ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.4, April 2009, pp.1038−1047
doi: 10.3724/SP.J.1001.2009.03251

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

移动传感器网络基于安全连接的节点位置优化*

贾 杰[1+], 陈 剑[1], 常桂然[2], 闻英友[1]

[1](东北大学 信息科学与工程学院,辽宁 沈阳 110004)

[2](东北大学 计算中心,辽宁 沈阳 110004)

Optimal Sensor Deployment Based on Secure Connection in Mobile Sensor Network

JIA Jie[1+], CHEN Jian[1], CHANG Gui-Ran[2], WEN Ying-You[1]

[1](College of Information Science and Engineering, Northeastern University, Shenyang 110004, China)

[2](Computing Center, Northeastern University, Shenyang 110004, China)

+ Corresponding author: E-mail: jiajieneu@163.com

Jia J, Chen J, Chang GR, Wen YY. Optimal sensor deployment based on secure connection in mobile sensor network. *Journal of Software*, 2009,20(4):1038−1047. http://www.jos.org.cn/1000-9825/3251.htm

Abstract: The reasonable deployment of sensor nodes while guaranteeing the secure connection is one of the most important challenges in designing wireless sensor network. Traditional algorithms merely aim at network coverage rate, which leads to the reduction of the secure connectivity degree. In this paper, the model of sensor nodes deployment is theoretically analyzed. Combined with rapid multi-objective optimization of the capacity of elitism non-dominated sorting genetic algorithm, an optimal sensor deployment algorithm based on secure connection is proposed, to guarantee the effect of network tracking and secure communication. The performance of algorithms under different deployment model is analyzed. Simulation results demonstrate that the novel algorithm proposed in this paper can implement network coverage rate and secure connection degree more rapidly and efficiently and hence meets the actual demand in wireless sensor network.

Key words: mobile sensor network; secure connection; deployment optimization; elitism non-dominated sorting genetic algorithm

摘 要: 传感器节点的合理分布并保障节点间安全通信是无线传感器网络设计中的关键问题.传统的节点分布优化算法仅以提高网络有效覆盖率为目标,极易导致网络安全连接度的降低.针对该问题,从理论上对传感器网络拓扑模型进行了建模分析.结合具有快速多目标优化能力的精锐非支配遗传算法,提出一种基于安全连接的节点位置优化算法,从而保证网络实现目标跟踪和安全通信的质量效果.分析了随机部署模型与基于预知分配坐标的高斯部署模型下算法的求解性能,仿真结果表明,所提出的算法能够快速收敛于网络覆盖率和安全连通度两者的折衷点,满足无线传感器网络的实际需求.

关键词: 移动传感器网络;安全连接;分布优化;精锐非支配遗传算法

* Supported by the National Natural Science Foundation of China under Grant No.60602061 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z413 (国家高技术研究发展计划(863)); the Natural Science Foundation of Liaoning Province of China under Grant No.20042042 (辽宁省自然科学基金)

Received 2007-06-30; Accepted 2007-12-24

中图法分类号: TP393 文献标识码: A

由于无线传感器网络(wireless sensor network,简称 WSN)所具有的大规模、自组织、随机部署、环境复杂、传感器节点资源有限、网络拓扑动态变化的特点,使得传感器网络的各个设计目标之间需要相互融合[1],偏向于任何一个设计目标都有可能损害其他研究目标.本文正是基于这一准则,系统地研究了传感器网络中节点位置优化与安全通信之间的关系,并提出一种基于安全连接的节点分布优化算法.

传感器网络节点位置优化是传感器网络的基本问题,属于网络拓扑控制范畴.节点位置的合理分布是保证网络覆盖质量和连通质量的前提条件,并能为 MAC 协议、路由协议的可靠性和可扩展性提供基础.由于受到传感器网络工作环境的限制,现有节点分布优化大多采用随机部署的策略.由于在随机部署环境中,节点分布的不均匀性易导致感知盲区的产生,随着微机电系统(micro-electro-mechanical systems,简称 MEMS)研究的进步,已经提出若干基于移动节点的拓扑控制算法[1−6],使得利用节点的移动性对感知盲区修补成为可能.在这些算法中,虚拟力导向算法[4,6]在提高网络覆盖率性能方面表现突出,该算法把每个传感器节点近似为一个虚拟电荷,由于受到其他节点的虚拟力作用向目标区域扩散,最终达到平衡状态,从而实现网络的充分覆盖.针对随机部署的缺陷,提出将监测区域划分为若干不相关区域,每组划分区域均对应一组节点,该组节点服从以分区中心为均值的高斯分布,这种部署方案即为高斯部署方案,现已证明高斯部署方案具有比随机部署方案更为优良的分布特性[7].由于高斯部署方案可以估计节点的最终分布位置,把对节点位置的估计融合于现有网络密钥分配机制,从而提高网络密钥分配的效率.但现有算法大多集中于如何极大化网络整体覆盖率以及减少网络冗余覆盖,对于节点分布优化和网络安全连接的关系还未展开研究.

安全是传感器网络的首要研究问题之一.在传感器网络部署初期,特别是在无人触及或容易受损的环境中,保证网络的安全性具有重要意义.对于安全通信而言,密钥管理是保证网络安全、提供可靠通信的重要内容.由于传统网络采用的集中性密钥服务器会带来大量的通信消息,并不适合资源受限的传感器网络节点.为了满足传感器网络的特定需求,已经提出若干适用于 WSN 的随机密钥预分配方案[7−11].预分配密钥方案使用随机图模型阐述节点之间是否存在安全连接,是目前研究最为广泛的密钥分配机制[8].该机制从一个大密钥池里随机选取一部分密钥[8]或者从多个密钥空间里随机选取若干个密钥[9]作为节点的密钥环.获取方式可以使用地理信息[8]、对称 BIBD(balanced incomplete block design)[10]、对称多项式[11]等.节点部署于目标区域后,互为邻居的各个节点之间通过某种协议确认彼此是否含有共享密钥消息,判断节点之间是否可以建立安全连接.若要完成节点之间安全连接的建立,需要满足两个条件:(1) 节点之间欧氏距离需要小于或等于其通信距离;(2) 节点之间需要存在至少一对共享安全密钥.利用高斯部署模型,Wu 在静态 WSN 中建立了基于地理信息的随机密钥预分配方案[7].假定网络的部署目标区域是一个二维矩形区域,且节点部署服从高斯分布,节点被划分为 $t\times n$ 个部署组,每个组 G_{ij}(i=1,…,t,j=1,…,n)的部署位置组成一个栅格.密钥池(密钥数为$|S|$)被划分成若干个子密钥池(密钥数为$|S_c|$),每个子密钥池对应一个部署组.若两个子密钥池水平或垂直相邻,则至少共享 $a|S_c|$个密钥;若两个子密钥池对角相邻,则至少共享 $b|S_c|$个密钥(a,b 满足以下关系:$0<a,b<0.25$ 且 $4a+4b=1$),如图 1 所示.对于组内每一节点,从对应的子密钥池中随机选取 m 个不同的密钥.在初始部署后,邻居节点之间根据是否存在共享密钥建立安全连接.与 Eschenauer 和 Gligor 所提出的随机密钥预分配方案(简称 E-G 方案)[8]相比,使用部署知识减少了节点预分配无用密钥的数量,提高了互为邻居节点之间的共享密钥概率,增强了网络抗毁性.

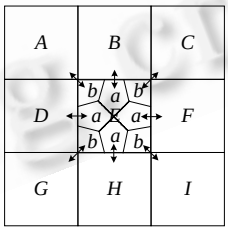


Fig.1 Probability of sharing secret key between neighboring key pool

图 1 相邻密钥池间共享密钥概率

由于随机部署环境中节点分布的不均匀性,利用移动节点对感知盲区的修复容易中断预先建立的安全连接.而采用基于预知地理信息的高斯部署模型后,虽然能够有效地提高节点之间安全连接建立的概率[7,12,13],但网络的安全连接度却会随着网络覆盖控制的调整而发生变化.如何研究一种能够同时兼顾网络覆盖率和网络

安全的拓扑控制机制,无疑具有重要意义.

1 问题模型与假设

针对无线传感器网络特点,给出如下假设:

(1) 假设传感器网络监测区域远大于网络边界范围,忽略边界效应对传感器网络的影响;

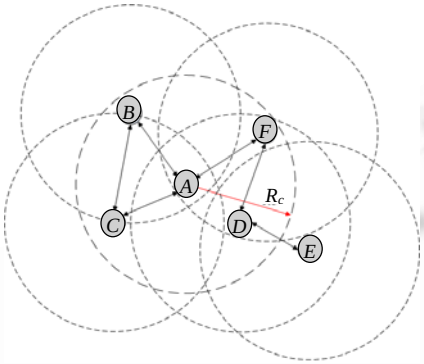
(2) 初始化配置后,各节点可以通过某种方式(如采用 GPS 定位系统或者相对定位算法等)迅速定位;

(3) 网络采用分簇结构,簇首选取算法与 HEED(hybrid energy-efficient distributed clustering)[14]类似,簇首选择主要依据两个因素,即主因素剩余能量和次因素簇内通信代价.通过周期性迭代的方法实现分簇,保证选举的簇首其能量充裕,能够完成节点分布优化算法的运算以及运算结果的广播;

(4) 节点具有移动能力,能够准确移动至优化后的位置中.

1.1 基于安全的节点分布优化问题

在传感器节点初始部署后,含有共享密钥的邻居节点之间通过交换共享密钥和节点 ID 号完成安全连接的建立,从而能够极大地防止恶意节点入侵,为全网数据的安全通信提供保障.网络初始安全拓扑可以抽象为二维平面内有向图 $G(V,E)$,其中 V,E 分别表示节点、安全连接的集合,$E\subseteq V\times V$.节点 i 的安全连接邻居节点集定义为有向图 $G(V,E)$内以 i 为中心、R_c 为半径的圆面区域内存在安全连接的节点集合,记作 $N(i)$.一个六节点的安全连接生成图如图 2 所示.节点 A 与节点 D 之间由于不存在共享密钥,在互为邻居节点的情况下,并不存在安全连接.



$N(A)=\{B,C,F\};N(B)=\{A,C\};N(C)=\{A,B\}$
$N(D)=\{E,F\};N(E)=\{D\};N(F)=\{A,D\}$

Fig.2 Graph of secure connection

图 2 安全连接生成图

由于传感器网络的初始拓扑并不能保证网络的有效覆盖,因此,应采用一种拓扑控制算法以在二者之间取得折衷,寻求安全连通情况下的网络最优覆盖.传感器网络中,基于安全的节点分布优化算法的主要任务即在完成节点初始安全连接建立的条件下,通过对节点位置的有效调整维持网络初始安全连通度且极大化网络有效覆盖率.问题形式上表述如下:二维目标监测区域 A 上随机投放 N 个节点,节点集 $S=\{s_1,s_2,\ldots,s_N\}$.需要寻找节点集最优分布组合 $\{\bar{X}_S,\bar{Y}_S\}=\{(x_{s_1},y_{s_1}),(x_{s_2},y_{s_2}),\ldots,(x_{s_N},y_{s_N})\}$,在不减少网络初始安全连通度 $SecLink(S)$的前提下,最大化网络有效覆盖率 $P_{cov}(S)$.可见,基于安全的节点分布优化问题是一个典型的多目标优化问题.

目标 1:网络有效覆盖率.定义为

$$\text{Max. } f_1(\bar{x})=P_{cov}(S) \tag{1}$$

目标 2:网络安全连通度.初始化部署后,若节点之间欧氏距离小于节点通信半径且存在共享密钥消息,则建立安全连接.网络安全连通度定义为拓扑控制前、后仍保持安全连接的链路总数:

$$\text{Max. } f_2(\bar{x})=SecLink(S)=\sum_i\sum_{j\in N(i)}SecLink(s_i,s_j) \tag{2}$$

$SecLink(s_i,s_j)$表示节点位置变化前、后的安全连接情况,定义为

$$SecLink(s_i,s_j)=\begin{cases}1, & \text{if } d(s_i,s_j)<R_c \text{ and } s_j \text{ shares key}\\ 0, & \text{otherwise}\end{cases} \tag{3}$$

对于每一个节点而言,还需要考虑节点位置移动所消耗的能量,因此,限定每个节点最大位移为 d_{th},有

$$d\,|s_i'(x,y)-s_i(x,y)|\le d_{th} \tag{4}$$

其中,$s_i'(x,y)$ 表示优化后的节点位置.

基于安全的节点分布优化问题所求目标函数的 2D 目标空间如图 3 所示.在所有目标的情况下,若一解向量不受任何其他决策向量支配,则这样的解称为 Pareto 最优解,如图 3 中白色点表示.全体 Pareto 解的集合以 X_p

表示,称为 Pareto 最优组.Pareto 最优组对应的目标向量称为 Pareto 最优前沿(Pareto optimal front),记为 $F(X_p)$,如图 3 中曲线所示.

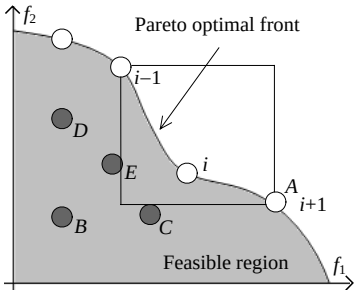


Fig.3 Illustration of Pareto solution

图 3 Pareto 解优化说明

1.2 传感器网络覆盖模型

传感器节点的感知模型直接决定其覆盖范围和监测能力,并最终决定网络有效覆盖率.本文选取二元感知模型,认为传感器节点的覆盖范围是一个以节点为圆心、半径为 r 的圆形区域,该圆形区域称为传感器节点的感知圆盘,r 称为传感器节点的感知半径,r 的大小由节点感知单元的能量特性决定.假定监测区域 A 上传感器节点集 $S=\{s_1,s_2,\ldots,s_N\}$,其中,$s_i=\{x_i,y_i,r_i\}$为节点 i 的覆盖模型,(x_i,y_i)为节点 i 的坐标,r_i 为节点 i 的感知半径.区域 A 上任意点 $P(x,y)$被节点 i 覆盖的事件定义为 I_i,点 $P(x,y)$被传感器节点 i 所覆盖的概率 $P_{cov}\{x,y,s_i\}$为一个二值函数:

$$P\{I_i\}=P_{cov}(x,y,s_i)=\begin{cases}1, & \text{若}(x-x_i)^2+(y-y_i)^2\le r_i^2\\ 0, & \text{其他}\end{cases} \tag{5}$$

且

$$P\{\overline{I}_i\}=1-P\{I_i\}=1-P_{cov}(x,y,s_i) \tag{6}$$

$\overline{I}_i$ 为 I_i 的补,表示点 $P(x,y)$未被传感器节点 i 覆盖.如果 I_i 和 I_j 无关,则存在如下关系:

$$P\{I_i\cup I_j\}=1-P\{\overline{I}_i\cap\overline{I}_j\}=1-P\{\overline{I}_i\}\cdot P\{\overline{I}_j\} \tag{7}$$

节点集 S 中只要有一个节点覆盖点 $P(x,y)$,即认为 $P(x,y)$被 S 覆盖.任意点 $P(x,y)$被节点集 S 覆盖的概率为

$$P_{cov}(x,y,S)=P\left\{\bigcup_{i=1}^{N}I_i\right\}=1-P\left\{\bigcap_{i=1}^{N}\overline{I}_i\right\}=1-\prod_{i=1}^{N}(1-P_{cov}(x,y,s_i)) \tag{8}$$

将监测区域 A 数字离散化为 $m\times n$ 个像素,每个像素的面积为$\Delta x\times\Delta y$,每个像素是否被覆盖由 $P_{cov}(x,y,S)$来衡量,则节点集 S 的有效覆盖率 $P_{cov}(S)$即为节点集 S 的覆盖面积 $A_{area}(S)$与监测区域 A 的总面积 A_s 之比:

$$P_{cov}(S)=\frac{A_{area}(S)}{A_S}=\frac{\sum_{x=1}^{m}\sum_{y=1}^{n}P_{cov}(x,y,S)\cdot\Delta x\cdot\Delta y}{\sum_{x=1}^{m}\sum_{y=1}^{n}\Delta x\cdot\Delta y}=\frac{\sum_{x=1}^{m}\sum_{y=1}^{n}P_{cov}(x,y,S)}{m\times n} \tag{9}$$

2 基于安全的节点位置优化算法

基于安全的传感器网络节点位置优化问题可以描述为以初始节点位置构成的坐标向量为输入参数、网络覆盖率和安全连通度为优化目标的优化问题.对于传统的单目标优化问题求解较为简单,例如,求最大网络有效覆盖率等.但对于网络覆盖率和安全连通度两个优化目标而言,由于目标间存在冲突,两者之间不存在唯一的最大值或最小值.相反地,需要寻找一个或多个冲突目标之间的折衷解,即 Pareto 最优解.由于常规算法在求解 Pareto 解上存在着困难[15],本文提出一种基于不受支配分类遗传算法(non-dominated sorting genetic algorithm II,简称 NSGA-II)的多目标优化算法.与传统的启发式算法相比,多目标进化类优化算法(multi-objective

evolutionary algorithm,简称 MOEA)具有多点搜索且优化过程中始终保持唯一最优解群体的特性,使得 MOEA 在求解多目标优化问题时具有优势.目前,多目标进化类算法已得到了广泛的研究,产生了 VELA,SPEA[16], NSGA[17],NSGA-II[18]等多种进化算法.NSGA 由两个主要过程构成:1) Pareto 排序过程用来强化不受支配个体;2) 适值分享过程用来保持群的多样性.NSGA-II 是在 NSGA 的基础上改进得到的一种 MOEA,它从 3 个方面对旧版进行改进:第一,不受支配的分类过程更快,搜索过程能够迅速收敛到 Pareto 最优前沿;第二,NSGA-II 用拥挤比较算子代替适值共享,不需要共享参数σ_{share},保证了群体多样性;第三,引入优越策略,防止优秀解的丢失.与其他多目标进化算法相比,NSGA-II 具有运算速度快、稳健性强、鲁棒性好、解集分散等特点,已成功应用于多目标优化领域.由于 NSGA-II 仅提供一种寻求 Pareto 最优前沿的方法,故针对 Pareto 解的选择,本文提供一种基于达标原理的方法.使用每个目标函数的上界和下界来定义目标,定义的不是一个目标点,而是一个目标区域.目标区域通常是部分搜索空间,并根据实际的折衷信息进行适应性调整.对目标区域里的解,分配的适值更高,使得搜索向着 Pareto 最优前沿的期望部分进行.这样,决策者可以放大全局的 Pareto 最优前沿,并得到一个更加精确的描述.

2.1 问题编码以及交叉和变异算子选择

遗传算法并不直接处理最优化问题的决策变量,而是与类似染色体的编码一起运行,用编码来表示解.本文采用以节点坐标作为染色体的编码方案,利用节点坐标的向量变化表示节点位置的移动情况,种群中,个体染色体编码表示全局节点的拓扑方案,从而完成问题空间和决策空间的映射.基于节点坐标的编码方案如图 4 所示.

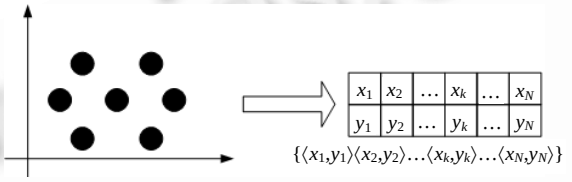


Fig.4 Coding representation of the optimal node distribution problem

图 4 节点优化分布问题编码方案

遗传算法通过引入重组和变异算子来不断修改被选中的个体,并在挑选间隔之间引入新个体,完成种群的进化.但是,由于本文采用基于节点坐标的编码方案,传统二进制遗传算法(genetic algorithm,简称 GA)中使用的遗传算子不能直接用于坐标向量中,故引入模拟二进制交叉(simulated binary crossover,简称 SBX)算法.SBX 从父代$\bar{a}_1$和$\bar{a}_2$中产生两个子代,用$\bar{c}_1$和$\bar{c}_2$表示,则子代个体中每个等位基因$C_{1,i}(x_{c_{1,i}}, y_{c_{1,i}})$和$C_{2,i}(x_{c_{2,i}}, y_{c_{2,i}})$分别表示为

$$\begin{cases} x_{c_{1,i}} = 0.5\cdot((1+\beta)\cdot x_{a_{1,i}} + (1-\beta)\cdot x_{a_{2,i}}) \\ y_{c_{1,i}} = 0.5\cdot((1+\beta)\cdot y_{a_{1,i}} + (1-\beta)\cdot y_{a_{2,i}}) \end{cases} \tag{10}$$

$$\begin{cases} x_{c_{2,i}} = 0.5\cdot((1-\beta)\cdot x_{a_{1,i}} + (1+\beta)\cdot x_{a_{2,i}}) \\ y_{c_{2,i}} = 0.5\cdot((1-\beta)\cdot y_{a_{1,i}} + (1+\beta)\cdot y_{a_{2,i}}) \end{cases} \tag{11}$$

其中,β表示该元素对应概率分布曲线的积分上限.

变异操作只应用于由双亲繁殖所得的后代个体,在所有后代个体构成的基因组集合中,按变异概率P_m选取基因组进行变异操作.如果元素a_i被选中参与变异,则

$$a_i' = \begin{cases} a_i - \delta(t, a_i - L_i), & random(0,1)<0.5 \\ a_i + \delta(t, U_i - a_i), & random(0,1)>0.5 \end{cases} \tag{12}$$

t是代数,L_i和U_i分别是a_i的上界和下界.指数函数$\delta(t,x)$定义如下:

$$\delta(t,x) = x\cdot u\cdot\left(-\frac{t}{T}\right)^{\eta},\ 0\le u\le 1 \tag{13}$$

其中,u是随机数,T是最大代数,η是决定概率分布的指数.返回一个[0,x]值,使得概率随着t的增加越来越接近于

0.该特性使得变异算子在 t 很小时均匀搜索解空间,保证群体多样性.在后期阶段搜索局部区域,提高搜索效率.

2.2 算法求解过程

簇首节点执行节点位置优化算法,完成全网节点最终位置计算后,簇首广播各节点的最终位置.为了完成优化算法的计算,簇首节点需要收集全局节点的初始位置信息和每个节点的ID.在算法实施过程中,传感器节点并不移动,而是计算随机部署的节点虚拟移动轨迹.一旦传感器节点位置确定后,则对相应节点进行移动操作.采用簇首节点执行优化算法能够节省每个节点分别计算所导致的能量消耗.在优化算法执行过程中,每个节点仅移动 1 次,有效避免了节点频繁移动对能量的消耗,延长了网络的生命周期.算法求解过程如图 5 所示.

Input: Initial sensor location $\{\overline{X}_{S\_initial},\overline{Y}_{S\_initial}\}$
Given number of generations T and Population size K
Recombination probability P_r and Mutation probability P_m
Reduction rate of the controlled elitism ρ;
Output: new sensors' location $\{\overline{X}_S,\overline{Y}_S\}$.

Step 1 (initialization):
  Set t=0,P'=∅;
  Generate an initial population P randomly;
  Calculate $P_{cov}(S)$ and $SecLinks(S)$ for each individual;
Step 2 (Non-Dominated sorting):
  P=P∪P';
  Do fast non-doninated sorting algorithm, resulting non-dominated fronts (F_1,F_2,…,F_R);
Step 3 (controlled elitism)
  Set r=1 and P=∅;
  While |P|<K **do**
    (1) Calculate n_r according to the controlled elitism scheme;
    (2) Sort F_r in descending order using crowded comparison;
    (3) Put the first n_r members of F_r in P, i.e., P=P∪F_r[1:n_r];
    (4) r=r+1.
Step 4 (Fitness assignment):
  Assign fitness to each individual according to its position in P;
Step 5 (Reproduction)
  Generate an offspring P' from P according to SBX and mutation operator;
  Calculate $P_{cov}(S)$ and $SecLinks(S)$ for each individual in P';
Step 6 (Termination):
  t=t+1;
  if t≥T or the required $P_{cov}(S)$ and $SecLinks(S)$ are met, **then** terminate;
  else go to **Step 2**.

Fig.5 Pseudocode of optimal nodes distribution algorithm based on security

图 5 基于安全的节点分布优化算法伪代码

在最坏情况下,fast-non-dominated sorting algorithm 的运算复杂度为 $O(2N^2)$,拥挤比较算子的运算复杂度为 $O(2N\log N)$,受控超越排序复杂度为 $O(2N\log(2N))$,因此,整个算法复杂度为 $O(2N^2)$,N 为部署节点总数.

3 算法仿真

为了验证算法的有效性,在 Matlab 环境下对算法进行评估.在所有的实验中,节点的通信半径均设置为感知半径的 2 倍,即保证在网络充分覆盖的情况下,网络总是连通的[19].

3.1 随机部署模型

随机部署模型是一种最为简单的节点放置策略,对任意网络节点 i 而言,其位置概率分布函数为

$$f_i(x,y)=\frac{1}{XY},x\in[0,X],y\in[0,Y],1\le i\le N \tag{14}$$

其中,X,Y 分别表示监测区域的长度和宽度,N 为投放节点总数.此时,各节点位置分布服从监测区域的均匀分布.随机密钥预分配方案采用 E-G 方案,部署前,服务器生成一个密钥总数为 P 的大密钥池及密钥标识,每一节点从密钥池里随机选取 k(k<<P)个不同密钥,这种随机预分配方式使得任意两个节点能够以一定的概率存在着共享

密钥.随机部署后,两个相邻节点若存在共享密钥,就随机选取其中的一个作为双方的配对密钥.

在 50×50 的监测区域上投放 32 个节点进行拓扑控制,节点感知半径为 7,根据随机图理论中节点度与网络节点总数的关系[12],有

$$p=\frac{n-1}{n}(\ln(n)-\ln(-\ln P_c)) \tag{15}$$

$$p'=1-\frac{((P-k)!)^2}{P!(P-2k)!} \tag{16}$$

当随机图连通概率 P_c=0.99 时,节点度 d=8,密钥池大小为 100 000,每个节点所携带密钥长度为 263,任意两个节点间存在共享密钥的概率为 0.5.

首先考察仅以网络覆盖率为优化目标、网络节点与安全连通度的变化情况,选用单目标遗传算法(single-objective genetic algorithm,简称 SGA).算法运行 200 代,仿真结果如图 6 所示.其中,连线表示节点之间存在安全连接.由图 6 可知,不考虑网络安全连接的情况下,虽然提高了网络覆盖率,但由于单目标优化算法忽视节点初始安全连接,最终导致网络安全连通度的极大损失.

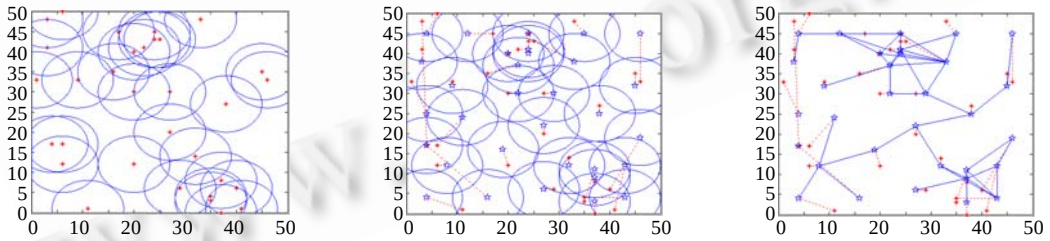
(a) Initial secure connection
(a) 初始化网络拓扑

(b) Final secure connection
(b) 最终节点安全覆盖

Fig.6 Results of single-objective genetic algorithm

图 6 单目标优化算法结果

然后考察安全连通度和网络覆盖率两个优化目标,算法选用 NSGA-II.为了直观比较单目标优化与多目标优化的区别,仿真在相同实验场景下进行,初始化网络拓扑与图 6(a)所示相同,算法运行 200 代,仿真结果如图 7 所示.其中,星号表示节点初始化位置,五角星表示节点最终优化位置,虚线表示节点移动轨迹,实线表示节点间安全连接关系.由图 7 可知,节点最终分布能够同时兼顾网络整体覆盖率和安全连通度,最终安全连接数目为 86,比初始化的 97 个安全连接稍少.但网络覆盖率则从初始化的 79.36%提高至 99.84%.可见,NSGA-II 能够快速计算网络覆盖率与网络安全连通度之间的折衷点,从而在保证网络安全性的前提下,提高网络有效覆盖面积.



(a) Initial network coverage
(a) 初始化网络拓扑

(b) Final network coverage
(b) 最终节点安全覆盖

(c) Change of secure connection degree
(c) 网络安全拓扑变化

Fig.7 Results of the multi-objective optimal algorithm

图 7 多目标优化算法优化结果

3.2 基于预知分配坐标的高斯部署模型

首先将整个投放区域离散化为 $t\times n$ 个相同面积的网格,同时对部署节点均匀划分为等量的 $t\times n$ 组,每组节点对应一个网格,且各组节点分布函数服从以对应网格为中心 $u=(x_i,y_i)$的二维高斯分布.

$$f_k^i(x,y\mid k\in G_{i,j})=\frac{1}{2\pi\sigma^2}e^{-[(x-x_i)^2+(y-y_i)^2]/2\sigma^2}=f(x-x_i,y-y_i) \tag{17}$$

其中,(x,y)表示第 K 组中任意节点的坐标,且每组中节点被选取的概率相同,均为 $1/(t\times n)$.节点概率分布函数为

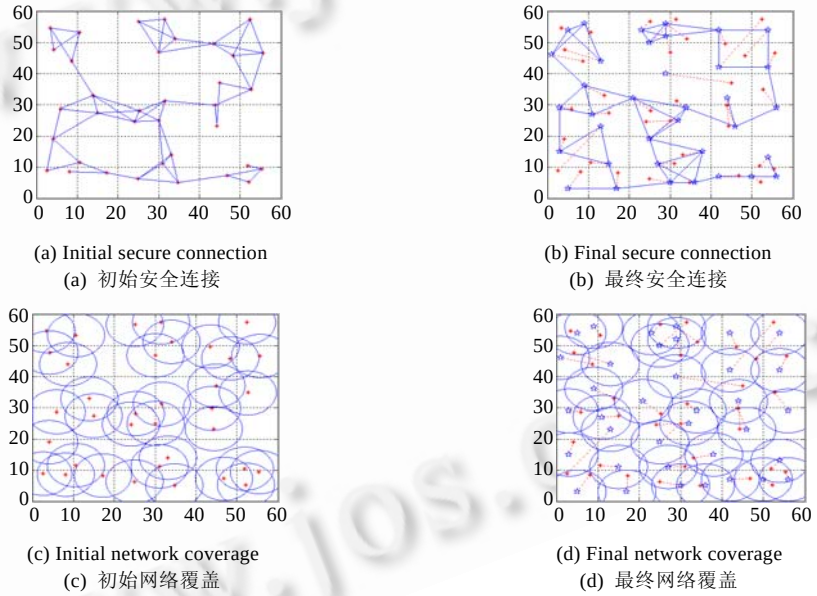
$$f_{overall}(x,y)=\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{1}{t\cdot n}\cdot f_k(x,y\mid k\in G_{i,j}) \tag{18}$$

采用基于分区为中心的高斯节点部署模型后,每组节点偏离分区中心 3σ距离的概率均小于 0.01(σ为高斯分布的方差).对同一个监测区域的节点或者相邻区域之间分配相同的密钥池,可以保证相同区域以及相邻区域节点之间更大的安全连通概率,并且在获得相同共享概率的条件下,所需密钥链长度更短.

为了考察高斯部署模型下算法性能的对比情况,我们设计了两个实验.首先在 60×60 监测区域上投放 36 个节点,节点感知半径为 7,监测区域均匀分割成大小为 20×20 的 9 个正方形区域,对应每个区域,节点分成 9 组,每组 4 个节点,各组节点均服从以节点中心为均值的高斯分布,节点变化方差σ^2=25.总节点密钥池大小为 100 000,$t=n=3$,$a=0.167$,$b=0.083$,各区域的密钥池大小$|S_c|$为[20]

$$|S_c|=\frac{|S|}{tn-(2tn-t-n)a-2(tn-t-n+1)b}=15899 \tag{19}$$

根据局部连通概率公式,选取节点密钥链长度为 67,则相邻节点间存在共享密钥概率 p=0.5.基于安全的节点分布优化算法运行至 200 代,其仿真结果如图 8 所示.



(a) Initial secure connection (a) 初始安全连接

(b) Final secure connection (b) 最终安全连接

(c) Initial network coverage (c) 初始网络覆盖

(d) Final network coverage (d) 最终网络覆盖

Fig.8 Simulation results of algorithm under Gaussian deployment deviation

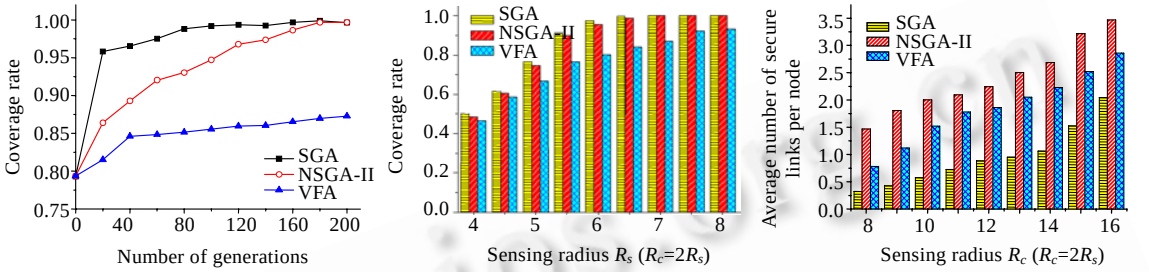
图 8 高斯部署模型下算法仿真结果

从图 8 中可以看出,在高斯节点部署模型下,采用基于安全的网络节点分布优化算法后,网络安全连通度由初始的 116 变化至 103,覆盖率从初始的 86.23%增加至 98.86%,且高斯部署模型具有比随机部署更为优良的节点分布特性.因此,在相同的密钥共享概率的前提下,除了需要更少的密钥长度外,网络能够获得更高的安全连通度.

鉴于现有虚拟力的拓扑控制算法在提高网络覆盖率性能上表现优异,接着我们考察了精锐非支配遗传算

法与虚拟力算法(virtual force algorithm,简称 VFA)以及 SGA 的性能对比情况.节点部署模型选用高斯模型,分别考察在感知半径为 7m 时 3 种算法的收敛速度对比情况以及在不同感知半径条件下,网络覆盖率和安全连通度的性能对比情况(由于在感知半径为 7m 时,NSGA-II 算法已经能够完成整个网络的充分覆盖,因此,设置网络节点感知半径变化范围为 4~8).

图 9(a)表示 SGA,NSGA-II,VFA 这 3 种算法收敛速度的对比情况.由于 NSGA-II 内在的全局搜索最优节点位置分布策略,算法迭代 180 代已经收敛至最优值,而 VFA 直至 160 代仍未完成搜索过程,因此,NSGA-II 其收敛速度优于 VFA.图 9(b)、图 9(c)分别表示 3 种算法网络覆盖率和网络安全连通度的对比情况.从图 9 中可以看出,SGA 虽然获得较好的网络覆盖率和较快的收敛速度,但是由于网络节点的全局移动,导致网络安全连通度的极大损失.采用基于安全的节点分布优化算法后,能够在网络覆盖率和安全连接数目之间达到平衡,具有比 VFA 更高的网络覆盖率且更高的网络安全性,其整体性能效果优于 VFA 和 SGA.



(a) Comparison of the convergence process (a) 收敛过程比较

(b) Comparison of the coverage rate (b) 网络覆盖率比较

(c) Comparison of the secure connection degree (c) 网络安全连通度比较

Fig.9 Comparisons of some algorithms

图 9 算法性能对比情况

4 结 论

无线传感网络节点位置优化有利于改善网络性能,提高网络有效覆盖面积.但是,现有优化算法在改善网络有效覆盖面积的同时,却极易导致网络初始化安全连通度损失.本文从理论上对传感器节点拓扑模型进行了建模分析,提出一种基于精锐非支配遗传算法的安全拓扑控制策略.通过非支配遗传算法完成网络覆盖率和安全连通度的折衷,动态优化网络节点位置分布,极小化网络安全连通度减少的损失,从而能够保证网络实现目标跟踪和安全通信的质量效果,满足无线传感器网络的实际需求.由于传感器网络通常工作在复杂的环境下,且因为实际需求有所不同而采用不同的部署模型,为使其应用范围更加广泛,本文分别对不同部署模型下算法有效性进行了仿真实验.实验结果表明,基于非支配遗传算法的优化策略能够快速实现对移动传感网络中节点位置的全局优化,并有效保持安全连通度.在不同节点部署模型下算法均表现优异,性能优于现有虚拟力算法,且收敛速度更快.

References:

[1] Poduri S, Pattem S, Krishnamachari B, Sukhatme G. A unifying framework for tunable topology control in sensor networks. Technical Report, CRES-05-004, Los Angeles: University of Southern California, 2005. 1−15.

[2] Heo N, Varshney PK. A distributed self spreading algorithm for mobile wireless sensor networks. In: Tachikawa K, ed. Proc. of the IEEE Conf. on Wireless Communications and Networking. New Orleans: IEEE Press, 2003. 1597−1602.

[3] Dhillon SS, Chakrabarty K. Sensor placement for effective coverage and surveillance in distributed sensor networks. In: Tachikawa K, ed. Proc. of the IEEE Conf. on Wireless Communications and Networking. New Orleans: IEEE Press, 2003. 1609−1614.

[4] Wong T, Tsuchiya T, Kikuno T. A self-organizing technique for sensor placement in wireless micro-sensor networks. In: Aoki K, ed. Proc. of the 18th Int'l Conf. on Advanced Information Networking and Application. Fukuoka: IEEE Press, 2004. 78−83.

[5] Zhou S, Wu MY, Shu W. Finding optimal placement for mobile sensors: Wireless sensor network topology adjustment. In: Proc. of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication. Shanghai: IEEE Press, 2004. 529−532. http://ieeexplore.ieee.org/iel5/9237/29278/01321942.pdf?arnumber=1321942

[6] Wang G, Cao G, Porta TL. Movement-Assisted sensor deployment. In: Li VOK, ed. Proc. of the 23rd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). Hong Kong: IEEE Press, 2004. 2469−2479.

[7] Du W, Deng J, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In: Li VOK, ed. Proc. of the 23rd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). Hong Kong: IEEE Press, 2004. 7−11.

[8] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Jajodia S, ed. Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS). Washington: ACM Press, 2003. 52−61.

[9] Liu D, Ning P. Location-Based pairwise key establishments for static sensor networks. In: Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. Fairfax: ACM Press, 2003. 72−82.

[10] Camtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. In: Molva R, ed. Proc. of the 9th European Symp. on Research in Computer Security. Sophia Antipolis: Springer-Verlag, 2004. 293−308.

[11] Zhou Y, Zhang Y, Fang Y. LLK: A link-layer key establishment scheme for wireless sensor networks. In: Pauly L, ed. Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC). New Orleans: IEEE Press, 2005. 1921−1926.

[12] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks. In: Jajodia S, ed. Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2002. 41−47.

[13] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. In: Jajodia S, ed. Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2003. 42−51.

[14] Younis O, Fahmy S. Heed: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. IEEE Trans. on Mobile Computing, 2004,3(4):366−379.

[15] Fonseca CM, Fleming PJ. Genetic algorithms for multiobjective optimization: Formulation, discussion and generalization. In: Forrest S, ed. Proc. of the 5th Int'l Conf. on Genetic Algorithms. San Francisco: Morgan Kaufmann Publishers, 1993. 416−423.

[16] Zitzler E, Thiele L. Multiobjective evolutionary algorithms: A comparative case study and the strength pareto approach. IEEE Trans. on Evolutionary Computation, 1999,3(4):257−271.

[17] Srinivas N, Deb K. Multi-Objective function optimization using non-dominated sorting genetic algorithms. Evolutionary Computation, 1995,2(3):221−248.

[18] Deb K, Pratap A, Agrawal S, Meyarivan T. A fast and elitist multi-objective genetic algorithm: NSGA-II. IEEE Trans. on Evolutionary Computation, 2002,6(2):182−197.

[19] Zhang H, Hou JC. Maintaining sensing coverage and connectivity in large sensor networks. Ad-hoc and Sensor Wireless Networks, 2005,1(1):89−124.

[20] Zou Y, Chakrabarty K. Sensor deployment and target localization based on virtual forces. In: Bauer F, ed. Proc. of the 22nd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). San Francisco: IEEE Press, 2003. 1293−1303.

贾杰(1980－),女,辽宁鞍山人,博士,主要研究领域为网络安全,无线自组织网络.

常桂然(1946－),男,博士,教授,博士生导师,主要研究领域为网络安全,无线通信,无线自组织网络.

陈剑(1980－),男,博士生,主要研究领域为无线通信,视频信号建模.

闻英友(1974－),男,博士,副教授,主要研究领域为下一代网络,网络安全,网络管理.