基于改进 NSGA2 算法的空间网络安全与性能优化

苗祎璠[1],杜杉杉[2],任佳豪[3],刘 然[3],石乐义[1,3*]
(1. 中国石油大学(华东) 计算机科学与技术学院,山东 青岛 266580;
2. 光大国际金融中心,山东 青岛 266071;
3. 中国石油大学(华东) 海洋与空间信息学院,山东 青岛 266580)

摘 要:在空间网络不断发展以及攻击威胁日益增加的背景下,其安全问题得到了研究人员的密切关注。但同时,其性能开销也会增大。为解决空间网络通信安全性、服务性能间的联合优化问题,选取机密性、完整性、可认证性作为安全程度的量化指标,选择时延作为性能指标,建立了网络安全与通信性能间的多目标优化模型。提出了一种 ISN-NSGA2 算法和纳什议价博弈的多目标优化决策方案。算法利用自适应锦标赛选择算子,促进种群较快收敛;运用基于拥挤熵的个体动态排挤机制代替拥挤距离一次性排挤,维持种群分布性;在得到一组非支配解后,使用合作博弈纳什议价模型进行折中决策。在 6 个基准多目标测试函数上对算法进行了性能测试,实验结果表明解的均匀性和收敛度均得到了很好的提升。采用该方案对模型求解,能够在适应网络安全和性能需求的情况下,从 Pareto 解集中选出使网络整体收益最大的最终决策解,有效实现两者的折中优化。

关键词:空间网络;通信安全;性能;自适应锦标赛选择;拥挤熵;动态排挤
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2023)08-0095-07
doi:10.3969/j.issn.1673-629X.2023.08.014

Security and Performance Optimization of Space Networks Based on Improved NSGA2

MIAO Yi-fan[1], DU Shan-shan[2], REN Jia-hao[3], LIU Ran[3], SHI Le-yi[1,3*]
(1. School of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China;
2. Everbright International Financial Center, Qingdao 266071, China;
3. School of Oceanography and Space Informatics, China University of Petroleum (East China), Qingdao 266580, China)

Abstract: In the context of the continuous development of space networks and the increasing threat of attacks, the security of space networks has received close attention from researchers. At the same time, its performance overhead will also increase. Aiming at the joint optimization problem between communication security and service performance of space networks, a multi-objective optimization model is constructed by selecting confidentiality, integrity, and authenticity as quantitative indicators of security degree and time delay as a measure of performance. An ISN-NSGA2 algorithm combined with Nash bargaining game is proposed for multi-objective optimization decision. The algorithm utilizes an adaptive tournament selection operator to promote faster population convergence, uses an individual dynamic crowding mechanism based on crowding entropy instead of one-time crowding at crowding distance to maintain population distribution, and uses a cooperative game Nash bargaining model for compromise decision making after obtaining a set of non-dominated solutions. The performance of the proposed algorithm is tested on six standard multi-objective test functions, and the experimental results show that the uniformity and convergence of the solution are well improved. Finally, using such scheme to solve the model, the decision solution that maximizes the overall network benefit can be selected from the Pareto solution set while adapting to the network security and performance requirements, effectively achieving the compromise optimization of both.

Key words: space network; communication security; performance; adaptive tournament selection; crowding entropy; dynamic crowding

收稿日期:2022-11-09 **修回日期**:2023-03-14
基金项目:国家自然科学基金资助项目(61772551);山东省自然科学基金资助项目(ZR2019MF034)
作者简介:苗祎璠(1998-),女,硕士研究生,研究方向为信息安全、拟态防御、博弈论;通信作者:石乐义(1975-),男,博士,教授,博导,CCF 会员(14178S),研究方向为计算机网络、信息安全、网络技术。

0 引 言

近年来,航空航天以及无线通信技术不断进步,空间卫星网络(简称空间网络)成为了国内外重点研究方向之一。但其通信安全面临着严峻挑战[1],性能分析和优化也成为了研究重点[2]。文献[3]提出了一种针对移动卫星环境的鲁棒密钥协商认证方案,具有较低的计算和通信开销。文献[4]提出一种适用于战术卫星的高性能组密钥管理算法,减轻了卫星节点的工作负载。现有工作多是对两者独立进行探讨,综合考虑空间网络安全和性能间相互关系并进行权衡优化的研究相对较少。随着安全技术在空间网络上的不断应用,网络安全和网络性能之间相互影响、制约,各种防护机制在提高网络可靠性的同时,会带来不同程度通信性能开销的增加。综合考虑性能、安全指标等的联合优化已成为空间网络研究领域的关键问题之一。

然而,空间网络的安全与服务性能的联合优化可以看作一个多目标优化问题(Multi - Objective Optimization Problem, MOP)。其结果是一系列较优的 Pareto 最优解集(Pareto-optimal Set,PS)。针对此问题有传统尺度化方法[5]以及进化算法[6]等。在众多进化算法中,Deb 等人提出的 NSGA2 算法[7]利用非支配等级和拥挤距离来衡量种群中个体的适应度。但该算法在解的收敛性、分布性等方面仍存在局限性。此后出现了许多改进 NSGA2 算法的多目标优化方法[8],但近期针对空间网络安全与性能的优化研究暂无文献查询。因此,该文利用改进的 NSGA2 算法很好地解决了空间网络安全与性能优化问题。

另外,空间网络安全和性能的均衡优化决策也是一个关键问题。目前,有许多国内外文献针对 NSGA2 算法的优化问题做了大量研究。常用的对非劣解集决策的方法有熵权法[9]、纳什均衡博弈[10]等。文献[11]以空间信息网络的高生存能力和低消耗为目标,提出了改进的 NSGA2 算法,利用 VIKOR 方法对 pareto 最优解进行模糊加权,得到了好的收敛效果。为了成本和压力间的均衡,文献[12]将 NSGA2 算法和 MOPSO 算法结合进行多目标优化。Esmikhani 等人[13]提出了基于多目标种群的模拟退火算法和改进的 NSGA2 算法,提高了模型的运行时间、成本和可用性。

综上所述,该文提出了基于改进 NSGA2 算法 ISN-NSGA2(NSGA2 Algorithm Based on Improved Spatial Network)与修正纳什议价模型的多目标优化决策方案,研究空间网络中通信安全与服务性能间的联合优化。针对 NSGA2 种群收敛精度低、分布性较差的问题,设计了自适应锦标赛选择算子,提出了基于拥挤熵的个体动态排挤策略,并基于修正的双人纳什议价模型进行最终解优选。最后,针对结果的收敛性和分布性进行评价,验证了新算法的有效性,并对模型进行了求解。

1 空间网络安全-性能优化问题建模

针对空间网络安全性和通信性能分别选取量化指标构建优化模型,从消息机密性、完整性以及真实性水平三个方面刻画空间网络通信安全程度,以时间延迟作为网络性能的衡量指标。根据相关研究成果给出形式化描述。

1.1 多目标优化模型描述与构建

1.1.1 通信安全性

(1)机密性。主要用于保证有用的信息不会泄露给未授权用户。机密性水平主要取决于密钥长度和加密算法。该文假定机密性级别最高为四,机密性水平 C_{level} 如下式[14]:

$$C_{\text{level}} = \frac{1}{2}\left[\left(2^{K_{\text{size}}/M_{\min}} - 1\right)\frac{8 - c_1}{2^{K_{\text{size}}/M_{\min}} + c_2} + c_1\right] \tag{1}$$

其中,K_{size} 表示密钥长度,$K_{\min}$ 表示密钥长度的最小取值,c_1 和 c_2 为调节因子,具体取值取决于 K_{size} 的范围。

(2)完整性。消息认证码(Message Authentication Code,MAC)是验证消息是否完整的一种主要技术。数据完整性水平随校验和呈指数增加。消息完整性水平 I_{level} 描述如下[8]:

$$I_{\text{level}} = \left(2^{M_{\text{ac}}/M_{\min}} - 1\right)\frac{c_3}{2^{M_{\text{ac}}/M_{\min}} + c_4} \tag{2}$$

其中,M_{ac} 是由 Hash 函数生成的消息认证码长度,$M_{\min}$ 表示认证码长度的最小取值,c_3 和 c_4 为调节因子,其值取决于 M_{ac} 的变化范围。

(3)可认证性。认证服务有效避免攻击者通过假冒终端或卫星实施恶意欺骗。空间网络使用单位时间内的认证次数来定量评估认证级别。对于特定认证算法,认证率越高,安全性越强。同理,身份认证水平 A_{level} 可表示如下[14]:

$$A_{\text{level}} = c_5\frac{r_m}{r_m + c_6} \tag{3}$$

其中,r_m 代表认证率,c_5、c_6 均为常数且由 r_m 的取值范围确定。可以观察到 A_{level} 随 r_m 缓慢增长,当 r_m 趋于最大值时,A_{level} 也缓慢达到认证的最高安全级别。

根据上述分析,空间网络通信安全水平由端到端认证水平、完整性水平和消息机密性水平组成,因此,总体通信安全性水平 S_L 可以描述为:

$$S_L = C_{\text{level}} + I_{\text{level}} + A_{\text{level}} \tag{4}$$

1.1.2 通信性能

假设单个数据包从发送端到达接收端的时间间隔,即总时延为 T。由于安全参数的提高在增强网络通信安全级别的同时也会带来额外性能开销,则 T 包

括用户端与卫星端之间收发数据时的加解密处理时延 C_{delay}、消息完整性验证时延 I_{delay}、通信双方的认证时延 A_{delay} 以及消息传播时延 T_{delay}。

(1)机密性时延:由加密延迟和解密延迟构成,加解密时间随密钥长度线性变化且呈正相关[8],可描述为式(5)。

$$C_{\text{delay}} = c_7 K_{\text{size}} + c_8 \tag{5}$$

其中,K_{size} 表示密钥长度,c_7、c_8 取决于具体加密算法。

(2)完整性验证时延:对于同一完整性算法,消息完整性延迟随校验和长度线性增加[14]。因此,数据完整性延迟可描述为式(6)。

$$I_{\text{delay}} = c_9 \text{MAC} + c_{10} \tag{6}$$

其中,c_9 和 c_{10} 由具体完整性验证算法决定。

(3)认证时延:是从发送身份验证请求到接收应答之间的时间[1]。其中,c_{11}、c_{12} 主要取决于网络状态和认证算法。则单个数据包在整个传输过程 T 中的认证时延[8]为:

$$A_{\text{delay}} = T(c_{11} r_m + c_{12}) \tag{7}$$

根据以上分析,可得单个数据包从地面发送端经卫星转发到达地面接收端这一过程的总时延 T 为:

$$T = C_{\text{delay}} + 2I_{\text{delay}} + A_{\text{delay}} + T_{\text{delay}} \tag{8}$$

1.2　问题模型

在上述工作基础上,建立由空间网络安全程度最大化和时间延迟最小化构成的多目标优化数学模型如下:

$$\begin{aligned} &\text{maximize } S_L(x) \\ &\text{maximize } T(x) \\ &\text{subject to} \begin{cases} \min(K_{\text{size}}) \leqslant K_{\text{size}} \leqslant \max(K_{\text{size}}) \\ \min(\text{Mac}) \leqslant \text{Mac} \leqslant \max(\text{Mac}) \\ \min(r_m) \leqslant r_m \leqslant \max(r_m) \end{cases} \end{aligned} \tag{9}$$

其中,目标函数 S_L 代表网络安全程度,追求自身最大化,T 代表网络通信时延,追求自身最小化,$X = (K_{\text{size}}, \text{Mac}, r_m)$ 为决策向量,决策向量组合成的策略总体称为决策空间。

2　基于 ISN-NSGA2 算法的多目标优化模型及决策

2.1　基于改进 ISN-NSGA2 算法的多目标优化

NSGA2 算法被广泛应用于多目标优化问题的求解。针对 NSGA2 种群收敛精度低、分布性差的缺陷,对锦标赛选择算子和精英选择机制进行了改进设计,使得到的解集在收敛性、分布性上都表现更优。

2.1.1　自适应锦标赛选择算子

N 元锦标赛选择是目前应用最广泛的一种选择算子。首先在父种群中随机取出 N 个个体,然后依据它们的非支配等级和拥挤距离选择出最优秀的个体作为下一代繁殖的亲本。但它也存在着收敛速度过慢或局部收敛的缺陷。因此,该文构造了一种自适应锦标赛选择算子,将选择强度 N 由固定值调整为随进化过程动态变化,引入了 Sigmoid 非线性函数:$f(x) = 1/(1 + e^{-ax})$,使得 N 值随迭代次数的增加而增大。该方法更能满足算法不同进化过程的动态需求。不同 a 值对应的 Sigmoid 曲线变化趋势如图 1 所示。

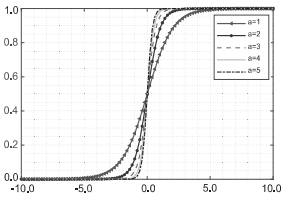

图 1　不同 a 值下的 Sigmoid 变化曲线

为了避免选择强度变化趋势过于陡峭,取 a 值为 1 对应的函数形式,基于 Sigmoid 函数调整的自适应锦标赛选择强度表达式如式(10)所示:

$$N = \text{round}\left[N_{\min} + (N_{\max} - N_{\min}) \frac{1}{1 + e^{10 - \frac{20g}{\text{Gen}}}}\right] \tag{10}$$

其中,$N_{\min}$ 和 $N_{\max}$ 分别为选择强度 N 的初始值和终止值,g 为当前进化代数,Gen 为进化次数,round( ) 为取整函数。图 2 展示了锦标赛选择强度随进化代数自适应变化的情况,调整后的选择规模随着进化代数的增加而递增。

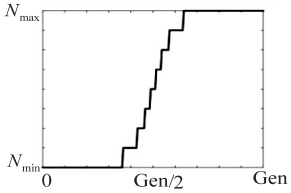

图 2　自适应锦标赛选择

2.1.2　基于拥挤熵的个体动态排挤

在 NSGA2 算法中,拥挤距离的计算在解的分布性和多样性保持方面发挥着重要作用。当规模过大时,同一等级中拥挤距离较小的个体将被直接淘汰。个体 i 的拥挤距离用各目标函数上排序后相邻两解的归一化距离之和表示:

$$\text{CD}_i = \sum_{j=1}^{m} \frac{f^j_{i+1} - f^j_{i-1}}{f^j_{\max} - f^j_{\min}} \tag{11}$$

其中,m 是目标函数的个数,f_i 是个体 i 的函数值,f_{i-1} 和 f_{i+1} 分别是个体 i 的前一个解和后一个解对应的函数值,$f^j_{\max}$、$f^j_{\min}$ 分别代表第 j 个目标函数的最大和最小值。拥挤距离值越大,说明其多样性越好,也就越优秀。但这种计算方式过于粗糙,不能准确反映个体的真实优劣情况。鉴于此,该文提出基于拥挤熵的个体动态排挤机制进行非劣解集缩减:引入拥挤熵代替拥挤距离,更加准确地评估解的优劣;将个体一次性排挤

改为动态排挤,逐个从当前非支配层中淘汰个体。

拥挤熵是一种新的拥挤度度量方法,其中融入了分布熵机制,利用分布熵的特性来描述个体在目标函数空间中与相邻解间的分布情况。个体 i 在目标函数 j 上的分布熵 E_i^j 为:

$$E_i^j = -\left[\mathrm{pf}_i^j \log_2(\mathrm{pf}_i^j) + \mathrm{pl}_i^j \log_2(\mathrm{pl}_i^j)\right]$$
$$\begin{cases} d_i^j = \mathrm{df}_i^j + \mathrm{dl}_i^j = f^j{}_{i+1} - f^j{}_{i-1} \\ \mathrm{pf}_i^j = \dfrac{\mathrm{df}_i^j}{d_i^j}, \mathrm{pl}_i^j = \dfrac{\mathrm{dl}_i^j}{d_i^j} \end{cases} \tag{12}$$

df_i^j 和 dl_i^j 分别代表个体 i 在第 j 个目标函数上与它的前、后邻解的距离,d_i^j 为两者之和,如图 3 所示。个体的分布性越好,分布熵就越大,当个体 i 在目标函数 j 上位于其相邻两解的中间时,它具有最优分布,此时对应的分布熵 E_i^j 为 1。将拥挤距离与分布熵结合,个体 i 在目标函数 j 上的拥挤熵 CDE_i^j 定义如下:

$$\mathrm{CDE}_i^j = \mathrm{CD}_i^j * E_i^j = -\frac{\mathrm{df}_i^j \log_2(\mathrm{pf}_i^j) + \mathrm{dl}_i^j \log_2(\mathrm{pl}_i^j)}{f^j{}_{\max} - f^j{}_{\min}} \tag{13}$$

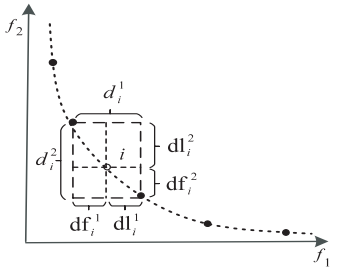

图 3 个体分布熵

个体 i 的整体拥挤熵 CDE_i^j 为个体在每个目标函数上对应的拥挤熵值之和,拥挤熵越大,个体越优秀。拥挤熵同时考虑了个体在目标函数空间的拥挤程度和分布情况,相较于拥挤距离可以更准确、合理地反映个体的优劣。综上,基于拥挤熵的个体动态排挤策略的步骤可描述为:

步骤 1:对合并种群 R_i 进行快速非支配排序,得到 k 个非支配集 $F_1, F_2, \cdots, F_k$,对于每个非支配集 F 中的解计算其拥挤熵,得到个体 i 的拥挤熵 i_{CDE};

步骤 2:令 $P_{t+1} = \Phi, i = 1$;

步骤 3:执行循环,若 $|P_{t+1}| + |F_i| < \mathrm{Pop}$(初始规模),那么 $P_{t+1} = P_{t+1} \cup F_i$,循环变量 $i = i + 1$;

步骤 4:循环结束,执行个体动态排挤:淘汰非支配集 F_i 中拥挤熵最小的个体,对其余个体重新计算拥挤熵,重复该过程,直至 $|P_{t+1}| = \mathrm{Pop}$。

2.1.3 ISN-NSGA2 优化算法流程

在上述基础上,图 4 给出了改进型算法的总体流程。改进的地方主要包括自适应锦标赛选择和精英选择。其中精英选择包括快速非支配排序、个体拥挤熵计算和个体动态排挤。

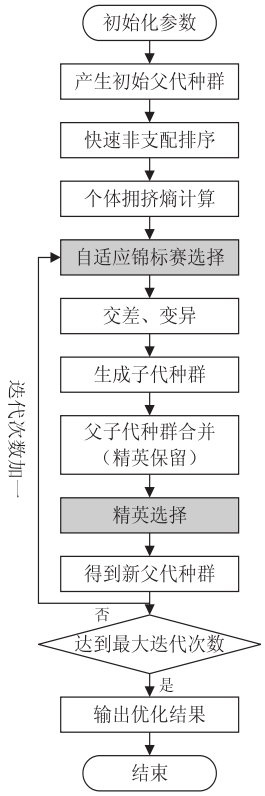

图 4 INSGA2 优化算法总体流程

2.2 基于修正双人纳什议价模型的双目标决策

在得到问题的一组非支配解后,基于修正的双人纳什议价模型进行最优解决策。经典双人纳什议价博弈模型为:

$$\begin{aligned} &\text{maximize } \amalg = \prod_{i=1}^{2} (f^i(X_j) - d^i) \\ &\text{subject to } f^i(X) \geqslant d^i (i = 1, 2) \\ &X_j \in S \quad (j = 1, 2, \cdots, n) \end{aligned} \tag{14}$$

其中,d^i 表示第 i 个博弈参与方的“谈判破裂点”,即双方能接受的最低效益;$f^i(X_j)$ 表示第 i 个博弈方执行策略 X_j 效益;$S = (X_1, X_2, \cdots, X_n)$ 表示双方的策略空间。博弈的目标是各参与者从各自“谈判破裂点”出发,通过不断讨价还价,进行各自收益的提高,并通过相互合作最大化联合效益 U。当 U 值最大化时,联合收益最大,也即达到合作博弈的均衡,此时的解 X_j 就称为“纳什议价解”(Nash Bargaining Solution,NBS)。

将纳什议价博弈思想应用于多目标决策。每个优化目标都被看作合作博弈中的参与方,目标函数可表征各博弈方的收益情况,Pareto 最优解集则作为博弈方的决策策略空间。空间网络安全性与时延代价的纳什议价博弈模型被描述为:

$$\begin{aligned} &\text{maximize } \amalg = (S_L(X) - S_L^{\mathrm{worst}})(T^{\mathrm{worst}} - T(X)) \\ &\text{subject to } S_L(X) \geqslant S_L^{\mathrm{worst}}, T(X) \leqslant T^{\mathrm{worst}} \\ &\{S_L(X), T(X)\} \in \mathrm{PF} \end{aligned} \tag{15}$$

其中, $S_L(X)$ 、$T(X)$ 分别代表博弈双方,即“安全方”与“时延方”,其范围为优化算法求解得到的 Pareto 最优前沿 PF ; S_L^{worst} 、T^{worst} 分别代表双方的最差值; Ц 代表联合收益。随着决策策略 X 的不断变化,双方在满足各自最小效用的前提下相互合作,以最大化联合收益为目标,选取最终解。

由于在空间网络环境下,对安全和性能均有较高要求,在原有模型基础上,使用 Minmax 方法进行目标函数的无量纲化处理,修正后的式子如式(16)所示:

$$\text{maximize Ц} = \left(\frac{S_L(X) - S_L^{\text{worst}}}{S_L^{\text{best}} - S_L^{\text{worst}}}\right)\left(1 - \frac{T(X) - T^{\text{best}}}{T^{\text{worst}} - T^{\text{best}}}\right) \tag{16}$$

3　实验分析与模型求解

3.1　实验性能测试

3.1.1　实验设置

该文选取多目标优化领域普遍采用的二目标标准测试函数 ZDT1、ZDT2、ZDT3、ZDT6 和三目标标准测试函数 DTLZ2 对 ISN-NSGA2 算法、NSGA2 算法进行性能测试。实验环境在 Windows 10 X64 系统下,电脑配置 1.00 GHz CPU 和 8 GB RAM,基于 MATLAB R2020 编程实现算法并画图。采用世代距离(Generational Distance,GD)和间距评价指标(Spacing,SP)对求解结果的收敛性和分布性进行评价。GD 和 SP 指标的具体计算如下:

$$\text{GD} = \frac{1}{P^*}\sqrt{\sum_{i=1}^{|P|} d_i^2}$$

$$d_i = \min_j\left\{\sum_{m=1}^{k}\left|f_m(v_i) - f_m(v_j)\right|\right\} \tag{17}$$

$$v_i, v_j \in P; i, j = 1, 2, \cdots, |P| \tag{18}$$

式中, P 是算法求解的 PF 上的点集, P^* 是真实 PF 上的点集, $d(v,P)$ 是解集 P^* 上的个体 v 与解集 P 上个体的最小欧氏距离。GD 值越小,算法所求 Pareto 前沿的收敛性越好。d_i 是个体 v_i 到其他解个体的最小距离, m 是目标函数的维度, $\bar{d}$ 是所有 d_i 的平均值。SP 指标度量的是各个解到其他解最小距离的标准差, SP 值越小,解集分布越均匀。

$$\text{SP} = \sqrt{\frac{1}{|P| - 1}\sum_{i=1}^{|P|}(d_i - \bar{d})^2} \tag{19}$$

3.1.2　测试与结果分析

为比较两种算法在分布性和收敛性上的性能差异,执行参数均统一设置如下:编码方式选择实数编码,种群规模取值 100,进化代数为 200,采用模拟二进制交叉、多项式变异,交叉和变异概率分别为 0.9 和 0.1。标准算法采用二元锦标赛选择,ISN-NSGA2 算法采用自适应锦标赛选择,其中 $N_{\max}$ 设置为 20, $N_{\min}$ 设置为 2。图 5 给出了两种算法在 5 个标准测试问题上所求 Pareto 前沿分布效果。图中深色部分为测试函数的真实前沿。

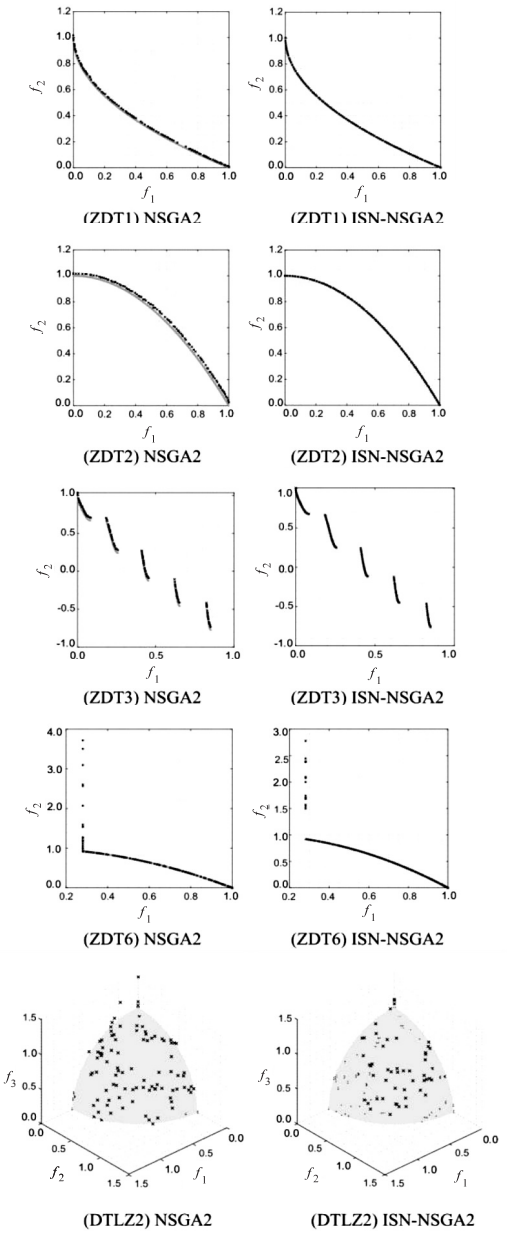

图 5　两种算法在 5 个测试函数上获得的 Pareto 前沿

左侧为原算法,右侧为改进算法。在解的收敛性方面,ISN-NSGA2 的求解结果与真实前沿更为接近。分布性方面,ISN-NSGA2 算法得到的 Pareto 前沿分布均匀且连续,这说明在解的多样性和分布性上 ISN-NSGA2 明显优于标准算法。

从统计数据的角度对算法作了进一步比较。将标准 NSGA2、改进的 NSGA2[15]、基于分解的多目标进化算法(Multi-Objective Evolutionary Algorithm based on Decomposition,MOEAD)[16] 和文中 ISN-NSGA2 算法在 5 个标准测试函数上分别独立运行 50 次,进化代数为

100,并对得到的指标结果统计最大、最小和平均值。

表 1 和表 2 分别给出了四种算法求解的 GD 和 SP 相关值。从表中数据可以观察到,文中算法的 GD 和 SP 的平均值均小于标准算法,说明 ISN-NSGA2 在收敛性和分布性上相较于其他算法均有提升。

表 1 四种算法的 GD 值比较

测试函数	GD 最大值				GD 最小值				GD 平均值			
	NSGA2	文献[15]算法	MOEAD	文中算法	NSGA2	文献[15]算法	MOEAD	文中算法	NSGA2	文献[15]算法	MOEAD	文中算法
ZDT1	6.60e-03	3.50e-02	3.02e-03	3.90e-03	2.40e-03	2.09e-03	1.15e-03	3.11e-04	7.88e-03	6.56e-03	2.15e-02	1.63e-03
ZDT2	3.49e-02	4.29e-02	5.11e-02	3.39e-02	3.30e-03	1.68e-03	1.174e-03	9.58e-04	9.10e-03	8.28e-03	2.43e-02	2.66e-03
ZDT3	1.18e-02	4.22e-02	2.61e-02	1.14e-02	9.10e-03	1.49e-03	5.72e-03	1.80e-03	1.22e-02	7.82e-03	1.07e-02	5.45e-03
ZDT6	2.07e-02	7.84e-02	3.32e-02	1.93e-02	1.55e-04	1.05e-03	5.39e-03	1.32e-04	2.96e-02	1.09e-02	4.78e-03	2.31e-03
DTLZ2	2.00e-03	2.49e-02	1.80e-03	1.50e-03	1.20e-03	1.20e-02	9.57e-04	9.21e-04	1.60e-02	1.58e-02	1.26e-03	1.10e-03

表 2 四种算法的 SP 值比较

测试函数	SP 最大值				SP 最小值				SP 平均值			
	NSGA2	文献[15]算法	MOEAD	文中算法	NSGA2	文献[15]算法	MOEAD	文中算法	NSGA2	文献[15]算法	MOEAD	文中算法
ZDT1	1.30e-02	3.56e-01	1.71e-02	3.04e-03	5.90e-03	1.72e-02	7.47e-03	2.18e-05	8.29e-03	6.22e-02	1.26e-02	3.77e-04
ZDT2	2.10e-02	4.28e-01	2.49e-02	2.42e-03	9.50e-03	1.25e-02	2.87e-03	8.05e-05	1.15e-02	7.95e-02	6.71e-03	6.20e-04
ZDT3	2.58e-02	4.21e-01	3.99e-02	1.10e-02	6.80e-03	1.246e-02	1.14e-02	2.80e-03	1.26e-02	7.50e-02	2.22e-02	4.54e-03
ZDT6	4.69e-01	7.83e-01	7.02e-01	1.26e-01	3.50e-02	8.50e-03	5.39e-03	1.50e-02	7.26e-02	1.07e-01	1.29e-01	5.18e-02
DTLZ2	7.09e-02	1.93e-01	8.91e-02	6.89e-02	1.20e-02	5.85e-02	6.63e-02	4.66e-02	5.98e-02	1.05e-01	7.58e-02	5.61e-02

图 6 给出了在 ZDT1 和 DTLZ2 函数下,标准 NSGA2 和文中算法独立运行 20 次获得的 GD 指标平均值随进化代数变化过程的曲线。对比可以发现,新算法的 GD 值降得更快,算法收敛速度提高,且在相同进化代数下,其值均小于标准算法的 GD 值。

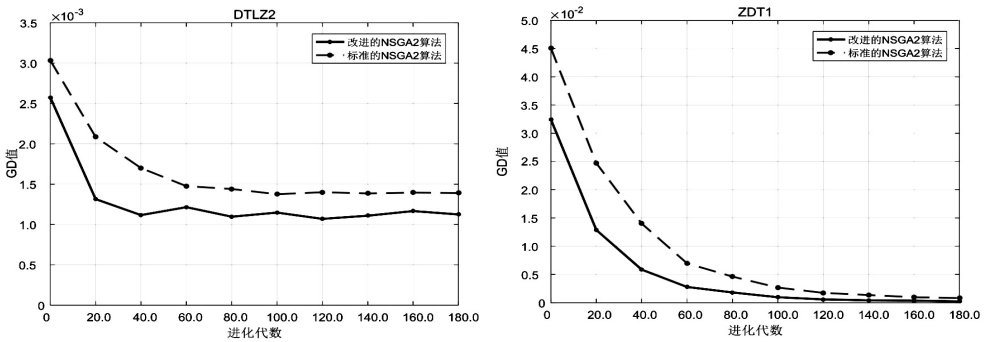

图 6 不同进化代数下两种算法 GD 值变化曲线

综上,提出的自适应锦标赛选择算子和基于拥挤熵的个体动态排挤策略是有效的,改进的算法相比标准算法在解分布性和收敛性上都表现更优。

3.2 模型求解

采用 ISN-NSGA2 算法对模型(9)进行求解。模型的决策变量为 $X=(K_{\text{size}},\text{Mac},r_m)$,密钥长度 K_{size}、消息认证码长度 Mac 的范围为:[16,32,64,128,256,512,1 024,2 048],认证率 r_m 的范围为[0.05,0.35],表 3 给出了模型中各参数的取值[9-10]。求解得到在各目标上的一组 Pareto 最优前沿如图 7 所示。横坐标表示空间网络通信的安全水平,纵坐标表示时延,图中 Pareto 最优解的分布体现了两目标间相互制约的关系。并利用式(16)进行最优解决策,最终结果如图 8 所示。

表 3 参数

参数	值	参数	值
c_1	3	c_8	75
c_2	3	c_9	0.02
c_3	4	c_{10}	9.1
c_4	2	c_{11}	0.5
c_5	6	c_{12}	0.21
c_6	0.2	T_{delay}/ms	270
c_7	0.2		

目标函数 $S_L=11.03$, $T=1\ 078.4$ ms,由公式(16)可得最优解决策,联合收益 U 最大为 0.782 4,策略 $X=(K_{\text{size}},\text{Mac},r_m)=(128,256,0.21)$,即设置密钥长度为 128 bits、消息认证码长度 256 bits,认证率 0.21/min时,网络整体利益最大且能实现空间网络安全程度与通信性能优化。

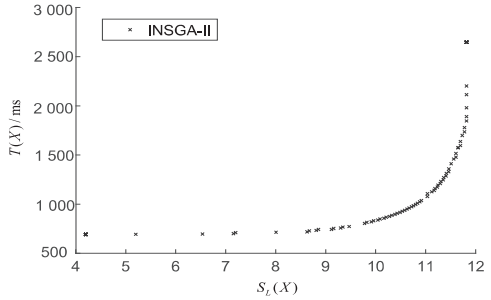

图 7　Pareto 最优前沿

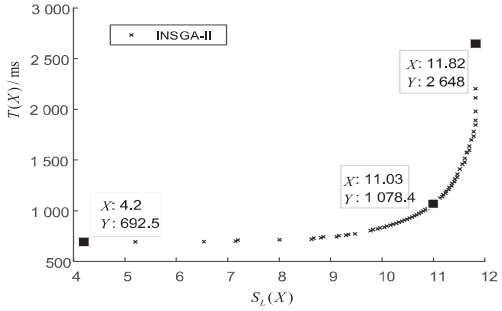

图 8　最优解决策

4　结束语

研究了空间网络中通信安全与服务性能间的联合优化。选取机密性、完整性、可认证性水平作为安全程度的量化指标,时延作为性能的衡量指标,以安全程度最大化、网络时延最小化为目标构建了数学模型。为求解该问题,提出改进 NSGA2 算法与修正纳什议价模型的多目标优化决策方案。ISN-NSGA2 采用了自适应锦标赛选择算子,将选择强度由固定值改进为随进化过程动态调整,有效改善了种群的收敛精度;引入拥挤熵作为新的拥挤度度量方法,更加准确地评估解的优劣,并将个体一次性排挤改为逐个淘汰,实现对非支配解集的均匀“修剪”;基于修正的双人纳什议价模型进行最优解决策,通过将目标建模为博弈双方,在其相互竞合作用下得到整体利益最大且兼顾双方公平的策略。实验表明,新算法在总体上有显著的收敛性、分布性和稳定性方面的优势。对模型求解能够得到获得满意网络通信质量和安全强度的折中优化解。所提方案兼顾了遗传算法全局寻优、通用性强的优点,同时为解的优选提供了一种公平客观的方法。

参考文献:

[1] XUE K, MENG W, LI S, et al. A secure and efficient access and handover authentication protocol for Internet of Things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.

[2] 朱　彦. 空间信息网络传输性能建模及分析[D]. 西安:西安电子科技大学, 2021.

[3] ALTAF I, SALEEM M A, MAHMOOD K, et al. A lightweight key agreement and authentication scheme for satellite-communication systems [J]. IEEE Access, 2020, 8: 46278-46287.

[4] ELMASRI M H, MEGAHED M H, ABD ELAZEEM M H. Design and software implementation of new high performance group key management algorithm for tactical satellite[C]// 2016 33rd national radio science conference (NRSC). Aswan City: IEEE, 2016: 149-158.

[5] CHO J H, WANG Y, CHEN R, et al. A survey on modeling and optimizing multi-objective systems[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1867-1901.

[6] ZINEDDINE M. Optimizing security and quality of service in a real-time operating system using multi-objective bat algorithm[J]. Future Generation Computer Systems, 2018, 87: 102-114.

[7] DEB K, PRATAP A, AGARWAL S, et al. A fast and elitist multiobjective genetic algorithm: NSGA-II[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(2): 182-197.

[8] RACHEDI A, BENSLIMANE A. Multi-objective optimization for security and QoS adaptation in wireless sensor networks [C]//2016 IEEE international conference on communications (ICC). Kuala Lumpur: IEEE, 2016: 1-7.

[9] ZHANG S B, LIU A J, LIANG X H. A multi-objective satellite handover strategy based on entropy in LEO satellite communications[C]//2020 IEEE 6th international conference on computer and communications (ICCC). Chengdu: IEEE, 2020: 723-728.

[10] ZHAO C, GUO D. Particle swarm optimization algorithm with self-Organizing mapping for Nash equilibrium strategy in application of multiobjective optimization[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 32(11): 5179-5193.

[11] WAN S, YANG P, ZHUO M, et al. An improved space information networks topology algorithm[C]//2021 IEEE international conference on information communication and software engineering (ICICSE). Chengdu: IEEE, 2021: 227-232.

[12] ZAREI N, AZARI A, HEIDARI M M. Improvement of the performance of NSGA-II and MOPSO algorithms in multi-objective optimization of urban water distribution networks based on modification of decision space[J]. Applied Water Science, 2022, 12(6): 1-12.

[13] ESMIKHANI S, KAZEMIPOOR H, SOBHANI F M, et al. Solving fuzzy robust facility layout problem equipped with cranes using MPS algorithm and modified NSGA-II[J]. Expert Systems with Applications, 2022, 210: 118402.

[14] CHEN J, ZENG H, HU C, et al. Optimization between security and delay of quality-of-service[J]. Journal of Network and Computer Applications, 2011, 34(2): 603-608.

[15] 熊　阳. 飞机起降保障作业动态调度策略研究[D]. 武汉:华中科技大学, 2020.

[16] 鲁宇明, 史　册, 黎　明, 等. 基于改进 MOEAD 算法的零件加工布局优化研究[J]. 机械设计, 2021, 38(5): 49-56.