_{avg,i,\nabla_j}(\beta, R_i, x, m) = \frac{d_{size}^{attack} (x^2 - 2\beta x)}{mR^2} (\varepsilon d_{avg,i,1}^a + 2E_{elec}) + \frac{d_{size}^{attack} (R_i^2 - x^2 + 2\beta R_i - 2\beta x)}{mR^2} (\varepsilon d_{avg,i,2}^a + 2E_{elec})$$

由此可知，整个 ∇_j 内收发数据的能量消耗可表示为

$$E_{avg,\nabla_j}(\beta, R_i, x, m) = \sum_{i=1}^n E_{avg,i,\nabla_j}(\beta, R_i, x, m) \quad (24)$$

mc_j 的移动轨迹由各弧线与半径 $(R - R_n + x)$ 构成， $arc(p_i, q_i)$ 的长度 $\overline{(p_i, q_i)} = \frac{2\pi(\beta + x)}{m}$ ， mc_j 移动所消耗的能量可表示为

$$E_{move,n,\nabla_j}(R_i, x, n) = e_{move} \left[\sum_{i=1}^n \overline{(p_i, q_i)} + R - R_n + x \right] = e_{move} \left[\sum_{i=1}^n \frac{2\pi(\beta + x)}{m} + R - R_n + x \right] \quad (25)$$

由式(24)和式(25)可得， ∇_j 中由于非法节点所引入的能量消耗为

$$E_{avg,\nabla_j}^{total}(R_i, x, n) = E_{move,n,\nabla_j}(R_i, x, n) + E_{avg,\nabla_j}(\beta, R_i, x, m) \quad (26)$$

由式(24)~式(26)可得，在多圆环区域动态簇头抑制策略中，非法节点引入的能量消耗为

$$E_{avg}^{total}(x) = mE_{avg,\nabla_j}^{total}(R_i, x, n) = m \left[E_{move,n,\nabla_j}(R_i, x, n) + E_{avg,\nabla_j}(\beta, R_i, x, m) \right] \quad (27)$$

5 实验与结果分析

利用 OPNET 仿真平台进行方案验证，网络配

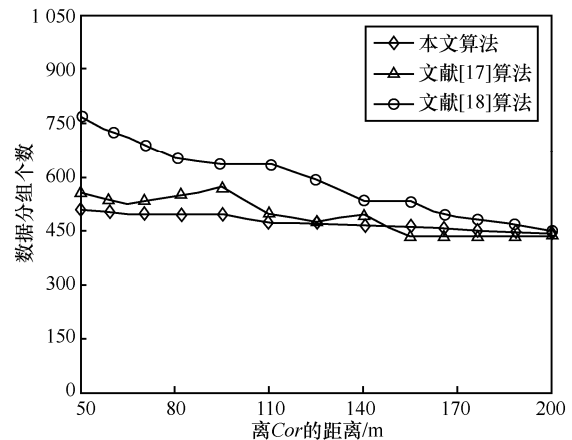
置采用 ZigBee 通信协议标准。实验中设置 4 种实验场景: 1) 基于不等簇半径和动态簇头的能量空洞攻击抑制算法; 2) 文献[5]中基于小世界的能量空洞攻击抑制算法; 3) 文献[17]中的 DEER 能量空洞攻击抑制算法; 4) 文献[18]中基于簇头轮转的能量空洞攻击抑制算法。通过测量簇头接收的瞬时数据分组个数、失效节点个数、簇头信号处理端电压采样和通信结束时簇头的剩余能量 4 个主要参数指标来对比不同能量空洞攻击抑制方案的性能。具体配置参数如表 2 所示。

参数	值
仿真区域半径/m	200
环形区域个数/个	10
簇头初始能量/J	50
终端节点初始能量/J	3
终端节点数量/个	2 000
发送单字节消耗的能量/J	50×10^{-9}
以 Cor 为中心的圆半径/m	50
数据帧长度/byte	256
簇头发射端等效电阻 R/Ω	1 000
运行总时间/h	56

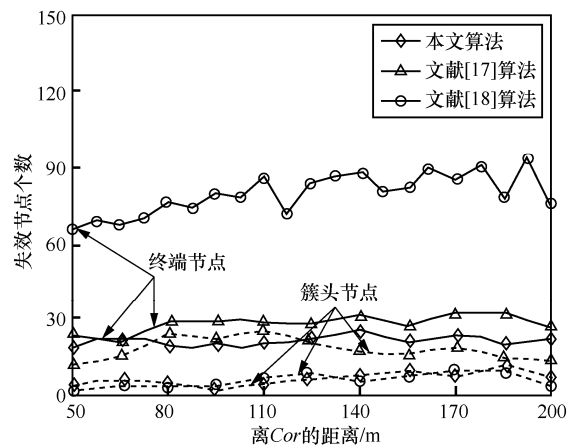
配置网络中终端节点发送数据的速率为 120 kbit/s, 当 $t=20$ h 时, 采用不同算法时簇头接收到的瞬时数据分组 (取距离 Cor 相等的 10 个簇头接收数据的均值) 和失效节点的个数随相距 Cor 的距离之间的关系如图 6 所示。

在图 6(a)中, 由于本文算法在部署各圆环区域内的簇头时采用了不等簇和动态簇头最优路径抑制能量空洞攻击, 在距离 Cor 为 50~200 m 时, 不同距离的簇头接收到的瞬时数据分组个数稳定在 450~480。结合簇头生命周期约束条件 $T \geq 1.1T_{min}$ 和接收到的瞬时数据分组变化幅度 $\frac{480-450}{450} < 0.1$ 可知, 网络可以有效抑制能量空洞攻击, 避免数据量过大导致部分簇头提前失效。文献[17]中的算法在簇头距离 Cor 小于 110 m 时接收数据分组个数明显大于本文算法。文献[17]虽然提出了满足延迟限制且能量消耗小的 DEER 算法且构建了一条簇头到 Cor 的最优路径, 但并未解决离 Cor 较近的区域数据汇聚导致单个簇头接收数据量过大的问题。文献[18]的算法采取终端节点与簇头周期轮转, 保证网络中

节点能量消耗相对均衡, 单个簇头接收到的数据量较大。如图 6(a)所示, 文献[18]算法中簇头接收瞬时数据量远大于其他算法。图 6(b)中, 本文算法下失效的簇头和终端节点个数均小于其他算法。文献[18]算法中终端节点失效的个数远大于其他算法。文献[17]采取最优路径传输导致部分簇头频繁中继数据。因此, 该算法的簇头失效个数大于本文算法。文献[18]的周期轮转算法使持有初始能量较少的终端节点承担部分路由功能, 加速了终端节点能量耗尽。相比其他算法, 本文算法在簇形汇聚网络中对抑制能量空洞攻击有明显优势。



(a) 采用不同算法时簇头接收的瞬时数据分组个数



(b) 采用不同算法时失效节点个数

图 6 $t=20$ h 时不同算法下的性能测试

当单个和多个圆环区域遭受能量空洞攻击时, 利用仿真系统对圆环内簇头信号处理端电路的电压采样测试结果如图 7 所示。

图 7(a)和图 7(b)分别为单个和多个圆环遭受攻击时采用文献[5]方案抑制后的时域电压曲线。图 7(a)中右侧出现较强的波峰, 图 7(b)中波峰抖动

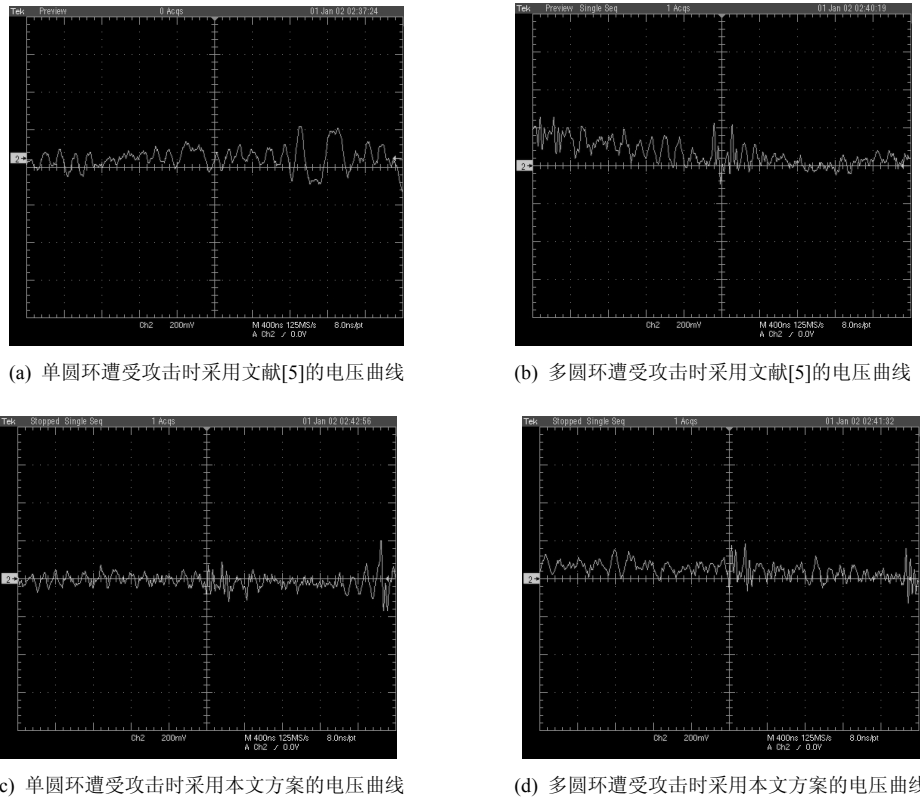


图 7 不同动态簇头路径优化策略下的能量消耗

的次数明显比图 7(a)多，这是由于多个圆环内出现攻击时数据向该簇头的汇聚量增大。图 7(c)和图 7(d)分别为采取本文抑制策略后簇头的电压曲线，簇头电压波形趋于一个较小的稳定值。设节点信号端电路的等效阻值为 R' ，则簇头生命周期 $T = \frac{E}{U^2 R'}$ 。由

图 7 的 4 种状态下簇头信号端电路的平均电压分别为 120 mV、160 mV、80 mV、100 mV。结合簇头初始能量、发射端等效电阻及 $T = \frac{E}{U^2 R'}$ 可得，4 种状

态下簇头的生命周期分别为 964.4 h、723.3 h、1 446.6 h、1 157.2 h。本文方案在能量空洞攻击下簇头的生命周期最长，对能量空洞攻击具有较好的抑制效果。

在 WSN 网络中仿真运行簇头轮转算法^[17]、DEER 算法^[18]以及本文算法，各节点发送数据帧长度为 256 byte。 $t=56$ h 时，网络通信结束，圆环区域内簇头的剩余能量如图 8 所示（簇头剩余能量为圆环区域内抽样节点的均值）。

从图 8 可以看出，在遭受能量空洞攻击时，3

种算法均可以保证外侧圆环簇头与内侧簇头的剩余能量具有较小的差值。其中，采用文献[18]算法时，第 10 个圆环中簇头与第 1 个圆环中簇头剩余能量差值为 3.52 J，采用文献[17]算法时，能量空洞攻击抑制性能下降，剩余能量差值为 4.89 J。本文算法使簇头剩余能量差值保持在 0.37 J，优于文献[17]和文献[18]算法。

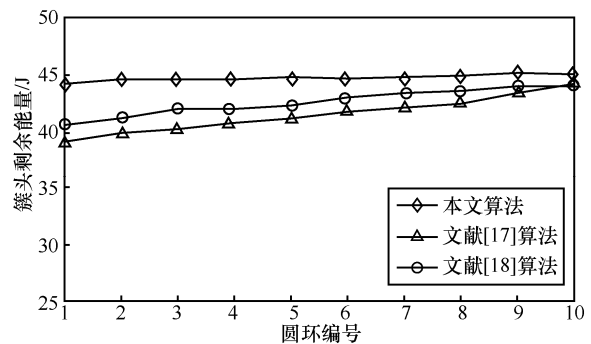


图 8 通信结束时不同圆环内簇头的剩余能量

6 结束语

本文在深入研究 WSN 数据转发规律和能量空洞攻击机制的基础上，建立了基于簇头生命周期最

优的攻击抑制模型并给出了约束条件,设计了一种不等簇半径的 WSN 能量空洞攻击抑制算法。与其他抑制算法相比,本文算法在优化网络节点布局的同时给出了动态簇头的移动路径。簇头生命周期对比分析和仿真实验结果表明,本文模型和算法可有效抑制能量空洞攻击。

参考文献:

- [1] 郁滨,周伟伟. ZigBee 同频攻击检测抑制模型研究[J]. 电子与信息学报, 2015, 37(9):2211-2217.
YU B, ZHOU W W. Co-channel attack detection and suppression model for ZigBee network nodes[J]. Journal of Electronics and Information Technology, 2015, 37(9):2211-2217.
- [2] KAI L, GE H W, XIONG N X, et al. Energy efficiency QoS assurance routing in wireless multimedia sensor networks[J]. IEEE Systems Journal, 2011, 5(4): 495-505.
- [3] HOU Y T, SHI Y, SHERALI H D, et al. On energy provisioning and relay node placement for wireless sensor network[J]. IEEE Transactions on Wireless Communications, 2005, 4(5): 2579-2590.
- [4] 周伟伟,岳云天,郁滨. ZigBee 节点多因子身份认证方案研究[J]. 系统仿真学报, 2015, 27(4):762-769.
ZHOU W W, YUE Y T, YU B. Research of multi-factor identity authentication scheme for ZigBee network nodes[J]. Journal of System Simulation, 2015, 27(4):762-769.
- [5] LI J, MOHAPATRA P. Analytical modeling and mitigation techniques for the energy holes in sensor networks[J]. Pervasive and Mobile Computing, 2007, 3(3):233-254.
- [6] JU R, ZHANG Y X, ZHANG K, et al. Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks[J]. IEEE Transactions on Industrial Informatics, 2016, 12(2):788-800.
- [7] KAMRAN L, NADEEM J, ASHFAQ A, et al. On energy hole and coverage hole avoidance in underwater wireless sensor networks[J]. IEEE Sensors Journal, 2016, 16(11):4431-4442.
- [8] XUE Y, CHANG X M, ZHONG S M, et al. An efficient energy hole alleviating algorithm for wireless sensor networks[J]. IEEE Transactions on Consumer Electronics, 2014, 60(3):347-355.
- [9] PERILLO M, CHENG Z, HEINZELMAN W. On the problem of unbalanced load distribution in wireless sensor networks[C]//The IEEE Global Telecommunications Conference Workshops (GLOBECOM'04). 2004:74-79.
- [10] HEINZELMAN W B, CHANDRAKASAN A P, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4):660-670.
- [11] DU T, QU S N, LIU F G, et al. An energy efficiency semi-static routing algorithm for WSNs based on HAC clustering method[J]. Information Fusion, 2015, 21(1):18-29.
- [12] WU X, CHEN G, DAS S K. Avoiding energy holes in wireless sensor networks with nonuniform node distribution[J]. IEEE Transaction on Parallel and Distributed Systems, 2008, 19(5):710-720.
- [13] KIM M G, HAN Y T, PARK H S. Energy-aware hybrid data aggregation mechanism considering the energy hole problem in asynchronous MAC-based WSNs[J]. IEEE Communications Letters, 2011, 15(11): 1169-1171.
- [14] MOHAMMED A, SABSH M, AHMED N S, et al. Mobile sink-based adaptive immune energy-efficient clustering protocol for improving the lifetime and stability period of wireless sensor networks[J]. IEEE Sensors Journal, 2015, 15(8):4576-4586.
- [15] LIU X X. A novel transmission range adjustment strategy for energy hole avoiding in wireless sensor networks[J]. Journal of Network and Computer Applications, 2016, 67(5):43-52.
- [16] MADAN R, LALL S. Distributed algorithms for maximum lifetime routing in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(8):2185-2193.
- [17] 余荣,孙智,周海军,等. 保证服务质量的最小能量无线传感器网络路由算法[J]. 清华大学学报(自然科学版), 2007, 47(10): 1634-1637.
YU R, SUN Z, ZHOU H J, et al. QoS and energy aware routing algorithm for wireless sensor networks[J]. Journal of Tsinghua University (Science and Technology), 2007, 47(10): 1634-1637.
- [18] 刘震,郭航. 基于同心环分簇网络模型的 WSN 能量空洞避免方法研究[J]. 计算机科学, 2013, 40(12):147-151.
LIU Z, GUO H. Study on concentric-ring and cluster-based energy hole avoiding method in wireless sensor networks[J]. Computer Science, 2013, 40(12): 147-151.

作者简介:



周伟伟(1990-),男,河南洛阳人,信息工程大学博士生,主要研究方向为无线传感器网络、物联网、博弈论和信息安全技术等。



郁滨(1964-),男,河南郑州人,博士,信息工程大学教授、博士生导师,主要研究方向为无线网络安全、电磁防护、图像处理、信息安全技术等。