蚁群算法在网络路径可靠性研究中的应用

程世娟[1,2],卢 伟[3],陈 虬[1]
CHENG Shi-juan[1,2],LU Wei[3],CHEN Qiu[1]

1.西南交通大学 力学学院,成都 610031
2.西南交通大学 数学学院,成都 610031
3.西华大学 数学与计算机学院,成都 610039
1.School of Mechanics,Southwest Jiaotong University,Chengdu 610031,China
2.School of Mathematics,Southwest Jiaotong University,Chengdu 610031,China
3.College of Mathematics and Computer,Xihua University,Chengdu 610039,China
E-mail:csjj3202@163.com

CHENG Shi-juan,LU Wei,CHEN Qiu.Study on network route reliability based on ant colony algorithm.Computer Engineering and Applications,2009,45(14):119-121.

Abstract: Ant colony algorithm is used to solve the traditional network reliability optimization question in this paper.Satisfaction results are obtained in seeking the most short-path reliability.The simulation experiment data shows that the ant colony algorithm is an effective way to solve the network reliability questions.

Key words: ant colony algorithm;network;reliability;pheromone updating

摘 要:用蚁群算法来解决网络可靠性优化中遍历所有节点的最短路可靠度问题和最可靠路径问题的研究中,并给出网络可靠度下界的一个估计。用 MATLAB 语言编程进行算法的实现和仿真。结果表明,用蚁群算法解决网络的可靠性问题是可行并有效的。

关键词:蚁群算法;网络图;可靠度;信息素更新规则
DOI:10.3778/j.issn.1002-8331.2009.14.036 **文章编号**:1002-8331(2009)14-0119-03 **文献标识码**:A **中图分类号**:TP393

1 引言

网络是指把某些元件有目的、按一定形式连接起来完成特定任务的总体。网络可靠度是网络在规定的时间内、在规定的条件下完成规定任务的能力[1]。网络可靠性优化是 NP-Hard 问题。传统的可靠性优化方法当网络的结构过于复杂时往往显的无能为力,蚁群算法的提出为网络结构可靠性优化问题提供了一个强有力的分析工具。

用蚁群算法解决网络可靠度问题,用 MATLAB 语言编程进行算法的实现和仿真。

2 网络可靠度问题

网络可靠度问题一般是求两终端问题:

$R=P$(由节点 v_i 可以到达节点 v_j)

即节点 v_i 到节点 v_j 有路可通的概率 P。

网络是由边组成的,每一条边都有寿命,因而这些边的故障会引起系统的故障。所以问题更确切的提法是:给定网络的每条边在时刻 T(取定的常数)正常工作的概率,求在时刻 T 信息可以由节点 v_i 到达节点 v_j 概率,即求在时刻 T 系统正常的可靠度 $R(T)$。

由于

$S=$(由节点 v_i 可以到达节点 v_j)=

(由节点 v_i 至少有一条路通到节点 v_j)=

(以节点 v_i、v_j 为源和汇的所有割集都不失效)

因此求网络两点之间的最小路集或最小割集是求网络可靠度的关键。

2.1 路集法

路集法主要有直接法、全概率公式法、不交化法。

2.1.1 直接法

直接法是计算网络可靠度的最原始最直观的方法。直接法的基本思想是列举使系统正常这一事件 S 发生的所有可能的互斥事件,于是系统可靠度可以表示为这一系列不交事件的和的概率。在文献[2]中指出:一般来说,当网络的弧的数目大于 7 时,直接法显得太繁琐。

2.1.2 全概率公式法

设 $A_1,A_2,\cdots,A_n$ 为给定网络的最小路集,由全概率公式得系统可靠度:

$$R=P\left(\sum_{i=1}^{m}A_i\right)=\sum_{i=1}^{m}P(A_i)-\sum_{i<j=2}^{m}P(A_iA_j)+\cdots+(-1)^{m-1}P\left(\bigcap_{i=1}^{m}A_i\right)$$

基金项目:西南交通大学校基金(No.2002B)。

作者简介:程世娟(1973-),女,讲师,博士研究生,主要研究领域:计算智能;卢伟(1971-),男,讲师,主要研究领域:计算智能;陈虬,男,教授,博导,主要研究领域:计算智能。

收稿日期:2008-03-19 **修回日期**:2008-07-03

上式共进行了 2^m-1 求和运算,因此当 m 很大时计算量是很大的。从数值计算的角度来说,这不是求大型网络可靠度的有效方法。

2.1.3 不交化方法

1975 年阿卡瓦等提出一种快速计算网络可靠度的不交化方法,其基本思想:对上述相容事件 $A_1,A_2,\cdots,A_n$ 经过不交运算后得到它的不交集合为 $B_1,B_2,\cdots,B_r$,则网络系统的可靠度为

$$R=P\left(\bigcup_{i=1}^{m}A_i\right)=P\left(\sum_{j=1}^{r}B_j\right)=\sum_{j=1}^{r}P(B_j)$$

大多数网络系统的最小路集合间是相交的,因此求出网络的最小路集后,在进行可靠度计算时,首先要将相容事件转化为不相容事件。布尔代数不交化和拓扑不交化是将相容事件转化为不相容事件的常用方法。

2.2 最小割集法

在计算系统可靠度时,若路集较多,一般用最小割集来计算。故障树分析法就是最小割集分析。

假设 $K_1,K_2,\cdots,K_l$ 为网络的最小割集,则系统的可靠度

$R=P(\overline{K}_1\cap\overline{K}_2\cap\cdots\cap\overline{K}_l)$

用割集计算系统的失效概率时,交叉项的数值随阶的增加迅速下降。

与路径枚举法相反,割集分析法是以割断输入输出通路的最少单元来求解系统失效概率的分析方法。系统发生失效必须是系统内任意最小割集中的全部单元发生失效,否则这种割集就不是最小割集。

3 蚁群算法

3.1 蚁群算法的基本原理

20 世纪 90 年代初期,意大利学者 Dorigo Macro 等从生物进化论中受到启发,通过模拟自然界中蚂蚁群体寻优的行为而提出了蚁群优化算法[3](Ant Colony Optimization,ACO)。蚂蚁属群居昆虫,相互协作的一群蚂蚁很容易找到从蚁穴到食物的最短路径,而单个蚂蚁则不能。根据仿生学家的研究结果,蚂蚁凭借路径寻优的能力能够找到蚁巢与食物之间的最短路径,其原理在于蚂蚁在所经过的路径上留下一种称为信息素的挥发性分泌物,蚂蚁在觅食过程中能够感知这种物质的存在及其强度,并以此来指导自己的运动方向,倾向于朝着这种物质强度高的方向移动。信息素强度越高的路径,选择它的蚂蚁就越多,则在该路径上留下的信息素的强度就更大,而强度大的信息素又吸引更多的蚂蚁,从而形成一种正反馈。通过这种正反馈,蚂蚁最终可以发现最佳路径, 导致大部分的蚂蚁都会走此路径。蚁群算法就是受这种行为启发,以人工蚂蚁模拟真实蚂蚁行为来求解组合优化问题的方法。它是继模拟退火算法、遗传算法、禁忌搜索算法、人工神经网络算法等启发式搜索算法之后的一种新型的基于群体智能的启发式仿生类进化算法。

3.2 基本蚁群算法数学模型

基本蚁群算法最初是用来解决问题的。TSP 的简单形象描述是:给定 n 个城市,有一个旅行商从某一城市出发,访问各城市一次且仅有一次后再回到原出发城市,要求找出一条最短的巡回路径。基本蚁群算法数学模型如下:

设 $b_i(t)$ 表示 t 时刻位于城市 i 的蚂蚁数目,$\tau_{ij}(t)$ 为 t 时刻边 (i,j) 上的信息量,n 表示 TSP 问题的规模,m 为蚂蚁数目,初始时刻各条路径上信息量相等。

蚂蚁 $k(k=1,2,\cdots,m)$ 在运动过程中,根据各条路径上的信息量决定其转移方向。用禁忌表 $tabu_k(k=1,2,\cdots,m)$ 来记录蚂蚁 k 当前走过的城市,集合随着 $tabu_k$ 进化过程作动态调整。在搜索过程中,蚂蚁根据各条路径上的信息量及路径的启发信息来计算状态转移概率。$P_{ij}^{k}(t)$ 表示在 t 时刻蚂蚁 k 由城市 i 转移到城市 j 的状态转移概率。

$$p_{ij}(t)=\begin{cases}\dfrac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}}{\sum_{s\in allowed_k}[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}} & j\in allowed_k\\ 0 & \text{其他}\end{cases}\tag{1}$$

$allowed_k=\{C-tabu_k\}$ 表示蚂蚁 k 下一步允许选择的城市。

α 为信息启发式因子,表示轨迹的相对重要性,反映了蚂蚁在运动过程中所积累的信息在蚂蚁运动时起的作用,其值越大蚂蚁之间协作性越强;β 为期望启发式因子,反映了蚂蚁在运动过程中启发信息在蚂蚁选择路径中的受重视程度,d_{ij} 表示相邻两个城市之间的距离。

$t+n$ 时刻在路径 (i,j) 上的信息量可按如下规则进行调整:

$$\tau_{ij}(t+n)=(1-\rho)\cdot\tau_{ij}(t)+\Delta\tau_{ij}(t)\tag{2}$$

式中,ρ 表示信息挥发系数,$1-\rho$ 表示信息素残留系数。

4 基于蚁群算法的网络可靠度研究

4.1 技术处理

基本蚁群算法的搜索目标是各边长度之和最小的路径;而网络路径的可靠度是组成路径各边的可靠度的乘积,且可靠度最大为所求。因此要借助蚁群算法解决网络的可靠度问题,首先要解决将求边权积最大问题变为求某种形式的边权和最小问题。

首先,对数函数是单调函数,具有把乘积的对数转化为对数的和的性质,根据可靠度的有界性,利用负对数函数来进行转换,取 $\eta_{ij}=1/-\log a_{ij}$,其中 a_{ij} 表示边的可靠度。

其次,为了确保搜索收敛到最优解,若节点 v_i 与 v_j 没有边直接连接,视这两点之间存在一条虚边直接相连,且其可靠度为 0.01(不能为 0,否则对数函数无意义)。

4.2 求网络中遍历所有节点的最短路可靠度

增加一个虚节点和两条连接虚节点和网络输入节点与输出节点的虚边,在搜索过程中规定必须经过虚边,遍历所有节点的最短路径问题为最短回路问题。

实例仿真:求网络图 1 中节点 v_1 与 v_{10} 之间遍历所有节点的最短路径的可靠度。

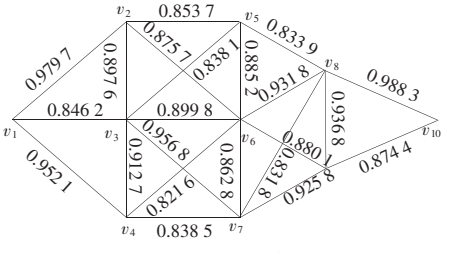

图 1　网络图

求解过程:产生一组[0.8,1]上的随机数作为给定网络各边的可靠度,通过增加虚边并按上述规则搜索,得到符合条件的最优路径:$v_1-v_2-v_5-v_3-v_4-v_7-v_6-v_8-v_9-v_{10}$,路径长度为 0.368 26。

由此得到,此网络中遍历所有节点的最短路可靠度为

$10^{-0.368\,26}=0.428\,3$。

4.3　求网络的最可靠路径

设网络的联络矩阵为 $\boldsymbol{A}$,其元素 a_{ij} 表示可靠度,若元素 $a_{ij}\neq 0$ 表示节点 v_i 与 v_j 有边直接相连接;若节点 v_i 与 v_j 间无边直接连接,令 $a_{ij}=0.01$。

用基本蚁群算法求解最可靠短路径问题步骤:

步骤 1　初始化。时间 $t=0$,循环次数 $N_c=0$,设置最大循环次数为 $NC_{\max}$,$\Delta\tau_{ij}(0)=0$。

步骤 2　将一定数目的蚂蚁置于起始输入节点,根据网络的联络矩阵 $\boldsymbol{A}$,选择满足 $a_{ij}>0.01$ 的 v_j 点作为 v_i 的下一个交叉点,对所有蚂蚁根据式(1)计算转移概率,根据公式(2)更新所选路径上的信息素。

步骤 3　重复步骤 2,直到所有蚂蚁都到达输出节点。

步骤 4　如果已经达到最大循环次数,循环结束,输出最短路径及其长度,否则返回步骤 2。

本文以 4.2 节中的实例为例,利用 Matlab 语言对蚁群算和改进的 Dijkstra 算法进行了仿真比较。取蚂蚁数 $m=3$,$NC_{\max}=150$ 蚁群算法在第 27 次循环时得到最优解,最优解率达到 80%,CPU 为 5.1 秒,若取蚂蚁数 $m=10$,则蚁群算法在第 2 次循环时就得到最优解,最优解几乎达到 100%。结果表明蚁群算法可以相对较快地找到可靠度最大的路径 v_1–v_2–v_5–v_8–v_{10},其可靠度为 0.738 8。

4.4　网络可靠度下界的一个估计

在很多情况下,无需知道或计算出网络的真实可靠度,只关心一个网络是否具备完成某项任务的能力,因此只需计算或了解网络的能力下限,即可靠度的下界。

在图 1 中,用基本蚁群算法搜索得到可靠度最大回路为 v_1–v_2–v_5–v_8–v_{10}–v_9–v_7–v_6–v_4–v_3–v_1。由此得到网络的两条不交最小路 A_1:v_1–v_2–v_5–v_8–v_{10},其可靠度 0.738 88;A_2:v_1–v_4–v_2–v_6–v_7–v_9–v_{10} 其可靠度 0.546 13。

设 $A_1,A_2,\cdots,A_n$ 为给定网络的最小路集,则:

$$P\left(\bigcup_{i=1}^{m}A_i\right)=\sum_{i=1}^{m}P(A_i)-\sum_{i<j}^{m}P(A_iA_j)+\cdots+(-1)^{m-1}P\left(\bigcap_{i=1}^{m}A_i\right)>$$

$$P(A_1\bigcup A_2)=P(A_1)+P(A_2)-P(A_1A_2)=$$

0.738 88+0.546 13–0.738 88×0.546 13=0.884 81

可以看作给定网络可靠度的一个下界。

5　结束语

上面讨论了蚁群算法在网络可靠性方面应用的可行性,并进行了实例仿真。蚁群算法是一种新生算法,具有很强的通用性和鲁棒性。许多研究已经证明,蚁群算法具有很强的发现较好解的能力,因为该算法不仅利用了正反馈原理,而且是一种本质并行的算法,蚁群算法凭借其优异的算法性能和算法特点很快成为启发式方法范畴内的一个独立分支,在有关国际会议上多次作为专题加以讨论。自 1998 年第一次国际蚁群算法国际会议召开后,蚁群算法更是成为智能仿生算法的研究热点,越来越多的研究人员正在从事这方面的工作。

参考文献:

[1] 曹晋华,程侃.可靠性数学引论[M].北京:科学出版社,1986.

[2] 王少萍.可靠性工程[M].北京:北京航空航天大学出版社,2000.

[3] Dorigo M,Cgmbardella L M.Ant colony system:A cooperative learning approach to the traveling salesman problem[J].IEEE Trans on Evolutionary Computation,1997,1(1):53–66.

[4] Colorm A,Dorigo M,Minieaao V.Distributed optimization by ant colonies[C]//Proc of the First European Conf on Artificial Life.Paris:France Elsevier Publishing,1991:134–142.

[5] 段海滨.蚁群算法原理及应用[M].北京:科学出版社,2005.

[6] 张曦煌,李彦中,李岩.基于加速寻径收敛的改进型蚁群算法[J].计算机工程与应用:2007,43(24):75–77.

[7] EFI1.1 Driver writers' guide[EB/OL].(2003).IntelCorporation.http://de–veloper.intel.com/technoledge/ef,i.

(上接 80 页)

在该协议中,U_i 首先对随机会话密钥 k_i'向 CA 进行承诺,虽然 CA 不能得到 k_i'的值,但是 U_i 也不能改动,然后 CA 用随机数 k_i''对 k_i'进行掩蔽,如果 U_i 改动了 k_i'的值,则 CA 可以在第(4)步中检测出来,从而认为 U_i 使用了阈下信道。

该协议是为了封闭签名中的会话密钥而设计的,Desmedt 认为该协议不能封闭失败中止式阈下信道[7],其构造如下:

设 b 为 U_i 所要发送的 1 比特阈下信息,在上述协议中的(1),(2),(4)步不变,第(3)步分为如下两步进行:

(3.1)U_i计算 $k_i=k_i'+k_i''$,使用 k_i 作为会话密钥进行签名;

(3.2)U_i 比较 r_i 的某一固定比特位是否等于阈下信息 b,如果相等则产生签名,否则终止协议。

如果嵌入成功,则 U_i 可以成功地完成阈下信息的发送,否则,签名失败,签名中心 CA 则认为 U_i 使用了阈下信道。因此,这是一种有风险的信道,而且该信道容量极小,几乎没有任何实用性,在实际应用中不予以考虑。因此,可以认为上述封闭方法可以有效地封闭实际应用中可能存在的阈下信道。

5　结论

分析了基于椭圆曲线的有序多重签名中阈下信道存在性得出,在该签名中宽带信道会被封闭,而窄带信道则可能存在于相邻的两个签名者之间,提出了一种基于承诺掩蔽的阈下信道封闭方案,并对该方案进行了具体分析。分析结果证明,提出的阈下信道封闭方案可有效地封闭实际应用中可能存在的阈下信道。

参考文献:

[1] 赖溪松.计算机密码学及其应用[M].北京:国防工业出版社,2001.

[2] 杜海涛,张青坡,钮心忻,等.一个新的离散对数有序多重签名方案[J].计算机工程与应用,2007,43(2):148–150.

[3] 祁明,隆益民,卓光辉.封闭阈下信道的若干新型签名方案[J].计算机工程与应用,2000,36(6):22–24.

[4] 裴士辉,桑兰芬,崔维力.椭圆曲线数字签名算法的阈下信道[J].吉林大学学报:信息科学版,2003,21(3):290–292.

[5] 赵元志,廖晓峰.椭圆曲线数字签名算法的阈下信道[J].计算机工程与应用,2005,41(21):92–93.

[6] 严安,杨明福.基于椭圆曲线的有序多重数字签名方案[J].计算机应用与软件,2007,24(2):164–165.

[7] Desmedt Y.Simmons' protocol is not free of subliminal channels[C]//The 9th IEEE Computer Security Foundations Workshop,1996:170–175.