文章编号:1001-506X(2013)06-1231-05 网址:www. sys-ele. com

基于 MATE 的卫星导航系统安全防护设计

张旺勋,侯洪涛,王维平
(国防科学技术大学信息系统与管理学院,湖南 长沙 410073)

摘 要:提出了基于多属性权衡空间探索方法的卫星导航系统安全防护设计方法。该方法由 4 个步骤组成:第一步,将决策者关注的任务需求和导航系统性能定义为各种"属性";第二步,通过分析这些属性,提出各种"设计变量",即各种防护手段;第三步,建立系统模型,将防护手段映射到属性和费用;第四步,权衡空间分析,在同一个权衡空间下比较各不相同的防护方案和手段。实验结果表明,该方法能够在同一个权衡空间详细考察比较所有备选方案的多个属性,从而为系统设计和评估提供更全面的参考依据。

关键词:卫星导航系统;安全防护;多属性权衡空间探索;费效分析
中图分类号:TN 967.1 **文献标志码**:A **DOI**:10.3969/j.issn.1001-506X.2013.06.17

MATE based design for protection of GNSS

ZHANG Wang-xun, HOU Hong-tao, WANG Wei-ping
(*School of Information System and Management, National University of Defense Technology, Changsha 410073, China*)

Abstract: A multi-attribute tradespace exploration (MATE) based design method for protection of global navigation satellite systems (GNSS) is presented. The method is composed of four phases. In the first phase, both the mission needs and GNSS performances that are preferred by decision-makers are defined and specified with attributes. In the second phase, the attributes are inspected and various design variables (i.e. protection means) are proposed. In the third phase, models are built to link the protection means to attributes and costs. In the fourth phase, tradespace analyses are made and all the designs are analyzed in the same tradespace. Experiment results show that these advantages of analyzing multi-attribute of all the designs in the same tradespace can provide comprehensive foundation for system design and evaluation.

Keywords: global navigation satellite systems (GNSS); protection; multi-attribute tradespace exploration (MATE); cost-effective analysis

0 引 言

全球卫星导航系统(global navigation satellite systems, GNSS)的广泛应用,使其成为国民经济发展的重要支柱和军用斗争的关键基础。它的作用和地位决定了其自身的安全性和系统导航对抗能力的重要性,系统安全防护措施的有无以及能力的强弱直接关系到国家的战略安全。因此,导航系统安全防护能力是与系统功能同等重要的属性,必须在系统论证及设计阶段就加以考虑。

目前研究卫星导航系统面临的威胁及其防御措施的文献较多,但大多数局限于定性列举和文字描述,定量分析的不多;在少数定量分析中,大部分是分析系统信号干扰与抗干扰的,而分析其他类型威胁的较少;现有研究方法也较少从全局角度分析和支持安全防护能力设计[1-3]。

与卫星导航系统安全防护研究类似的有系统安全风险分析、可靠性设计、复杂网络抗毁性等。但这些研究侧重点不同,系统安全风险分析与可靠性设计主要是从系统设计和管理的角度来进行研究,旨在提高系统的性能,而不关注威胁防护的攻防对抗;复杂网络抗毁性则认为所有复杂系统都可以抽象为网络,并通过抗毁性等测度研究系统特性,但卫星导航系统各分系统之间并不仅限于通信关系,抽象为网络问题难度较大。

总体来讲,目前对卫星导航系统面临的威胁及其防护手段较清楚,但对安全防护的整体研究和顶层设计研究较弱,主要原因在于:①大系统整体设计优化方法研究基础薄弱;②没有有效地分析多种威胁手段及其防护策略对系统整体及服务性能影响的评估方法。

本文在分析导航系统面临威胁及应对策略基础上,提

收稿日期:2012-03-26; **修回日期**:2012-11-21; **网络优先出版日期**:2013-04-03。
网络优先出版地址:http://www.cnki.net/kcms/detail/11.2422.TN.20130403.1110.020.html
基金项目:国家自然科学基金(60974074,61074107)资助课题

出了基于多属性权衡空间探索(multi-attribute tradespace exploration, MATE)的卫星导航系统安全防护设计方法。

1 MATE 方法介绍

MATE 是一种将决策理论和基于仿真的设计相结合的概念设计方法[4],是一种以价值为中心的、利用权衡空间探索来进行的系统设计和决策方法。该方法由麻省理工学院(Massachusetts Institute of Technology, MIT)的 Adam Ross 和 Nathan Diller 提出。

截止目前,MIT 已经将 MATE 应用于多个项目,包括空间系统架构设计[5]、演化采办[6]、价值稳健性[7]、政策不确定性研究[8]、模块化[9]、卫星雷达系统的动态设计[10]、体系设计[11]、对地观测卫星星座设计[12]等。

用 MATE 方法进行系统设计和分析包括 3 大步骤:明确需求、列举备选设计方案、备选方案的评估。图 1 给出了 MATE 方法的步骤过程[13]。

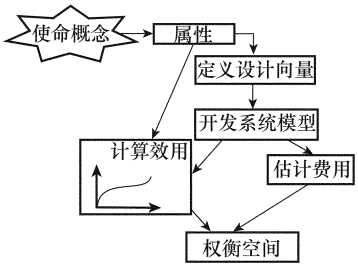

图 1 MATE 方法步骤图

第 1 步,通过决策者的喜好确定多个属性,这些属性通过多属性效用理论(multi-attribute utility theory, MAUT)集成为一个效用函数。第 2 步,通过分析这些属性,提出一系列的设计变量。所有的设计变量构成一个设计向量,而设计向量的所有取值则构成了权衡空间。第 3 步,通过系统模型评估各备选设计方案的费用和效用。

一般的系统设计过程可以看作是决策者在一个空间中不断地精简修正以减少备选方案的数量,直到选定某一个解决方案。图 2 给出了 4 种常见的系统设计方法,这 4 种方法对设计空间的范围考虑的各不相同:①局部解;②部分边界解;③边界解集合;④全空间探索。

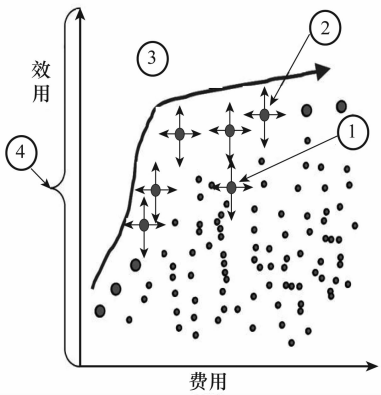

图 2 4 种不同的设计方法

很明显,方法④全空间探索方法考虑了所有的方案,这样就可以更加详细并且动态地分析权衡空间,通过分析不同点对变化的反应情况,可以得出哪些点更加稳健或者更适应这种变化[7]。

2 基于 MATE 的导航系统安全防护设计

借鉴 MATE 的思想,将用户和设计者关心的卫星导航系统的性能作为"属性",以各种防护手段作为"设计变量",提出了由 4 个步骤组成的卫星导航系统安全防护设计评估方法。

(1) 由导航系统总体论证专家、安全防护领域专家、相关技术领域专家根据当前的主要使命任务和卫星导航系统安全防护需求给出关心的属性(包括属性的定义、单位、范围、价值增长方向等),各属性的效用曲线以及最后总的效用函数。

表 1 和图 3 给出几个示例属性:水平定位精度、垂直定位精度、报警时间、危险误导信息(hazardously misleading information, HMI)的概率、可用性[14]。

表 1 导航系统常用属性

属性	定义	可接受范围
水平精度/m 垂直精度/m	系统测量或估计位置、时间等导航信息与真实值之间的重合度。	1←30 2.5←5
报警时间/s	从出现报警条件到报警消息到达用户设备天线的时间。	1←10
HMI 的概率	HMI 指没有发出完好性报警而实际上误差超过了报警门限的情况。	2×10^{-9}←2×10^{-7}
可用性	系统服务可以使用的时间百分比。	0.99～0.999 9

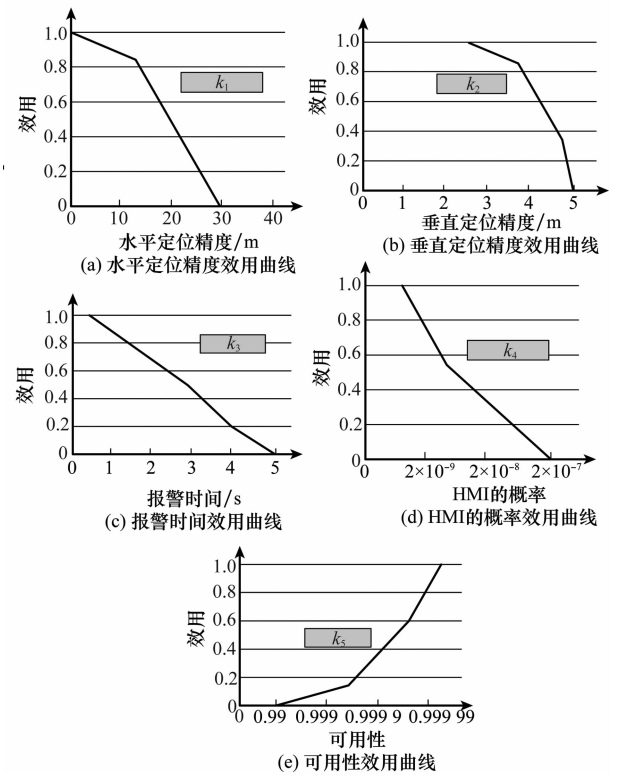

图 3 导航系统常用属性的效用曲线

表 1 包括了上述 5 个属性的定义和可接受范围，其中的数据是假设的未来 20 年某 GNSS 系统在某特定场景下的预期性能指标；第三列的箭头表示效用增长方向。图 3 给出了上述 5 个属性的示例效用曲线，k_i(i=1,2,…,5)表示各属性的权重。

将各属性综合起来的总的效用函数可采用如下的形式(也可以有其他复杂的形式)：

$$U(\underline{X}) = \sum_{i=1}^{5} k_i U(X_i) \tag{1}$$

式中，$U(\underline{X})$是总的效用值；$U(X_i)$是属性 i 的效用值；k_i 是各属性的权重，不同作战场景、不同应用终端，k_i 取值根据实际有所不同。

(2) 根据第 1 步提出的属性，分析并提出可能影响到这些属性的防护手段。通过属性来决定需要哪些设计变量(防护手段)的这种过程，建立了决策者所关心的“价值”与技术领域的明确关联。关联关系可通过表 2 所示的设计价值映射矩阵(design value mapping matrix, DVM)给出。

表 2　设计价值映射矩阵

手段名称	变量范围	水平精度	垂直精度	报警时间	HMI 的概率	可用性	总影响
星间链路	S_1	9	9	0	0	9	27
轨道间距	S_2	1	1	1	1	3	7
伪卫星技术	S_3	9	9	0	0	9	27
自然更换	S_4	1	1	0	0	3	5
新的军用码	S_5	3	3	0	0	9	15
核与激光加固	S_6	1	1	0	3	3	8
保安措施	S_7	0	0	9	9	3	21
冗余配置	S_8	3	3	0	3	0	9
逐渐方式下降	S_9	1	1	0	0	3	5
通信链路加密	S_{10}	0	0	0	3	9	12
组合导航	S_{11}	9	9	0	0	3	21
物理加固	S_{12}	3	3	0	0	9	15
扩频	S_{13}	3	3	0	0	1	7
抗干扰技术	S_{14}	9	9	1	1	9	29
保密反欺骗技术	S_{15}	1	1	0	9	9	20

表 2 的右上角是第一步列出的所有属性，左下角是所有的防护手段，中间部分的数字表示防护手段对属性的影响程度，9 表示设计变量对属性具有很大的影响，3 表示具有中等影响，1 表示影响较低，0 表示手段对属性没有贡献和影响作用。第 3 列变量范围 S_j 表示各种防护手段的可能取值范围。这一步只是定性的估计防护手段对属性的影响程度，通过这个映射矩阵，可以帮助设计者或决策者，将有限的资源放到那些对系统属性或性能影响较大的设计变量上(这里是防护手段)。对于设计变量与属性之间关系的详细评估将在下一步建立系统模型之后进行。

(3) 建立系统模型。模型主要是建立防护手段、设计变量、其他常量到系统费用和效能的映射，如图 4 所示。通过模型可以计算各方案的效用和费用。

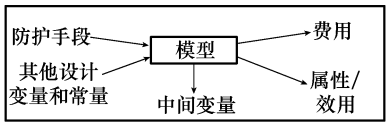

图 4　模型映射关系

本文构建一个简单的模型，具体算法如下，总的效用函数采用的方程(1)计算，其中单个属性的效用根据式(2)计算。

$$U(X_i) = \sum_{j=1}^{M} w_{ij} u_{ij} \tag{2}$$

式中，X_i 表示第 i 个属性；$U(X_i)$表示属性 i 的效用值；u_{ij} 表示防护手段 j 对属性 i 的效用贡献，这个效用值可以通过专家评分、对导航系统的建模仿真等多种手段来计算，这里不展开阐述；w_{ij} 表示防护手段 j 对属性 i 的影响权重，这个权重主要与作战场景和敌方的攻击手段有关(如“核与激光加固”防护手段只有在敌方对我采用核攻击或激光武器时才起作用，若敌方对我采取其他攻击，其权重应该为 0)，另外与不同的导航应用也有关系，因为不同的应用终端因为空间、费用等约束，有些防护手段是没法采取的，因此，在建模仿真计算的过程中，这个权重根据作战场景和服务终端等约束来确定。

根据式(1)和式(2)，总的效用可以表示为

$$U(\underline{X}) = \sum_{i=1}^{5} k_i \left(\sum_{j=1}^{M} (w_{ij} u_{ij}) \right) \tag{3}$$

总的费用表示为

$$Cost = (1 + 0.2) \sum_{j=1}^{M} c_{jl} \tag{4}$$

式中，c_{jl} 表示防护手段 j 在范围 S_j 中取第 l 种值时的费用；0.2 表示防护手段与系统其他部分接口等开支。

(4) 权衡空间分析。根据上一步建立的模型，每个由效用和费用描述的设计方案被放在同一个权衡空间，使得系统决策者可以在同一个权衡空间下比较各不相同的防护方案和手段。图 5 是 MIT 用权衡空间分析演化采办的例子[6]，图中每个点表示一种方案，横轴表示方案的费用，纵轴表示各方案的效用值。由图可以看出，在这个权衡空间中，有不少方案的效用接近 1，同时有更多的方案属于“可控方案”，即相对其他方案而言，它们的费用较高，效用较低，但是如果需求或系统环境发生变化，这些可控方案，很有可能变成效费比较高的方案；图中左上角用实线连起来的点组成了“Pareto 最优边界”，它们具有很好的效费比，最优边界的点对于系统决策具有很大的价值。

通过权衡空间分析，可以获取很多有益于决策的信息，如通过比较不同环境变量下权衡空间整体的变化情况，可以研究不同环境变量或决策者偏好的改变对系统效费的影响；根据某一属性设置点的大小或颜色可以分析系统总体对该属性变换的敏感性；通过某一点的详细信息分析，可以将某一具体方案的指标分配给其子系统或将信息提供给用户和决策者，为最终决策提供参考。

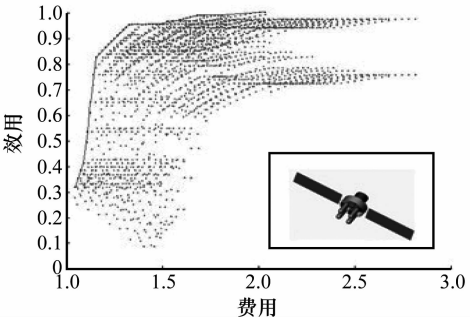

图 5 权衡空间费效分析示例

3 示例分析

本节通过一个示例，具体说明方法的使用和操作步骤。根据前文所述，方法共包括 4 个步骤，分别是根据需求提取属性、导出设计变量、建立系统模型以及权衡空间分析。

(1) 根据当前的主要使命任务和卫星导航系统安全防护需求给出关心的属性。

假设某侦察部队要在卫星导航系统的指导下，完成对敌方某特定区域的侦察任务。用户最关心的系统性能是水平定位精度与可用性。要求水平定位精度达到 20 m 以下，可用性为 0.9 以上。效用曲线如图 6 所示。

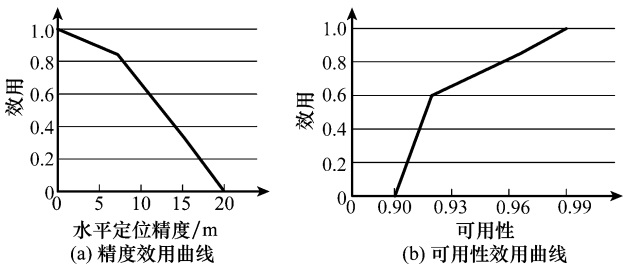

图 6 精度与可用性效用曲线

总的效用函数初步可采用式(1)的形式，具体如式(5)所示。

$$U(\underline{X}) = 0.6U_1 + 0.4U_2 \tag{5}$$

式中，U_1，U_2 分别为可用性和水平定位精度的效用值。根据任务场景，权重设为 0.6 和 0.4。

(2) 根据第一步提出的属性，提出可控的设计变量(防护手段)，并通过 DVM 确定需要重点考虑和关注的设计变量。

根据图 4 和表 2 列举的所有防护手段，结合本例中的任务场景，在这类小规模冲突中，敌方可能实施的攻击手段一般都只针对用户端，不会对卫星或地面测控系统进行大规模攻击。结合表 2 中的影响值大小，本例考虑的防护手段(设计变量)包括：接收机物理加固、伪卫星技术、组合导航、研制新的军用码、抗干扰技术、反欺骗技术。各防护手段取值如表 3 所示。

表 3 防护手段变量取值表

防护手段名称	变量取值范围
物理加固	1. 研制新材料 2. 原材料加厚 3. 某种涂料
伪卫星技术	1. 陆基 2. 天基
组合导航	1. 惯性导航 2. 网络辅助 3. 其他卫星系统
研制新的军用码	1. M1 2. M2 3. PM
抗干扰技术	1. 新的信号调制 2. 波束增强技术 3. 射频干扰检测技术 4. 自适应调零天线 5. 抗干扰滤波技术
反欺骗技术	1. 载噪比变化检测 2. 到达角检测 3. 双频伪距差检测 4. 与本地惯导比对 5. 通过其他导航系统信号对比

根据表 3，本例共考虑 6 个设计变量，6 个设计变量组成了设计向量，各防护手段的不同方案取值的不同组合构成了设计向量空间，即所有的备选方案权衡空间。

(3) 建立系统模型。模型主要是建立防护手段、设计变量、其他常量到系统费用和效用的映射。

准确的模型对于系统设计与分析具有重要的意义，本文旨在于介绍 MATE 方法，因此对具体建模不做赘述，实际运用中，可以根据需求建立不同模型，建立从防护手段和其他量到系统效用和费用的映射关系。本例采用前文提到的简单数学模型，并根据式(2)～式(5)计算最终的费用和效用。

(4) 权衡空间分析。根据表 3，本例共有 1 350 种方案。各方案的费用和效用情况如图 7 所示，图中横轴是归一化之后的费用，纵轴是系统总的效用，由精度和可用性根据式(5)计算获得。

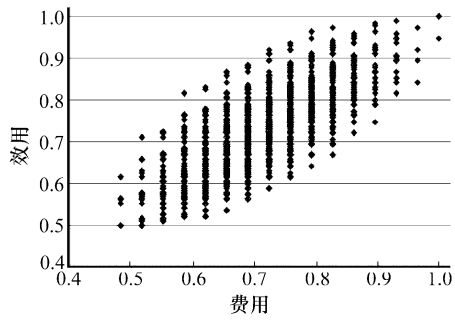

图 7 安全防护设计权衡空间

首先，可以直观地从图中看出，效用较高的点都集中在图的右上部，但同时这些方案的费用也是比较高的；而较经

济的方案都集中在左下部分，但这部分的效用值又较低。在不同的经济约束条件下或对效用不同要求，可以有侧重的在 Pareto 边界上选择适合的方案。

另外，分析评估权衡空间的方法有很多，其中 3 种基本的方法是：①仔细考察整个权衡空间的所有点；② 根据某一个属性的值为权衡空间中的点设置不同的大小和颜色；③选择个别的点（一般选择 Pareto 最优边界点）研究其详细信息。限于篇幅，此处不展开阐述，文献[11]和文献[13]有较详细的介绍。这里仅选择 Pareto 边界最右上方和最左下方的点进行分析，右上角的是 279 号方案（1，1），其总体效能为 1，费用为 1，各设计变量（防护方案）详细取值为（新材料、天基、惯性导航、PM 码、波束增强、到达角检测）；左下角的是 998 号方案（0.5，0.517 2），其总体效能为 0.615 8，费用为 0.482 8，各设计变量（防护方案）详细取值为（某种涂料、陆基、其他卫星系统、M1 码、抗干扰滤波技术、双频伪距差检测）。

Pareto 边界上的点无优劣之分，在不同的经济约束条件下或对效用不同要求，可以有侧重的在 Pareto 边界上选择适合的方案。如本例中为成功完成任务，不惜一切代价，那么可以考虑右上角的方案 279 以达到最优效用，而不用顾忌经济方面的因素；而如果此次任务的经费有限，假设为不超过 0.8，那么可以在 0.8 以左考虑适合自己的 1 184 号方案（0.793 1，0.963 2），其费用在 0.8 以下，总体效用也达到了较高的 0.963 2。

在最后一步的权衡空间分析中，不仅可以静态地查看比较所有备选方案的详细信息，还可以通过改变某一个设计变量，动态地观察设计方案在权衡空间中的变化路径，从而分析不同设计方案的敏感性或对变化的稳定性[11]。

4　结　论

卫星导航系统的安全防护对于经济发展、军事斗争具有极其重要的战略意义，定量评估不同防护手段的费效为系统设计和发展提供了科学依据。本文给出了一种基于 MATE 的安全防护设计框架，首先通过与相关专家的交流，以“属性”的形式描述导航系统安全防护的需求；然后以各防护手段作为“设计变量”，建立两者的映射关系；各“设计变量”的组合即不同的安全防护方案组成了“设计空间”；通过模型建立防护方案到效用和费用的映射，从而可以在同一个空间比较分析全部方案，为卫星导航系统的安全防护设计提供全面详细的参考和依据。

参考文献：

[1] Cai Z W, Chu H L. Analysis of the counter work strategy and technology of GPS navigation[J]. *GNSS World of China*, 2006(2):29－33.（蔡志武，楚桓林. GPS 导航对抗策略与技术分析[J]. 全球定位系统，2006(2)：29－33.）

[2] Li R G, Yu Z F, Jiao X. Countermeasures and efficiency evaluation of military satellite system[J]. *Electronic Warfare*, 2005(6):27－30.（李柔刚，余志锋，焦逊. 军用卫星系统对抗策略及效能评估[J]. 电子对抗，2005(6)：27－30.）

[3] Yang B, Yuan J P, Yue X K. Analysis and simulation of GPS jamming using pseudolites[J]. *Fire Control and Command Control*, 2007, 32(11): 111－113.（杨博，袁建平，岳晓奎. 利用伪卫星干扰 GPS 的可行性分析与仿真[J]. 火力与指挥控制，2007，32(11)：111－113.）

[4] Ross A M, Hastings D E, Warmkessel J M, et al. Multi-attribute tradespace exploration as front end for effective space system design[J]. *Journal of Spacecraft and Rockets*, 2004, 41(1): 20－28.

[5] Ross A M. Multi-attribute tradespace exploration with concurrent design as a valuecentric framework for space system architecture and design[D]. Massachusetts: Massachusetts Institute of Technology, 2003.

[6] Derleth J E. Multi-attribute tradespace exploration and its application to evolutionary acquisition[D]. Massachusetts: Massachusetts Institute of Technology, 2003.

[7] Ross A M. Managing unarticulated value: changeability in multi-attribute tradespace exploration[D]. Massachusetts: Massachusetts Institute of Technology, 2006.

[8] Weigel A. Bring policy into space systems conceptual design: qualitative and quantitative methods[D]. Massachusetts: Massachusetts Institute of Technology, 2002.

[9] Shah N B. Modularity as an enabler for evolutionary acquisition[D]. Massachusetts: Massachusetts Institute of Technology, 2004.

[10] Ross A M, McManus H L, Long A, et al. Responsive systems comparison method: case study in assessing future designs in the presence of change[C]// *Proc. of the AIAA Space Conference & Exposition*, 2008.

[11] Chattopadhyay D. A method for tradespace exploration of systems of systems[D]. Massachusetts: Massachusetts Institute of Technology, 2009.

[12] Rader A A, Newland F T, Ross A M. An iterative subsystem-generated approach to populating a satellite constellation tradespace[C]// *Proc. of the AIAA Space Conference & Exposition*, 2011.

[13] Richards M G. Multi-attrbute tradespace exploration for survivability [D]. Massachusetts: Massachusetts Institute of Technology, 2009.

[14] Kaplan E D, Hegarty C J. *Understanding GPS: principles and applications*[M]. 2nd ed. Massachusetts: Artech House Inc Press, 2006.

作者简介：

张旺勋（1985－），男，博士研究生，主要研究方向为体系论证与仿真、系统安全性。

E-mail：zhangwangxun2010@163.com

侯洪涛（1977－），男，讲师，博士研究生，主要研究方向为卫星总体性能建模与分析、复杂系统建模。

E-mail：houhongtao@nudt.edu.cn

王维平（1962－），男，教授，博士，主要研究方向为系统论证与仿真评估、体系工程与体系仿真。

E-mail：wang.wp2010@gmail.com