多路 GNSS 欺骗干扰信号功率控制策略

黄　森，陈树新，杨宾峰，吴　昊
(空军工程大学信息与导航学院，西安，710077)

摘要　为满足多路 GNSS 欺骗干扰信号整体获得目标接收机高捕获性能的实际应用需求，设计了一种多路信号互相关干扰约束下的信号功率最优控制策略。分析了多路欺骗信号功率对噪声基底的影响，研究了在此情况下欺骗信号的捕获性能。以噪声基底上升和欺骗信号相对捕获概率为约束，构建了控制策略的目标函数，利用遗传算法进行寻优计算。仿真结果表明，该策略实现了多路欺骗信号的捕获性能优于真实信号，且此时噪声基底的抬升不超过 10 dBW，欺骗信号功率不具有相关性。

关键词　全球导航卫星系统；欺骗干扰；功率控制；噪声基底；多路信号
DOI　10.3969/j.issn.1009-3516.2017.01.013
中图分类号　TN972　　**文献标志码**　A　　**文章编号**　1009-3516(2017)01-0076-05

A Power Control Strategy of Multiple GNSS Spoofing Signals

HUANG Sen, CHEN Shuxin, YANG Binfeng, WU Hao
(Information and Navigation College, Air Force Engineering University, Xi′an 710077, China))

Abstract: In order to meet the needs of the high captured performances integrally by target receiver for multiple GNSS spoofing signals, a power control strategy based on the cross-correlation interference of multiple signals is proposed. This paper analyzes the influence of multiple spoofing power on the noise floor, and discusses the acquisition of spoofing signal. Taking the rise of noise floor and spoofing relative acquisition probabilities as a bound, an objective function is built, and the optimized solutions is obtained based on genetic algorithm. The simulations show that the performance of multiple spoofing acquisition is superior to that of the authentic according to the proposed strategy, and at the same time the noise floor rises no more than 10 dBW, and the spoofing power is uncorrelated.

Key words: GNSS; spoofing interference; power control; noise floor; multiple signals

全球卫星导航系统(GNSS)技术已被广泛的装备于各类武器系统上，其军事应用已经渗透到现代战争的各个环节，并发挥着不可替代的作用。在建立导航系统的同时，GNSS 干扰技术也不断发展。GNSS 欺骗式干扰[1-6]因具有智能化、灵活度高、隐蔽性好等优点，受到极大关注。

欺骗干扰模式主要包括转发式欺骗和生成式欺骗 2 种类型。文献[7～8]定量分析了生成式欺骗信号对接收机实现相关峰牵引所需满足的信号功率条件。文献[9]推导了 GNSS 欺骗信号对目标接收机

收稿日期：2016-07-20
基金项目：国家自然科学基金(51577191)
作者简介：黄　森(1993－)，男，浙江乐清人，硕士生，主要从事卫星导航干扰研究. E-mail：409181582@qq.com

引用格式：*黄森，陈树新，杨宾峰，等. 多路 GNSS 欺骗干扰信号功率控制策略[J]. 空军工程大学学报(自然科学版)，2017，18(1)：76-80.*
HUANG Sen, CHEN Shuxin, YANG Binfeng, et al. A Power Control Strategy of Multiple GNSS Spoofing Signals[J]. Journal of Air Force Engineering University(Natural Science Edition), 2017, 18(1): 76-80.

载噪比估计的影响。文献[10]提出一种通过测量信号功率的相关性来检测欺骗干扰的技术。文献[11]推导了 GPS 接收机对转发式欺骗干扰的捕获概率，得出在典型条件下，转发器只需较小的功率增益便有更高的捕获概率。文献[12]提出了针对在传统欺骗干扰模式下，欺骗信号注入目标接收机效率不高的问题，提出构建拒止环境掩护欺骗信号注入，并证明了其可行性。从信号注入角度看，生成式和转发式都需要通过控制欺骗信号的功率，进而获得更高的相关峰，使得欺骗信号被捕获的概率大于真实信号。但目前国内针对欺骗信号捕获性能的分析多数只停留在对单路信号模型上，在拓展到多路信号模型时，还应考虑其它因素对捕获性能的影响，比如信号间的互相关干扰。

从多路信号角度出发，本文先通过公式推导分析了多路欺骗信号功率对噪声基底的影响，然后又定量给出了不同噪声基底与欺骗信号捕获性能的函数关系，得到欺骗信号不能通过无限制的增加功率来获得高捕获性能的结论，最后提出一种利用噪声基底和欺骗信号相对捕获概率为约束条件的目标函数，并通过遗传算法寻优得到多路欺骗信号功率最优分配策略。

1　欺骗信号功率对捕获性能的影响

对于 GPS 系统而言，卫星信号的捕获过程是在设定好不同 PRN 码的各通道里，在载波频率和码相位两维域内，扫描式搜索最大的 PRN 码相关峰[13]。因为信号受到噪声的干扰，所以相关峰的幅值可视为一个随机变量，服从方差与噪声有关的高斯分布。理想的单路信号模型将噪声简单的视为热噪声，并赋予固定值进行信号捕获性能分析。然而，为贴近实际欺骗场景，在多路模型下实现多路欺骗信号整体捕获性能最优，需要考虑 PRN 码间的互相关干扰作用[10]，不能盲目增加干信比。

1.1　欺骗信号功率对噪声估计的影响

在捕获过程中，GPS 信号在经过码环相关后，其第 l 路信号的自相关幅值：

$$y_l[K]=\sqrt{P_l^a}\exp(\mathrm{j}\varphi_l)+\sum_{\substack{i=1\\ i\neq l}}^{N_{Auth}}\sqrt{P_l^a}F_{il}[K]+\sum_{k=1}^{N_{Spoof}}\sqrt{P_k^s}F_{kl}[K]+\eta[K] \tag{1}$$

式中：

$$F_{il}[K]=\frac{1}{N}\sum_{n=(K-1)N+1}^{KN}c_i(n-\tau_{ilK})c_l(n)\exp(\mathrm{j}\Delta\omega_{ilK}+\mathrm{j}\Delta\varphi_{ilK}) \tag{2}$$

式中：$F_{il}[K]$ 表示第 i 路与第 l 路信号之间的互相关干扰，P_i^a 和 P_k^s 分别表示第 i 路真实信号功率和第 k 路欺骗信号功率，φ_l 表示第 l 路信号的载波相位，$\Delta\varphi_{ilK}$ 、$\Delta\omega_{ilK}$ 和 τ_{ilK} 分别表示第 i 路本地同步信号与第 l 路卫星信号之间的载波相位差、多普勒频移差和时延，$\eta[K]$ 表示服从正态分布的环境噪声。在实际应用中，一般通过虚构一个不存在信号列表中 PRN 码 f，与信号进行相关运算，来估计噪声基底。由于 f 与信号列表中的任一 PRN 码不相关，于是有：

$$\sqrt{P_l^a}\exp(\mathrm{j}\varphi_l)=0 \tag{3}$$

因此，噪声基底估计的相关结果 $\sigma^2_{y_f[K]}$ 可写为：

$$\sigma^2_{y_f[K]}=\mathrm{var}\Big[\sqrt{P_l^a}\exp(\mathrm{j}\varphi_l)+\sum_{\substack{i=1\\ i\neq l}}^{N_{Auth}}\sqrt{P_l^a}F_{if}[K]+\sum_{k=1}^{N_{Spoof}}\sqrt{P_k^s}F_{kf}[K]+\eta[K]\Big]=\sum_{\substack{i=1\\ i\neq 1}}^{N_{Auth}}P_l^a\,\mathrm{var}[F_{if}[K]]+\sum_{k=1}^{N_{Spoof}}P_k^s\,\mathrm{var}[F_{kf}[K]]+\mathrm{var}[\eta[K]] \tag{4}$$

式中：$F_{if}[K]$ 和 $F_{kf}[K]$ 分别表示第 i 路真实信号与第 k 路欺骗信号在噪声基底估计中产生的参量；$\mathrm{var}[\cdot]$ 表示求随机变量方差。这两者是包含了 I/Q 支路的复数信号，且数值上服从均值为 0 的二维正态分布，可以表示为：

$$F_{if}[K]\sim N_c\left(\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\sigma^2_{I,F_{if}} & 0\\ 0 & \sigma^2_{Q,F_{if}}\end{bmatrix}\right) \tag{5}$$

取互相关协方差 $\sigma^2_{I,F_{if}}=\sigma^2_{Q,F_{if}}=0.000\,33$[10]。环境噪声 $\eta[K]$ 产生的积分值也服从零均值的高斯分布，可表示为：

$$\eta[K]\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\frac{\sigma_n^2}{N}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) \tag{6}$$

则考虑白噪声和互相关干扰因素后的噪声基底估计可表示为：

$$\hat{\sigma}_n^2=\sigma^2_{y_f[K]}=\frac{N_0}{2NT_s}+\Big(\sum_{i=1}^{N_{Auth}}P_i^a+\sum_{k=1}^{N_{Spoof}}P_k^s\Big)\sigma^2_{I,F_{if}} \tag{7}$$

令相干积分周期 $T_{\mathrm{coh}}=NT_s=1$ ms，环境噪声功率 $N_0=-204$ dBW/Hz，单路真实信号平均功率为 -158 dBW[13]，真实与欺骗信号均为 10 路，且各路欺骗信号功率相等。此时每一路真实信号 P_i^a 和欺骗信号 P_k^s 与噪声基底估计 $\hat{\sigma}_n^2$ 的信噪比 SNR 分别为 K_i^a 和 K_k^s，定义为：

$$K_i^a=\frac{P_i^a}{2\hat{\sigma}_n^2}\ ,\ K_k^s=\frac{P_k^s}{2\hat{\sigma}_n^2} \tag{8}$$

根据式(7)和式(8)可以得到欺骗信号功率与噪声估计、真实信号信噪比、欺骗信号信噪比 3 者的关系，经仿真实验，结果见图 1。

从图 1 中可以看出：①噪声基底 $\hat{\sigma}_n^2$ 随着欺骗信

号总功率的增加而上升,且当总功率超过−158 dBW时效果明显;②真实信号信噪比 K_i^a 随着欺骗信号总功率增加而下降;③欺骗信号信噪比 K_k^s 随着欺骗信号总功率增加而上升。

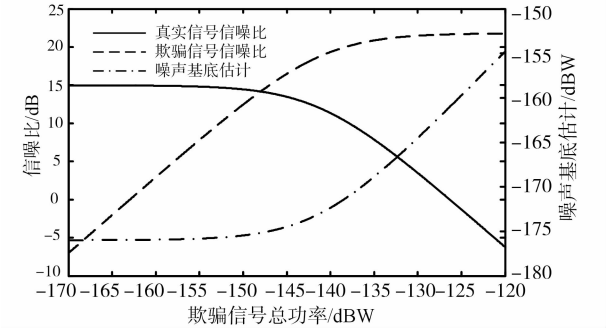

图 1 噪声基底、信噪比与欺骗信号总功率的关系

Fig. 1 Signal-to-noise ratio and nose floor estimation versus total spoofing power

1.2 欺骗信号对捕获性能的影响

在 GPS 信号捕获过程中,接收机在每个频率和 PRN 码相位的搜索方格中对 I 路和 Q 路信号进行测量和跟踪,在非相干积分后得到自相关幅值 $V=\sqrt{I^2+Q^2}$,并比较幅值与门限,判定信号存在与否。当不存在卫星信号时,V 呈瑞利分布,通过积分概率密度函数,可以求得信号捕获虚警概率[14]:

$$P_{\mathrm{fa}}=\int_{Vt}^{\infty}\frac{v}{\hat{\sigma}_n^2}e^{-\frac{v^2}{2\hat{\sigma}_n^2}}\mathrm{d}v \tag{9}$$

当存在 i 路卫星信号时,V 呈莱斯分布,通过积分概率密度函数可得检测概率[15]:

$$P_{\mathrm{d}}=\int_{Vt}^{\infty}\frac{v}{\hat{\sigma}_n^2}e^{\frac{-v^2+a_i^2}{2\hat{\sigma}_n^2}}I_0\left(\frac{va_i}{\hat{\sigma}_n^2}\right)\mathrm{d}v \tag{10}$$

式中:Vt 为判决门限值;a_i^2 为第 i 路信号相干积分后的功率;$I_0(\cdot)$ 为第一类零阶贝塞尔函数。信号捕获中利用给定的虚警概率 P_{fa},根据式(9)计算门限值 $Vt=\sigma_n\sqrt{-2\ln P_{\mathrm{fa}}}$。服从莱斯分布的概率密度函数积分值可视为相干积分后信噪比 K_i^a 和 K_k^s 的函数。

实施欺骗式干扰时,GPS 接收机前端同时存在 2 路相同 PRN 码信号,应以接收机检测到信号,且该信号为欺骗信号的条件概率来作为欺骗信号捕获性能的依据,此时第 i 路真实信号和欺骗信号检测概率分别为 $P_{d,i}^a$ 和 $P_{d,i}^s$。该条件概率称为欺骗信号的相对捕获概率 P_{r}:

$$P_{\mathrm{r}}=\frac{P_{d,i}^s}{P_{d,i}^s+P_{d,i}^a} \tag{11}$$

在 1.1 节仿真条件下,欺骗信号总功率与单路信号捕获概率的关系见图 2。

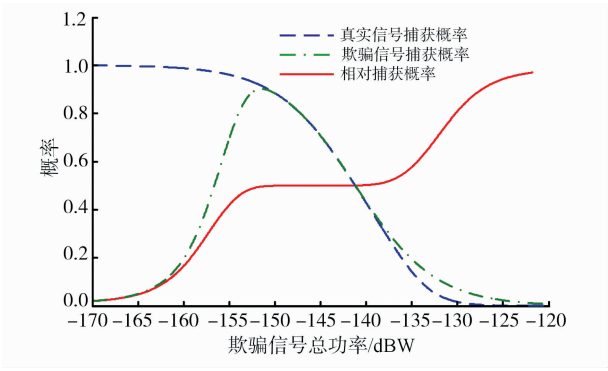

图 2 捕获概率与欺骗信号总功率的关系

Fig. 2 Acquisition probability versus total spoofing power

图 2 中可以看到:①欺骗信号的相对捕获概率随欺骗信号总功率的增大而增大;②当欺骗信号总功率很大时,真实信号与欺骗信号的捕获概率都很小,这将导致信号无法注入;③实际中,可以控制每路欺骗信号功率,使得每路欺骗信号捕获概率趋势不一致。

综合 1.1 和 1.2 节可以看出,在单路模型中为增加欺骗信号的捕获性能而不限制地增加欺骗信号功率,对多路模型不适用。多路模型下,每一路欺骗信号功率增加,都将通过欺骗信号总功率来抬升噪声基底,从而导致每一路信号捕获性能下降。此外,已有的技术还可通过测量噪声基底抬升幅度,来检测是否存在欺骗干扰信号。所以,各欺骗信号支路同时满足高捕获性能受到噪声基底和各相对捕获概率的约束,为此本文采用优化功率控制来解决问题。

2 基于遗传算法的信号功率优化

2.1 构建目标函数

取每一路欺骗信号的相对捕获概率 $P_{r,i}$ 和噪声基底 $\hat{\sigma}_n^2$ 为衡量单路欺骗欺骗效果的参数,其中希望噪声尽可能的小,以躲避抗欺骗干扰技术和信号捕获概率过小的情况;希望每一路的相对捕获概率 $P_{r,i}$ 尽可能大。综合以上两方面,可将目标函数设为:

$$F=\sum_{i=1}^{N}\frac{\hat{\sigma}_n^2}{P_{r,i}} \tag{12}$$

此函数值越小,对应的欺骗信号功率分配越优。此外,由于欺骗信号相对捕获概率为 $P_{r,i}=0.5$ 时,无法体现其优先被捕获能力,因此增加函数的约束条件为 $P_{r,i}>0.5$。

2.2 信号功率优化过程

利用遗传算法优化功率分配问题的具体过程如下[16-18]:

1)编码。经仿真实验发现,当欺骗功率增益接近 30 dB,欺骗信号的捕获概率已达到 1,因此可以

将欺骗功率增益的范围定为 [0，30]，编码时以每路信号欺骗功率增益进行长度为 L 的二进制编码，10 路功率增益编码串接表示个体，共有 $10L$ 位二进制数，可以根据功率控制的进度要求确定 L 的取值，本文取 $L=40$。

2）种群初始化。设种群大小为 M，取第 k 代的种群 $\boldsymbol{G}_k$，随机生成初始种群 $\boldsymbol{G}_0$，其中 $g_{0,j,m}$ 服从 0～1 等概率分布，$\boldsymbol{G}_k$ 中第 j 个个体表示为：

$$\begin{aligned}&\boldsymbol{G}_{k,j}=(g_{k,j,1},g_{k,j,2},\cdots,g_{k,j,m}),\\&m=(1,2,\cdots,10L)\end{aligned}\tag{13}$$

3）适应度函数设计。遗传算法中适应度函数值越小，个体将被分配的适应度越大，越容易被保留，因此上一节构建的目标函数可直接作为适应度函数使用。其约束条件可通过构建惩罚函数，使不满足约束条件的个体适应度函数值增大，罚函数可表示为：

$$P_{r,i}=\begin{cases}P_{r,i}, & P_{r,i}>0.5\\ 0.01P_{r,i}, & P_{r,i}\leqslant 0.5\end{cases}\tag{14}$$

4）应用遗传算子。采用选择、重组、变异、重插入的顺序进行遗传运算。①选择：从父代种群中选择优良个体，剔除掉目标函数 F 值大的个体。②重组：调用单点交叉函数，使父代个体两两为组进行交配，以一定概率交换部分基因。③变异：使个体的每个基因以特定的概率发生变异，这可以避免寻优过程过早收敛于局部最优。④重插入：用子代代替父代并返回结果种群，更新父代种群进行新一轮算法计算。

5）优化解输出

当遗传算法进行到指定代数后停止计算，选择末代最优个体，并将二进制编码解码，获得最优功率分配方案。

3　仿真计算

仿真实验中，假设空间中有 10 颗不同俯仰角的卫星，且精确已知其达到定位目标的功率大小，其值见表 1[11]。在本次试验中，遗传算法各参数取值为：编码长度 $N=20$；种群大小 $M=60$；遗传代数 50，交叉概率 0.1，变异率为 0.035，代沟为 0.9。为展示遗传算法优化功率分配过程，画出目标函数最优解的历代变化情况，见图 3。

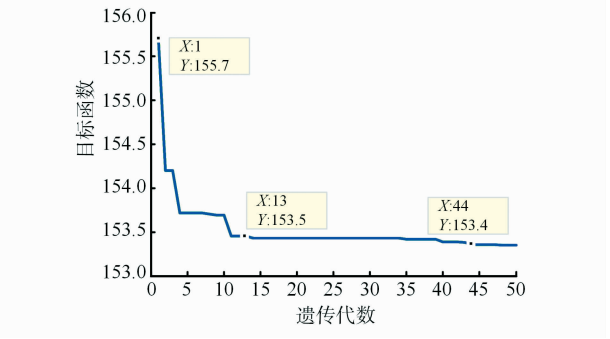

图 3　最优解的变化情况

Fig. 3　The changing situation of the optimal solutions

由图 3 可知，当遗传进行到第 21 代时，目标函数趋于稳定值。取最末代最优个体，所得优化的欺骗概率以及对应的信号信噪比和捕获概率见表 1。可以看出：①每路欺骗信号功率随机分配不具有相关性；②每路欺骗信号都得到超过 50％的相对捕获概率；③在功率最大的第 7、8、9、10 路真实信号上，欺骗增益最小，控制了欺骗信号总功率；④最优解时的噪声功率为－163.679 8 dBW。

表 1　最优解时各支路参数

Tab. 1　Branches' parameters of the optimum solution

信号支路	第 1 路	第 2 路	第 3 路	第 4 路	第 5 路	第 6 路	第 7 路	第 8 路	第 9 路	第 10 路
真实信号功率/dBW	－161.2	－159.4	－159.9	－156.9	－156.5	－155.4	－154.7	－154.1	－153.8	－153.30
功率增益/dBW	17.72	19.70	15.81	21.30	17.24	19.27	18.35	6.57	8.13	13.61
欺骗信号功率/dBW	－143.48	－139.70	－144.09	－135.60	－139.26	－136.13	－136.35	－147.53	－145.67	－139.69
欺骗信号信噪比	52.32	124.97	45.46	321.26	138.17	284.47	270.17	20.60	31.61	125.19
相对捕获概率	0.93	0.89	0.91	0.80	0.78	0.72	0.68	0.64	0.63	0.60

4　结语

本文从多路卫星信号互相关干扰角度出发，经公式推导和仿真实验，定量分析得到欺骗信号总功率与欺骗信号捕获性能的关系，得到在多路信号模型下不能无限制增加欺骗信号功率，以达到高捕获性能。以噪声基底和相对捕获概率为参数构建目标函数，提出了一种新的欺骗信号功率控制策略。仿真实验结果表明，该策略得到的多路欺骗信号同时获得超过 50％的相对捕获概率，此时欺骗功率增益不具有相关性，噪声基底抬升不超过 10 dBW，避免了现有基于检测信号功率相关性和噪声基底的抗欺骗干扰技术，增强了欺骗信号的隐蔽性。该多路信号模型符合应用实际，其功率控制策略对欺骗干扰技术的研究具有一定的指导意义。

参考文献(References):

[1] PSIAKI M L, HUMPHREYS T E, GNSS Spoofing and Detection[J]. Proceeding of the IEEE, 2016, 104(6): 1-13.

[2] SCHMIDT D, RADKE K, CAMTEPE S, et al. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures[J]. ACM Computing Surveys, 2016, 48(4): 1-31.

[3] JAFARNIA A, BROUMANDAN A, NIELSEN J, et al. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques[J]. International Journal of Navigation & Observation, 2012, 2012(9): 1.

[4] KERNS A J, SHEPARD D P, BHATTI J A, et al. Unmanned Aircraft Capture and Control Via GPS Spoofing[J]. Journal of Field Robotics, 2014, 31(4): 617-636.

[5] LARCOM J A, LIU H. Modeling and Characterization of GPS Spoofing[C] // IEEE International Conference on Technologies for Homeland Security. 2013: 729-734.

[6] 黄龙，唐小妹，王飞雪. 卫星导航接收机抗欺骗干扰方法研究[J]. 武汉大学学报，2011，36(11)：1344-1347.
HUANG L, TANG X M, WANG F X. Anti-Spoofing Techniques for GNSS Receiver[J]. Geomatics and Information Science of Wuhan University, 2011, 36(11): 1344-1347. (in Chinese)

[7] JAFARNIA-JAHROMI A, LIN T. Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver[C] // Proceedings of the International Technical Meeting of the Institute of Navigation. 2012: 790-800.

[8] 黄龙，吕志成，王飞雪. 针对卫星导航接受机的欺骗干扰研究[J]. 宇航学报，2012，33(7)：884-890.
HUANG L, LÜ Z C, WANG F X. Spoofing Pattern Research on GNSS Receivers[J]. Journal of Astronautics, 2012, 33(7): 884-890. (in Chinese)

[9] DEHGHANIAN V, NIELSEN J. GNSS Spoofing Detection Based on Receiver C/No Estimates[C] // Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 2878-2884.

[10] BROUMANDAN A, JAFARNIA-JAHROMI A, et al. GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation[C]// Position Location & Navigation Symposium. IEEE, 2012: 479-487.

[11] 刘延斌，苏五星，闫抒升. 转发式欺骗信号干扰 GPS 接收机的效能分析[J]. 空军雷达学院学报，2004，18(4)：4-6.
LIU Y B, SU W X, YAN S S. Effectiveness Analysis of Repeater Deception Jamming Signal upon GPS Receiver[J]. Journal of Air Force Radar Academy, 2013, 18(4): 68-70. (in Chinese)

[12] 史密，陈树新，吴昊，等. 拒止环境实现注入的 GPS 欺骗干扰[J]. 空军工程大学学报(自然科学版)，2015，16(6)：27-31.
SHI M, CHEN S X, WU H, et al. A Spoofing Pattern Based on Denial Environment[J]. Journal of Air Force Engineering University (Natural Science Edition), 2015, 16(6): 27-31. (in Chinese)

[13] 谢钢. GPS 原理与接收机设计[M]. 北京：电子工业出版社，2009.
XIE G. Principles of GPS and Receiver Design[M]. Beijing: Publishing House of Electronics Industry, 2009. (in Chinese)

[14] JAFARNIA A, BROUMANDAN A, NIELSEN J, et al. GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power, and C/N0 Measurements[J]. International Journal of Satellite Communications and Networking, 2012, 30(4): 181-191.

[15] 胡彦逢，边少锋，曹可劲，等. GNSS 接收机欺骗干扰功率控制策略[J]. 中国惯性技术学报，2015，23(2)：207-210.
HU Y F, BIAN S F, CAO K J, et al. Spoofing Power Control Strategy for GNSS Receiver[J]. Journal of Chinese Inertial Technology, 2015, 23(2): 207-210. (in Chinese)

[16] 李明. 遗传算法的改进及其在优化问题中的应用研究[D]. 长春：吉林大学，2004.
LI M. The Study on Improved Genetic Algorithm and Its Application in Optimization Questions [D]. Changchun: Jilin University, 2004. (in Chinese)

[17] 王银年. 遗传算法的研究与应用[D]. 无锡：江南大学，2009.
WANG Y N. The Research and Application of Genetic Algorithm [D]. Wuxi: Jiangnan University, 2009. (in Chinese)

[18] 张毅，代恩灿，罗元. 基于改进遗传算法的移动机器人路径规划[J]. 计算机测量与控制，2016，24(1)：313-316.
ZHANG Y, DAI E C, LUO Y. Mobile Robot Path Planning Based on Improved Genetic Algorithm[J]. Computer Measurement & Control, 2016, 24(1): 313-316. (in Chinese)

(编辑：徐楠楠)