doi：10.11830/ISSN.1000-5013.201606018

# 网络入侵环境下健康节点选择方法设计与仿真

张军

（江苏海事职业技术学院 信息工程系，江苏 南京 211170）

**摘要：** 提出一种网络入侵环境下健康节点通信选择算法.针对节点特征建立模糊数学模型，对健康节点选择的成本进行约束，引入粒子群优化算法，结合不确定因素，对参数进行优化，实现健康节点的选择.实验结果表明：与传统的 BP 神经网络方法相比，改进的网络入侵环境下健康节点通信选择算法提高了健康节点选择的精度，缩短了运行时间，能将入侵后的误差控制在合理的范围内.

**关键词：** 网络入侵；健康节点；模糊约束；BP 神经网络；粒子群算法

**中图分类号：** TP 127 **文献标志码：** A **文章编号：** 1000-5013(2016)06-0754-04

# Health Design and Simulation of the Node Selection Method in Environment of Network Intrusion

ZHANG Jun

(Department of Information and Engineering, Jiangsu Maritime Institute, Nanjing 211170, China)

**Abstract:** Accurately selectting health node in network intrusion environment can guarantee the normal operation of the network. Fuzzy mathematics model is established based on the node characteristics to constraint the cost of the health node selection. Introducing the particle swarm optimization algorithm combining with the uncertainties to optimize the parameters, and to achieve healthy node selection. The experimental results show that compared with the traditional BP neural network method, the improved network intrusion environment health communication node selection algorithm improved the precision of node selection of health, shorten the operation time. After the invasion, the error can be controlled in a reasonable range.

**Keywords:** network invasion; health node; fuzzy constraints; BP neural networks; particle swarm algorithm

伴随网络技术发展而产生的网络安全问题越来越多，由此，相关网络安全防范技术应运而生.网络入侵后，对网络节点的选择是确保网络安全的基础[1-3].对网络入侵环境下健康节点进行准确选择，利用未被感染节点进行通信，可以保证遭受网络入侵时，整个网络仍有正常工作节点，在一定程度上保证网络的正常运行[4-5].对网络节点进行选择技术，成为相关领域专家学者研究的重点课题，受到越来越广泛的关注.一般采用主成分分析法[6]对网络入侵环境下节点可能感染区域中的布局进行划分和功能定位[7-8]，但是，此方法不能确保网络的安全.本文通过对网络入侵环境下健康节点选择问题进行分析，比较不同健康节点选择方法的优缺点，用模糊变量反应节点中的不确定性，引入粒子群算法来优化选择参数，建立网络入侵环境下健康节点选择模型，验证该方法的有效性和优越性.

**收稿日期：** 2016-10-13

**通信作者：** 张军(1973-)，男，副教授，主要从事网络安全技术、量子通信理论的研究. E-mail：njhxzhr@163.com.

**基金项目：** 江苏省现代教育技术重点研究课题(2015-R-42639)

## 1　节点选择特征模糊模型的设计

在网络受到入侵的环境下，未受攻击节点选择是一个非常复杂，且涉及到许多不同条件的过程，该过程通常面临一些不确定因素. 所以，要根据节点的固定特征，一层层地筛选，淘汰不合适的节点，逐步缩小选址的范围，直到最终选出最优的健康节点.

节点选择过程中，较大的难点是节点特征的描述，入侵过程具有较大的随机性. 利用模糊数学模型表示节点入侵后的特征，在一定约束条件下，描述节点的模糊性. 构建成本最小化的模糊线性规划模型，该模型表示为

$$f=\min\{\sum_{l\in L}f_l^dY_l^d+\sum_{i\in I}\sum_{j\in J}\sum_{k\in K}C_{k,l,i}^fg_kX_{i,j,k}^f+\sum_{i\in I}\sum_{j\in J}\sum_{k\in K}C_{i,j,k}^nd_kX_{i,j,k}^n+\sum_{k\in K}\sum_{l\in L}\sum_{m\in M}C_{k,l,i}^rg_kX_{i,j,k}^r+\sum_{k\in K}\sum_{l\in L}\sum_{m\in M}C_{k,l,m}^dg_kX_{k,l,m}^d\}. \tag{1}$$

式(1)中：$Y_l^d$ 为网络入侵环境下健康节点选择的决策变量；$X_{i,j,k}^f$ 为网络入侵环境下节点的总数；$X_{k,l,i}^r$ 为网络入侵环境下非健康节点的数量；$X_{k,l,m}^d$ 为网络入侵环境下需要维持网络正常运行的节点数量；$C_{k,l,i}^f$ 和 $C_{i,j,k}^n$ 分别代表网络入侵环境下节点选择的总费用和成本；$C_{k,l,i}^r$ 和 $C_{k,l,m}^d$ 分别代表网络入侵环境下未损坏健康节点的协方差矩阵；$g_k$ 表示网络入侵环境下的模糊约束变量.

求解模糊现行规划，在不确定信息因素下，将入侵网络设计成一个模糊机会约束模型，对该模型进行约束，即

$$S=\mathrm{pos}\{\sum_{l\in L}f_l^dY_l^d+\sum_{i\in I}\sum_{j\in J}\sum_{k\in K}C_{i,j,k}^nd_kX_{i,j,k}^f\}+\sum_{j\in J}\sum_{k\in K}d_kX_{i,j,k}^f+\sum_{l\in L}\sum_{i\in I}X_{k,l,i}^r+\sum_{k\in K}g_k\sum_{i\in I}X_{k,i,l}^r, \tag{2}$$

$$\mathrm{pos}\{\sum_{l\in L}f_l^dY_l^d+\sum_{i\in I}\sum_{j\in J}\sum_{k\in K}C_{i,j,k}^nd_kX_{i,j,k}^f\}\geqslant a_1, \tag{3}$$

$$\mathrm{pos}\{\sum_{k\in K}\sum_{l\in L}X_{k,l,i}^rg_k=\sum_{j\in J}\sum_{k\in K}d_kX_{i,j,k}^f\}\geqslant a_2, \tag{4}$$

$$\mathrm{pos}\{\sum_{l\in L}\sum_{i\in I}X_{k,l,i}^r\}\geqslant a_3, \tag{5}$$

$$\mathrm{pos}\{\sum_{k\in K}g_k\sum_{i\in I}X_{k,l,i}^r+\sum_{k\in K}g_k\sum_{m\in M}X_{k,l,m}^d\leqslant e_l^d\}\geqslant a_4. \tag{6}$$

式(2)～(6)中：$I,L,K$ 为可能发生网络入侵的总次数；$f$ 代表健康节点被选中的概率；$a_1,a_2,a_3,a_4$ 为健康节点选择的信任度；$C_{i,j,k}^n$ 为健康节点选择的排列数；$k$ 为受网络入侵影响的区域；$l$ 为网络入侵时节点的选择中心；$e_l^d$ 为中心中最大节点数量；$g_k$ 为网络入侵环境中网络入侵时节点选择中心节点之间的距离；$X$ 表示发生网络入侵的模糊概率；模型约束条件量 pos{ * }表示网络入侵事件发生的可能性.

## 2　基于粒子群算法的节点选择确认过程

在以上模型进行节点选择基础上，采用粒子群算法进行节点选择. 粒子群算法主要通过每个个体的配合与比较，实现复杂的空间区域内寻求最优解的过程. 为了方便分析研究，需要对节点样本进行归一化处理，分为正指标处理方法和负指标处理方法，具体过程描述为

正指标处理：

$$X_i^*=\frac{X_i-X_{\min}}{X_{\max}-X_{\min}}, \tag{7}$$

负指标处理：

$$X_i^*=\frac{X_{\max}-X_i}{X_{\max}-X_{\min}}. \tag{8}$$

式(7)～(8)中：$X_i$ 为样本中各个参数指标值；$X_i^*$ 为规范化处理后所得数据；$X_{\max}$ 为样本中同一指标数据的最大值；$X_{\min}$ 为样本中同一指标数据的最小值.

在进行节点样本预处理后，假设粒子群的种群为 $N$，在 $d$ 维空间下，粒子群可以表示为 $X_i=(X_{i,1},X_{i,2},\cdots,X_{i,d})$，速度可以用 $V_i=(V_{i,1},V_{i,2},\cdots,V_{i,d})$ 表示. 那么，粒子移动速度在 $t+1$ 时，可以表示为 $V_{i,d}$，即

$$V_{i,d}(t+1)=V_{i,d}(t)+c_1\phi_1[p_{i,d}(t)-x_{i,d}(t)]+c_2\phi_2[p_{e,d}(t)-x_{i,d}(t)]. \tag{9}$$

式(9)中：$c_1$ 和 $c_2$ 为常量，是粒子群的学习因子；$\phi_1$ 和 $\phi_2$ 是 0 到 1 之间的随机数；$p_{i,d}$ 是粒子当前的最佳

位置;$p_{e,d}$是种群最优的位置,即最优解.

为了提高粒子群算法的全局搜索和局部搜索能力,引入一个权重因子 $u$,$u\in(0,1)$.对粒子群参数进行优化,对式(9)进行转换,转换结果表示为

$$V_{i,d}(t+1)=uV_{i,d}(t)+c_1\phi_1[p_{i,d}(t)-x_{i,d}(t)]+c_2\phi_2[p_{e,d}(t)-x_{i,d}(t)]. \tag{10}$$

利用粒子群优化算法进行网络入侵环境下健康节点选择时,具体实现流程描述如下.

1) 对粒子进行初始化,设定每个粒子的初始位置 $c$,$\lambda$,$\varepsilon$,设定初始速度.2) 输入网络入侵环境下节点的样本训练集.3) 利用初始化后的粒子位置和速度,对网络入侵环境下节点的样本训练集进行SVM训练,并记录粒子的最优位置,全局的最优位置即为当中适应值的位置.4) 将式(11)作为粒子的适应度函数,计算每个粒子的适应度值,即

$$Q=\sqrt{\sum_{i=1}^{n}(S-S^*)^2/n}. \tag{11}$$

式(11)中:$S$代表样本$i$训练后的预测值;$S^*$是样本综合评估值;$n$是样本的数量;$Q$是适应值.5) 利用每个粒子的适应度值,对粒子的位置和速度进行更新.6) 更新位置和速度后,计算出每一次迭代的粒子的目标函数值,如果该函数值比之前的极值更好,则用该函数值取代之前的极值;否则,不作改变.7) 设置合适的参数,判断粒子群算法中局部粒子是否到达最优位置,直到达到最优位置时,停止迭代.此时,可以获取网络入侵环境下健康节点的最优选择参数,完成网络入侵环境下的健康节点选择.8) 最后,用SVM算法进行返回考察,算法结束,健康节点选择结束.

## 3 实例验证和分析

### 3.1 参数的选择和设置

为了验证文中方法进行网络入侵环境下健康节点选择的有效性,需要进行相关的仿真实验.实验环境为:Windows 7系统,2.20 GHz处理器,4 G内存,编程环境为VS 2010,最大迭代次数$G=50$,同时,采用MATLAB对数据进行辅助分析.

通过分析比较,预测结果误差表示为$K(x,x_i)=\exp(-\lambda|x-x_i|^2)$.

为了提高粒子群算法的准确率和计算效率,需要对参数进行合理的选择.种群规模$N$一般在10到20之间比较合适;学习因子$c_1$,$c_2$一般相等,设为2左右;权重$u$与搜索算法的能力有关,太大或太小都不利于搜索,因此,一般取值在0.9~1.2之间;粒子的最大速度与搜索的步长有关,合适的速度有利于搜索,寻找最优解,一般在0~1之间.

通过分析可以将种群规模$N$设为12,学习因子$c_1=c_2=1.9$,权重$u$设为1.0,粒子的最大速度设为0.4,最大的迭代次数设为100.通过MATLAB计算工具,得到经过粒子群算法优化后的训练结果为:惩罚参数$c=20.23$;适应度函数参数$\lambda=0.158$;损失函数的参数$\varepsilon=0.032\ 4$.

### 3.2 不同方法健康节点选择精度与误差的对比

与传统BP神经网络方法[9-10]进行对比,结果如表1所示.表1中:$\sigma$为节点选择精度,$\sigma=S^*/S$;$\eta$为对比的参数选择预测值和整体评估值的相对误差,即

$$\eta=|S-S^*|/S^*. \tag{12}$$

表1 实验结果对比

Tab.1 Experimental results contrast table

| 网络入侵类型 | 粒子群优化算法 | | 传统神经网络算法 | |
|---|---|---|---|---|
| | $\sigma$/% | $\eta$ | $\sigma$/% | $\eta$ |
| 口令入侵 | 96.3 | 1.61 | 73.4 | 3.22 |
| 特洛伊木马入侵 | 95.7 | 1.11 | 77.9 | 4.21 |
| 节点入侵 | 98.6 | 1.73 | 76.8 | 3.64 |
| 黑客入侵 | 97.4 | 1.26 | 74.7 | 4.26 |
| DOS入侵 | 95.9 | 1.28 | 79.5 | 4.32 |
| 伪远程入侵 | 96.8 | 1.37 | 78.6 | 4.78 |

由表 1 可知：在相同类型的网络入侵环境下，利用文中方法选择中节点的选择精度高于其他方法；同时，能将相对误差控制在合理的范围内，在不同类型的网络入侵环境下，其优势更加明显.

### 3.3　不同方法的网络运行时间对比

为进一步验证文中方法进行健康节点选择的性能，将不同方法下网络入侵后的运行时间进行对比，结果如表 2 所示. 表 2 中：$t$ 为总运行时间；$t_{ave}$ 为每个节点平均运行时间.

表 2　不同方法下网络运行时间比对

Tab. 2　Comparison on the network running time under different methods　　s

| 网络入侵类型 | BP 神经网络方法 | | 粒子群优化算法 | |
|---|---|---|---|---|
| | $t$ | $t_{ave}$ | $t$ | $t_{ave}$ |
| 口令入侵 | 2.19 | 0.028 | 13.89 | 0.197 |
| 特洛伊木马入侵 | 3.57 | 0.044 | 12.54 | 0.238 |
| 节点入侵 | 2.67 | 0.039 | 10.97 | 0.473 |
| 黑客入侵 | 1.66 | 0.041 | 14.37 | 0.567 |
| DOS 入侵 | 2.54 | 0.033 | 12.89 | 0.347 |
| 伪远程入侵 | 1.99 | 0.021 | 11.45 | 0.299 |

由表 2 可知：在相同类型的网络入侵环境下，利用文中方法的健康节点选择中节点的运行总时间远远高于传统方法. 在不同类型的网络入侵环境下，文中方法的优势更加明显，说明该方法的时效性较高，性能优越.

## 4　结束语

提出一种网络入侵环境下健康节点通信选择算法. 首先，建立针对健康节点选择的模糊数学模型，对健康节点选择的成本进行约束；在此基础上，引入粒子群优化算法，考虑多种不确定性因素，对参数进行了优化；最终，实现网络入侵环境下健康节点选择. 仿真实验对不同方法下健康节点的定位精度、相对误差、总耗时进行对比. 实验结果表明：与传统的 BP 神经网络方法相比，文中方法大大提高了健康节点选择的精度，缩短了运行时间，能将误差控制在合理的范围内，对完善网络入侵环境下健康节点的理论体系和实际运用具有一定的意义.

**参考文献：**


[1]　戴天虹，李昊. 基于改进 APIT 算法的无线传感器网络节点定位[J]. 传感器与微系统，2016，35(1)：135-138.

[2]　XU Kun，LIU Hongli，LIU Dawei，et al. Linear programming algorithms for sensor networks node localization[C]// IEEE International Conference on Consumer Electronics. Hangzhou：IEEE Press，2016：115-123.

[3]　SONG Yang，DONG Enqing，LIU Wei，et al. An iterative method of processing node flip ambiguity in wireless sensor networks node localization[C]// International Conference on Information Networking. Chengdu：IEEE Computer Society，2016：92-97.

[4]　王景珲. 一种基于 DV-Hop 的无线传感器网络节点定位算法[J]. 计算机工程，2015，41(1)：82-86.

[5]　CHO S Y. Measurement error observer-based IMM filtering for mobile node localization using WLAN RSSI measurement[J]. IEEE Sensors Journal，2016，16(8)：2489-2499.

[6]　郑学伟. 基于多维定标算法的 WSN 安全节点定位研究[J]. 电子设计工程，2015(15)：72-74.

[7]　鲁银芝，仲元昌，杨柳，等. 大规模带状无线传感器网络节点定位算法[J]. 传感器与微系统，2015，34(1)：138-141.

[8]　严丽，王启志. GA-Elman 网络的网络控制系统预测[J]. 华侨大学学报(自然科学版)，2014，35(6)：620-624.

[9]　胡明霞. 基于 BP 神经网络的入侵检测算法[J]. 计算机工程，2012，38(6)：148-150.

[10]　张敏. 一种基于灰度区间的 BP 神经网络算法研究[J]. 科技信息，2012(35)：97-99.


**(责任编辑：黄晓楠　　英文审校：吴逢铁)**