基于当前最优解的分段搜索策略的人工蜂群算法

毛 力 周长喜 吴 滨

(江南大学物联网工程学院 无锡 214122) (轻工过程先进控制教育部重点实验室 无锡 214122)

摘 要 为了克服人工蜂群算法在求解函数优化问题中所存在的局部搜索能力差、收敛精度低的缺点,提出了一种基于当前最优解的分段搜索策略的人工蜂群算法。该算法中跟随蜂利用由全局当前最优解和个体当前最优解引导的局部搜索策略逐维进行变异,并采用基于"分段思想"的局部搜索策略对蜜源进行贪婪更新,以提高蜜源的更新效率,从而提高了人工蜂群算法的局部搜索能力。6个标准测试函数的仿真实验结果表明,与基本人工蜂群算法相比,改进后的人工蜂群算法在寻优精度和收敛速度上均有明显提高。

关键词 人工蜂群算法,当前最优解,分段搜索,局部搜索

中图法分类号 TP18 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.12.056

Artificial Bee Colony Algorithm Based on Strategy of Segmental-search with Current Optimal Solution

MAO Li ZHOU Chang-xi WU Bin

(School of Internet of Things, Jiangnan University, Wuxi 214122, China)

(Key Laboratory of Advanced Process Control for Light Industry (Ministry of Education), Jiangnan University, Wuxi 214122, China)

Abstract An artificial bee colony (ABC) algorithm based on the strategy of segmental-search with current optimal solution was proposed in this paper, in order to overcome the drawbacks of poor local searching capability and slow convergence of conventional ABC algorithm. In this algorithm, onlooker bees utilize the local search strategy guided by the global current optimal solution and individual current optimal solution to mutate dimension, and the local search strategy based on the strategy of segmental-search is used to improve the updating rate of food sources, which enhances the local search capability of the algorithm. The simulation results of six standard functions show that the modified ABC algorithm can attain significant improvement on solution accuracy and convergence rate compared with the basic ABC algorithm.

Keywords Artificial bee colony (ABC), Current optimal solution, Segmental-search, Local search

1 引言

人工蜂群(Artificial Bee Colony, ABC)算法[1]是2005年由土耳其学者Karaboga提出的一种新的群体智能算法。文献[2]表明ABC算法因其原理简单、控制参数少、灵活性强及适应性高等特点,越来越多地被各界学者所关注,并在求解函数优化问题中显示出强大的生命力。但ABC算法和其他群智能算法一样,在求解函数优化问题时也存在早熟收敛、局部搜索能力差、收敛精度低等问题[3-6]。针对ABC算法局部搜索能力差等缺陷,许多学者纷纷提出改进方案。王冰[7]提出在跟随蜂阶段采用一种基于当前局部最优解的搜索策略,并采用基于一般的反向学习的策略进行种群初始化;Zhu等人[8]提出利用全局最优解改进ABC算法的搜索策略来提高其局部搜索能力;Banharnsakun等人[9]提出利用当前全局最优解代替随机选取的邻域个体并根据当前全局最优解的适应度调整邻域搜索步长的跟随蜂局部搜索策略;葛宇等人[10]提出了基于极值优化策略的高效率的寻优机制来重新设计ABC算法中跟随蜂的局部搜索方案。这些改进方案在一定程度上增强了ABC算法的局部搜索能力,对提高算法性能和扩大其适用范围具有重要研究意义。

为进一步改进ABC算法在求解函数优化问题中的局部搜索能力,提高算法的精度,本文提出一种基于当前最优解的分段搜索策略的人工蜂群算法(FABC)。该算法利用全局当前最优解和个体当前最优解来改进跟随蜂的局部搜索策略,并在此基础上进一步采用"分段思想"优化蜜源的更新方式,从而有效提高了人工蜂群算法的局部搜索能力,使算法的收敛精度和收敛速度得到一定程度的改善和提高。

2 人工蜂群算法

ABC算法是模仿蜜蜂的行为而提出的一种智能优化算法。蜂群包括雇佣蜂、跟随蜂及侦查蜂3类。蜜蜂寻找食物源的过程被抽象成寻找优化问题最优解的过程[11-13]。

到稿日期:2014-12-07 返修日期:2015-03-26 本文受轻工过程先进控制教育部重点实验室(江南大学)开放课题项目(APCLI1004),国家青年科学基金项目(F030204),现代农业产业技术体系专项资金(CARS-49)资助。

毛 力(1967-),男,副教授,硕士生导师,主要研究领域为人工智能、数据挖掘,E-mail:changxi0309@163.com;周长喜(1989-),男,硕士生,主要研究领域为人工智能;吴 滨(1970-),男,讲师,主要研究领域为工业自动化。

首先，ABC 算法在 D 维的解空间中随机产生 SN 个初始解(食物源) $X_i=(x_{i1},x_{i2},\cdots,x_{iD})$。雇佣蜂随机选择蜜源的任意一维分量按式(1)进行变异，搜索新蜜源。

$$v_{ij}=x_{ij}+R(x_{ij}-x_{kj}) \tag{1}$$

式中，v_{ij} 为新蜜源的位置；$k\in\{1,2,\cdots,SN\}$，$j\in\{1,2,\cdots,D\}$，k 和 j 都是随机选取的，且 $k\neq i$；R 为[-1,1]间的随机数，用来控制邻域范围。

雇佣蜂遵循贪婪选择策略对新的蜜源进行筛选，若其适应度值优于旧蜜源，则放弃旧蜜源选择新蜜源；反之，保持原来位置不变。雇佣蜂完成搜索过程之后将蜜源信息传递给跟随蜂，跟随蜂按照轮盘赌的方式选择蜜源，并按式(2)计算蜜源被选择的概率 P_i。

$$P_i=fit_i/\sum_{j=1}^{SN}fit_j \tag{2}$$

其中，fit_i 是蜜源 X_i 对应的适应度。

如果雇佣蜂在经过 limit(用来判断个体是否陷入停滞的阈值)次迭代搜索后仍没有提高解的质量，那么雇佣蜂变为侦查蜂，且由侦查蜂依据式(3)随机地产生一个新解来替代原来的解。

$$x_{ij}=x_{\min,j}+\mathrm{rand}(0,1)(x_{\max,j}-x_{\min,j}) \tag{3}$$

其中，$x_{\max,j}$ 和 $x_{\min,j}$ 为解空间 x_{ij} 的上下界。

3 改进人工蜂群算法

在 ABC 算法寻优过程中，雇佣蜂和侦查蜂负责全局搜索，该算法全局搜索能力较强；而跟随蜂主要在优质蜜源附近作局部搜索，促使优秀个体逐步向最优位置演化，并且跟随蜂的搜索模式与算法的收敛精度和速度密切相关。本文就跟随蜂局部搜索策略中存在的不足进行讨论，并提出改进方案。

3.1 基于当前最优解的跟随蜂局部搜索策略

基本 ABC 算法中跟随蜂采用与雇佣蜂相同的搜索策略，因此跟随蜂也具有很强的全局探索能力，而局部搜索能力相对较弱。为了提高 ABC 算法的局部搜索能力，改进算法中的跟随蜂基于雇佣蜂全局当前最优解和个体当前最优解进行局部寻优，且在每次迭代中逐维更新蜜源每一维度的值，以增加该可行解在搜索空间中的多样性。其中，全局当前最优解是跟随蜂根据雇佣蜂所传来的蜜源信息来选择的当前全局最优蜜源 X_g，个体当前最优解为每个雇佣蜂自己到目前为止搜索到的最优蜜源 X_b。因此本文在受粒子群优化算法的启发的基础上提出了基于最优解引导的跟随蜂局部搜索策略，如式(4)所示：

$$x'_{ij}=x_{ij}+R\times\varphi(x_{bj}-x_{kj})+R\times\varphi(x_{gj}-x_{ij}) \tag{4}$$

其中，x'_{ij} 表示新产生的第 j 维分量，其对应的新个体记为 X'_i；R 为[-1,1]间的随机数，j,k 均随机选择，且 $k\neq b$，x_{bj} 表示个体当前最优解 X_b 的第 j 维分量；x_{kj} 为个体 X_k 的第 j 维分量；x_{gj} 表示全局当前最优解 X_g 的第 j 维分量，且 $g\neq i$。

$$\varphi=\mathrm{e}^{-iter/MCN} \tag{5}$$

其中，φ 为收缩因子，$iter$ 是当前迭代次数，MCN 是最大迭代次数。

与基本 ABC 算法中的搜索策略不同，本文所采用的是跟随蜂在当前最优解的引导下在自身周围进行局部搜索的策略。φ 的值可以适时调节步长，有助于跟随蜂寻找新的蜜源，提高寻优性能。在迭代初期，由于 φ 的值较大，有效地扩大了领域的搜索范围，提高了算法的局部搜索能力；而随着迭代次数的增加，φ 的值逐渐变小，有效地缩小了领域的搜索范围，将有助于算法进行深度寻优并快速寻找到最优解。

3.2 基于“分段思想”的跟随蜂局部搜索策略

在基本 ABC 算法中跟随蜂的搜索策略是在优质蜜源附近随机地选择一维分量经过变异来进行局部搜索，而跟随蜂变异后的新蜜源的适应度值也是不确定的，如果新蜜源比原来蜜源优秀则更新，否则不更新，从而降低了产生更优蜜源的概率，使蜜源不被更新的可能性变大，增加了无效搜索次数，进而致使其局部搜索效率下降。为此，改进算法中的跟随蜂采用基于“分段思想”的局部搜索策略对蜜源进行贪婪更新，其具体思路如图 1 所示：跟随蜂 X_i 在搜索空间中的某一维度按式(4)进行搜索，如果搜索到蜜源 X_1，则将 OX_1 用 K(例如 $K=3$)个点划分为若干个相等的区段，计算蜜源 X_2、X_3、X_4 对应的适应度值，从中选择适应度值最好的蜜源 X_4 与原蜜源 X_i 进行贪婪更新；若搜索到的蜜源是 X_5，则将 OX_5 用 K 个点划分为若干个相等的区段，计算蜜源 X_6、X_7、X_8 对应的适应度值，从中选择适应度值最好的蜜源 X_8 与原蜜源 X_i 进行贪婪更新。由于蜜源 X_4 或 X_8 是这 K 个蜜源中适应度值最好的，因此大大增加了蜜源 X_i 被更新的概率，从而有效提高了跟随蜂的局部搜索效率，使算法的性能得到明显改善。

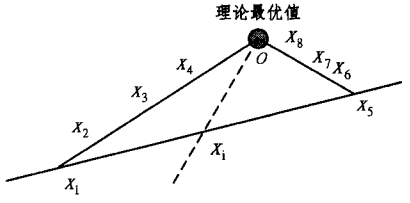

图 1 基于“分段思想”的搜索示意图

3.3 基于当前最优解的分段搜索策略的 ABC 算法流程

对于最小值优化问题 Min($f(X)$)，改进的 ABC 算法的具体实现步骤如下。

步骤 1 初始化算法参数，随机产生 SN 个解，每个解 $X_i=(x_{i1},x_{i2},\cdots,x_{iD})$ 是一个 D 维向量，最大迭代次数为 MCN、分段点个数为 K、阈值参数为 limit。

步骤 2 对种群中每个雇佣蜂 X_i 在 D 维度空间中利用式(1)逐维进行搜索，若新个体比原来个体优秀则更新，否则保留 X_i。

步骤 3 选择雇佣蜂变异后的全局当前最优解 X_g 和个体当前最优解 X_b，以供基于当前最优解引导的跟随蜂局部搜索策略式(4)使用，并由式(2)计算每个食物源被选择的概率。

步骤 4 跟随蜂根据轮盘赌的方式选择部分适应度较好的蜜源，然后每个跟随蜂在 D 维度空间中利用式(4)逐维进行变异，并采用基于“分段思想”的局部搜索策略对蜜源进行贪婪更新。

步骤 5 当蜜源连续 limit 次迭代都未得到更新，则由侦查蜂按照式(3)随机产生一个新蜜源进行替换。

步骤 6 记录到目前为止的最优解。

步骤 7 判断是否达到最大迭代次数 MCN，若满足，则输出最优解，否则转到步骤 2。

3.4 时间复杂度分析

ABC 算法的时间复杂度[14]为 $O(MCN\times SN)$，文献[7]中的 Best-so-far ABC 算法的时间复杂度也为 $O(MCN\times SN)$；本文提出的方案对跟随蜂的局部搜索策略进行了改进，ABC 算法中的跟随蜂只是随机地选择任意一维分量进行变

异，而 FABC 算法中的跟随蜂则是利用基于全局最优解和个体最优解引导的跟随蜂局部搜索策略进行变异，故其时间复杂度增加了 $O(MCN\times SN\times(D-1))$；并采用基于“分段思想”的局部搜索策略进行贪婪更新，其时间复杂度取决于分段点个数 K，其时间复杂度又增加了 $O(MCN\times SN\times D\times K)$，所以 FABC 算法的时间复杂度为 $O(MCN\times SN\times D\times(K+1))$，其中 D 为个体的维数，分段点个数 K 为常数，例如图 1 中 $K=3$，故经过约减后 FABC 算法的时间复杂度也为 $O(MCN\times SN)$，即这 3 种算法的时间复杂度相同。

4 仿真实验及分析

为评估 FABC 算法的性能，本文使用 6 个典型的测试函数[15]对 FABC 算法、ABC 算法以及文献[9]中改进的 ABC (Best-so-far ABC)算法的稳定性、寻优精度和收敛速度进行对比实验。

4.1 测试函数选择

表 1 列出了 6 个测试函数的搜索范围和理论最优值。其中函数 f_1 和 f_2 是单模态函数，在定义域内只有一个极值点，主要用来测试算法的寻优精度和收敛速度；f_3 至 f_5 是非线性多模态函数，存在多个局部极值点，用来测试算法的全局寻优性能和避免早熟的能力；函数 f_6 被称作变态函数，该函数的变量之间具有很强的关联性，并且理论最优值位于一个弯曲的、平滑路径上的谷底，由于该函数较特殊，通常用来评价优化算法的性能。

表 1 测试函数的搜索范围和理论最优值

函数	搜索范围	理论最优值
f_1	[−50,50]	0
f_2	[−100,100]	0
f_3	[−5.12,5.12]	0
f_4	[−32,32]	0
f_5	[−600,600]	0
f_6	[−30,30]	0

Sphere 函数：

$$f_1(x)=\sum_{i=1}^{n}x_i^2$$

Step 函数：

$$f_2(x)=\sum_{i=1}^{n}(\lfloor x_i+0.5\rfloor)^2$$

Rastrigin 函数：

$$f_3(x)=\sum_{i=1}^{n}[x_i^2-10\cos(2\pi x_i)+10]$$

Ackley 函数：

$$f_4(x)=-20\exp(-0.2\sqrt{\frac{1}{n}\sum_{i=1}^{n}x_i^2})-\exp(\frac{1}{n}\sum_{i=1}^{n}\cos(2\pi x_i))+20+e$$

Griewank 函数：

$$f_5(x)=\frac{1}{4000}\sum_{i=1}^{n}(x_i)^2-\prod_{i=1}^{n}\cos(\frac{x_i}{\sqrt{i}})+1$$

Rosenbrock 函数：

$$f_6(x)=\sum_{i=1}^{n-1}[100(x_{i+1}-x_i^2)^2+(x_i-1)^2]$$

4.2 实验结果与分析

FABC、ABC 和 Best-so-far ABC 3 种算法在对比实验中的参数设置如下：种群规模 $SN=50$，分段点个数 $K=2$，判断是否陷入停滞的阈值参数 limit=10，维度 $D=30$，最大循环次数 $MCN=1000$。

为了测试算法的性能，分别使用以上 3 种算法对每个测试函数在 30 维的条件下进行 30 次独立实验，得出其对应的最优值、最差值、平均值、标准差和平均时耗，测试结果如表 2 所列。其中，平均时耗是指 3 种算法各自独立运行 30 次达到收敛稳定精度所需要时间的平均值；同时，图 2－图 7 分别给出了 3 种算法各自独立运行 30 次的平均适应度值进化曲线。

表 2 30 维函数测试结果的比较

函数	算法	最优值	最差值	均值	方差	平均时耗/s
Sphere	ABC	1.6700E−05	6.9189E−04	1.6405E−04	1.3229E−04E−06	1.3415
	Best-so-far ABC	1.3323E−14	2.0214E−11	2.9886E−12	5.7394E−12	1.0514
	FABC	5.9609E−17	3.3292E−16	2.6260E−16	9.4501E−17	0.4287
Step	ABC	0	0	0	0	1.1650
	Best-so-far ABC	0	0	0	0	0.4310
	FABC	0	0	0	0	0.1126
Rastrigin	ABC	0.8516	8.9060	5.7034	1.8371	1.4794
	Best-so-far ABC	1.7053E−13	4.0388E−09	3.6781E−10	7.9573E−10	1.4275
	FABC	0	0	0	0	0.5885
Ackley	ABC	0.0328	0.7183	0.1992	0.1212	2.0381
	Best-so-far ABC	2.3084E−07	1.2750E−04	2.5382E−05	3.5412E−05	2.2851
	FABC	7.9936E−15	1.5099E−14	1.2731E−14	3.1409E−15	1.1772
Griewank	ABC	3.1814E−04	0.0355	0.0124	0.0102	1.4447
	Best-so-far ABC	0	3.3204E−11	4.6000E−12	8.9976E−12	1.5191
	FABC	0	1.1102E−16	1.0362E−16	2.8167E−17	0.5112
Rosenbrock	ABC	16.5106	139.3078	67.7364	25.9937	1.3594
	Best-so-far ABC	2.9588E−04	28.3553	12.1822	14.1306	1.4398
	FABC	4.2461E−07	0.0342	0.0040	0.0073	1.2702

表 2 中的数据表明：ABC 算法的稳定性较差、收敛速度慢且收敛精度不高；Best-so-far ABC 算法利用当前最优解及其对应的适应度值改进跟随蜂的邻域搜索方式，从而增强了该算法的局部搜索能力，也在一定程度上提高了算法的求解质量；FABC 算法中跟随蜂在雇佣蜂逐维变异后的当前最优解的基础上进一步进行局部寻优，并把“分段思想”引入跟随蜂的局部搜索策略中，显著提高了算法的局部搜索能力，进而使算法的性能得到明显提高。

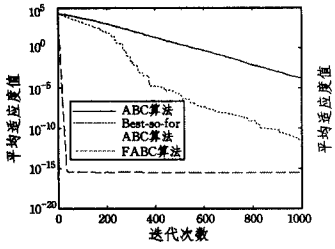

图 2 Sphere 函数进化曲线

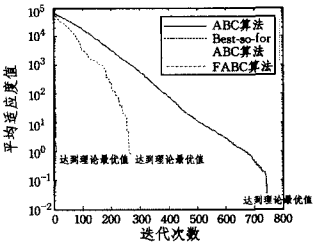

图 3 Step 函数进化曲线

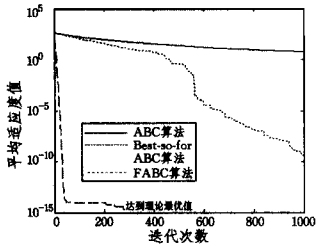

图 4 Rastrigin 函数进化曲线

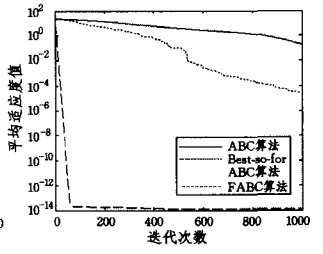

图 5 Ackley 函数进化曲线

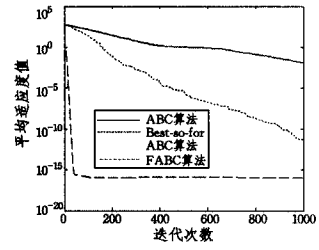

图 6 Griewank 函数进化曲线

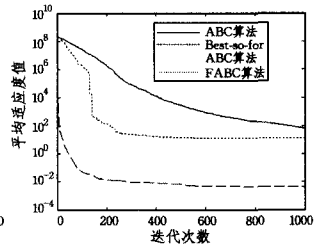

图 7 Rosenbrock 函数进化曲线

从表 2 中的数据分析可知，FABC 算法的最优值和最差值的精度与 ABC 算法和 Best-so-far ABC 算法相比，明显得到了提高，并且 FABC 算法对各测试函数均具有较高的寻优精度。虽然针对函数 f_2 3 种算法都达到了理论最优值，但由图 3 可知，FABC 算法所需要的迭代次数远小于其它两种算法；对除函数 f_2 以外的所有测试函数，FABC 算法的均值和方差与另外两种算法相比，均出现了数量级级别的提升，这说明 FABC 算法的收敛精度和稳定性较高，具有较好的鲁棒性。

另外，从表 2 中可知，FABC 算法的平均时耗小于 ABC 算法和 Best-so-far ABC 算法，虽然 FABC 算法在每次迭代过程中都在跟随蜂搜索阶段利用基于当前最优解的局部搜索策略逐维进行变异，并采用“分段思想”的蜜源更新方式增加了计算量，从而增加了每次迭代的运行时间，但是从图 2—图 7 可以看出，FABC 算法达到稳定收敛精度所需要的迭代次数远少于 ABC 算法和 Best-so-far ABC 算法，并且在进化中 FABC 算法始终保持向最优解进化的趋势，特别是对于函数 f_2 能在几次迭代内就收敛到理论最优值以及对函数 f_3 能在 300 次迭代内收敛到理论最优值。故 FABC 算法比另外两种算法具有更快的收敛速度。

上述实验结果表明，与 ABC 算法和 Best-so-far ABC 算法相比，FABC 算法具有更高的收敛精度和更快的收敛速度。FABC 算法中基于当前最优解的跟随蜂局部搜索策略及基于“分段思想”的蜜源更新方式的引入明显增强了算法的局部搜索能力，从而使算法的寻优精度和收敛速度得到了明显改善和提高。

结束语 本文针对基本 ABC 算法中跟随蜂局部搜索能力较差的问题，提出了具体的改进方案。改进方案中跟随蜂在雇佣蜂逐维变异后的全局当前最优解和个体当前最优解的引导下进行局部搜索，并采用基于“分段思想”的搜索方式更新蜜源，以提高蜜源更新的成功率。仿真实验结果表明，在求解函数最小值优化问题时，本文给出的改进基本 ABC 算法不仅具有较强的鲁棒性，而且还能有效避免算法陷入局部最优，使其具有更高的寻优精度和更快的收敛速度。

参 考 文 献

[1] Karaboga D. An idea based on honey bee swarm for numerical optimization[R]. Technical Report-TR06. Kayseri: Erciyes University, Engineering Faculty, Computer Engineering Department, 2005

[2] Karaboga D, Akay B. A comparative study of artificial bee colony algorithm[J]. Applied Mathematics and Computing, 2009, 214(1): 108-132

[3] Gao Wei-feng, Liu San-yang. A modified artificial bee colony algorithm [J]. Computers & Operations Research, 2012, 39(3): 687-697

[4] 王志刚，夏慧明. 求解车辆路径问题的人工蜂群算法[J]. 计算机工程与科学，2014，36(6)：1088-1094
Wang Zhi-gang, Xia Hui-ming. An artificial bee colony algorithm for the vehicle routing problem[J]. Computer Engineering & Science, 2014, 36(6): 1088-1094

[5] Gao Wei-feng, Liu San-yang, Huang Ling-ling. A novel artificial bee colony algorithm based on modified search equation and orthogonal learning [J]. IEEE Trans Cybern, 2013, 43(3): 1011-1024

[6] Li Guo-qiang, Niu Pei-feng, Xiao Xing-jun. Development and investigation of efficient artificial bee colony algorithm for numerical function optimization [J]. Applied Soft Computing, 2012, 12(1): 320-332

[7] 王冰. 基于局部最优解的改进人工蜂群算法[J]. 计算机应用研究，2014，31(4)：1023-1026
Wang Bing. Improved artificial bee colony algorithm based on best solution[J]. Application Research of Computer, 2014, 31(4): 1023-1026

[8] Zhu Guo-pu, Kwong Sam. Gbest-guided artificial bee colony algorithm for numerical function optimization[J]. Applied Mathematics and Computation, 2010, 217: 3166-3173

[9] Banharnsakun A, Achalakul T, Sirinaovakul B. The best-so-far selection in artificial bee colony algroithm [J]. Applied Soft Computing, 2011, 11(2): 2888-2901

[10] 葛宇，梁静，王学平. 基于极值优化策略的改进的人工蜂群算法[J]. 计算机科学，2013，40(6)：247-251
Ge Yu, Liang Jing, Wang Xue-ping. Improved artificial bee colony algorithms based on extremal optimization strategy[J]. Computer Science, 2013, 40(6): 247-251

[11] Karaboga D, Basturk B. On the performance of artificial bee colony algorithm[J]. Applied Soft Computing, 2008, 8 (1): 687-697

[12] 张超群，郑建国，王翔. 蜂群算法研究综述[J]. 计算机应用研究，

2011,28(9):3201-3205
Zhang Chao-qun, Zheng Jian-guo, Wang Xiang. Application Overview of research on bee colony algorithms[J]. Research of Computers,2011,28(9):3201-3205
[13] Gao Wei-feng, Liu San-yang. Improved artificial bee colony algorithm for global optimization[J]. Information Processing Letters,2011,111(17):871-882
[14] 王翔,李志勇,许国艺,等. 基于混沌局部搜索算子的人工蜂群算法[J]. 计算机应用,2012,32(4):1033-1036,1040
Wang Xiang, LI Zhi-yong, Xu Guo-yi, et al. Artificial bee colony algorithm based on chaos search operator [J]. Journal of Computer Applications,2012,32(4):1033-1036,1040
[15] Karaboga D, Basturk B. A powerful and efficient algorithm for numerical function optimization: Artificial Bee Colony (ABC) algorithm [J]. Journal of Global Optimization,2007,39(3):459-471

(上接第 232 页)

结束语 开展深空探测对于人类文明具有重大的意义,由深空节点、中继节点、地面用户和控制中心等构成的深空网络是开展深空探测的重要形式。深空通信与近地通信的不同之处于在于巨大的信号衰减、通信时延和能量损耗,因此传统的即时通信不能适用于深空通信,需要为其研究全新的通信形式,这其中包括安全通信的机制。

本文提出了一个高效的适用于深空网络的安全通信机制,该机制中深空节点采用基于属性的加密算法加密数据,用户持有与其授权属性集相对应的访问树。深空节点加密数据时为密文选择一组加密属性,用户能够解密数据当且仅当密文的属性能够满足用户的访问树。这是一种不需要进行用户认证的、高效的安全通信机制,深空节点还可以为密文选择不同的属性以满足不同的安全性需求,能够灵活更改或限制用户解密能力。进一步的研究工作可以选择更高效的属性加密方案以满足更高的要求。

参 考 文 献

[1] 欧阳自远,李春来,邹永廖,等. 深空探测的进展与我国深空探测的发展战略[J]. 中国航天,2002(12):28-32
Ouyang Z Y, Li C L, Zou Y L, et al. Advances in deep space exploration and the development strategy of China's deep space exploration [J]. Aerospace China,2002(12):28-32
[2] 姜昌,黄宇民,胡勇. 研究与开发天基深空通信跟踪(C&T)网的倡议[J]. 飞行器测控学报,1999,18(4):28-37
Jiang C, Huang Y M, Hu Y. An initiative of research and development of space-based communications and tracking(C&T) network [J]. Journal of Spacecraft TT&C Technology, 1999, 18(4):28-37
[3] Hooke A. The interplanetary internet [J]. Communication of the ACM,2001,44(9):38-40
[4] Akyildiz I F, Akan Ö B, Chen C, et al. Interplanetary internet: state-of-the-art and research challenges [J]. Computer Networks,2003,43(2):75-112
[5] Bhasin K, Hayden J L. Space Internet architecture and technologies for NASA enterprises [J]. International Journal of Satellite Communications,2002,20(5):311-332
[6] Mukherjee J, Ramamurthy B. Communication technologies and architectures for space network and interplanetary internet [J]. IEEE Communications Surveys & Tutorials,2013,15(2):881-897
[7] Sodnik Z, Furch B, Lutz H. Optical intersatellite communication [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2010,16(5):1051-1057
[8] Marchese M. Interplanetary and pervasive communications [J]. IEEE Aerospace and Electronic Systems Magazine,2011,26(2):12-18
[9] 林闯,董扬威,单志广. 基于 DTN 的空间网络互联服务研究综述[J]. 计算机研究与发展,2014,51(5):931-943
Lin C, Dong Y W, Shan Z G. Research on space internetworking service based on DTN [J]. Journal of Computer Research and Development,2014,51(5):931-943
[10] Wenbo M. Modern cryptography: theory and practice [M]. Prentice Hall PTR,2004
[11] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-Crypto'84. Berlin: Springer-Verlag,1984:47-53
[12] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C] // Advances in Cryptology-Crypto 2001. Berlin: Springer-Verlag,2001:213-229
[13] 郝云芳,吴静,王立炜. Boneh-Boyen_1 基于身份加密体制的安全密钥分发[J]. 计算机科学,2012,39(Z6):35-37
Hao Y F, Wu J, Wang L W. Secure key issuing for Boneh-Boyen$_1$ identity-based encryption [J]. Computer Science, 2012, 39(Z6):35-37
[14] Sahai A, Waters B. Fuzzy identity based encryption[C]// Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer-Verlag,2005:457-473
[15] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C] // ACM conference on Computer and Communications Security. Alexandria, USA: ACM Press,2006:89-98
[16] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// Proceedings of IEEE Symposium on Security and Privacy. Oakland, USA: IEEE Computer Society, 2007:321-334
[17] Lewko A, Waters B. Decentralizing attributed-based encryption [C] // Advances in Cryptology-EUROCRYPT 2011. Berlin: Springer-Verlag,2011:568-588
[18] Zhang Guo-yan, Liu Lei, Liu Yang. An attribute-based encryption scheme secure against malicious KGC[C]// IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK: IEEE Computer Society,2012:1376-1380
[19] 陈燕俐,杜英杰,杨庚. 一种高效的基于属性的认证密钥协商协议[J]. 计算机科学,2014,41(4):150-154,177
Chen Y L, Du Y J, Yang G. Efficient attribute based authenticated key agreement protocol [J]. Computer Science,2014,41(4):150-154,177