拒止环境实现注入的GPS欺骗干扰

史 密，陈树新，吴 昊，毛 虎
(空军工程大学信息与导航学院，西安，710077)

摘要 为解决GPS欺骗干扰信号注入目标接收机效率不高的问题，设计了一种基于构建拒止环境掩护欺骗信号注入的GPS欺骗干扰模式。分析了拒止环境下信号载噪比变化情况，研究了该干扰模式欺骗信号的捕获和跟踪性能，并结合GPS信号和接收机参数的典型值，计算了为构建欺骗干扰所需的拒止环境不同干信比对应的带限白噪声信号功率，从欺骗信号的捕获和跟踪的角度证明了其可行性，该文最后给出了该模式的干信比和带限白噪声信号功率的一般性限定条件。

关键词 GPS欺骗干扰；拒止环境；信号注入；捕获跟踪
DOI 10.3969/j.issn.1009-3516.2015.06.006
中图分类号 TN972 **文献标志码** A **文章编号** 1009-3516(2015)06-0027-05

A GPS Spoofing Pattern Based on Denial Environment

SHI Mi, CHEN Shuxin, WU Hao, MAO Hu
(Information and Navigation College, Air Force Engineering University, Xi′an 710077, China)

Abstract: In order to cope with the problem of low efficiency of GPS spoofing-signal injection, a GPS spoofing pattern based on denial environment which covers for signal injection is proposed. With an analysis on exchange of signal carrier noise ratio, the acquisition and tracking of spoofing signal in this pattern is discussed. Given representative parameters of GPS signal and receiver, the preferential signal ratio of spoofing signal to authentic signal and power of band-limited white noise are calculated for the requirement of constructing denial environment. This jamming pattern is proved from the perspective of acquisition and tracking of spoofing signal, at last the general limit of signal ratio of spoofing signal to authentic signal and power of band-limited white noise are deduced.

Key words: GPS spoofing; denial environment; signal injection; acquisition and tracking

GPS干扰技术可以分为压制式干扰和欺骗式干扰两大类。随着诸如空时二维滤波、自适应天线等GPS抗干扰技术的普遍应用，成功压制目标接收机所需功率增加，大大降低了干扰效能[1-3]。与压制式干扰不同，而欺骗式干扰通过发射与GPS信号格式相同的虚假信号，待环路捕获跟踪之后，诱导目标接收机产生错误定位信息。该方法所需功率小、隐蔽性强，相对于单纯的压制干扰更加智能，是GPS干扰研究的热点方向。

目前国内针对欺骗式干扰的研究集中在转发式

收稿日期：2015-01-16
基金项目：国家自然科学基金资助项目(61273049)
作者简介：史 密(1991—)，男，河北保定人，硕士生，主要从事GPS干扰研究.E-mail:977953350@qq.com

引用格式：*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 Mi, CHEN Shuxin, WU Hao, et al. A GPS Spoofing Pattern Based on Denial Environment[J]. Journal of Air Force Engineering University: Natural Science Edition, 2015, 16(6): 27-31.*

欺骗方面,主要分析研究了转发式欺骗的区域映射问题、GPS 转发时延算法、转发时延对定位精度的影响和收发隔离问题等[4-5]。而在欺骗信号注入方面,目前,欺骗干扰主要采用“先压制后欺骗”的模式,以期接收机在搜索阶段捕获欺骗信号。然而,该模式在一般背景环境下接收机捕获真实信号和欺骗信号的概率相近[6],欺骗信号的功率优势得不到发挥,干扰效能不高。因此,结合传统的 GPS 干扰手段设计合理灵巧的欺骗干扰模式,以提高目标接收机对欺骗信号的捕获跟踪性能,对成功实施欺骗显得尤为重要。

1 拒止环境下的欺骗干扰模式

1.1 工作模式分析

欺骗过程中,接收机前端同时存在 GPS 真实信号和欺骗信号,并且在不加抑制的情况下(C/A 码标称最低接收功率相当于 45 dB·Hz 的载噪比),当搜索方格对齐真实信号的载波频率和码相位时,其载噪比可以使真实信号的捕获概率接近于 1。因此在欺骗过程中需压制 GPS 信号的注入能力。

基于拒止环境实现注入的 GPS 欺骗干扰,就是在向目标接收机转发欺骗信号的同时,辅助发射一定功率的带限白噪声(BLWN)干扰,从而构建拒止环境,掩护欺骗信号注入目标接收机。该干扰模式下,接收机前端同时存在 GPS 真实信号、转发欺骗信号和 BLWN 干扰信号。BLWN 干扰可以提高环境噪声基底,降低真实信号和欺骗信号的等效载噪比。此时,接收机捕获真实信号与欺骗信号的概率都有所下降,但真实信号捕获概率降低更快,因此相对提高了欺骗信号的捕获概率。由于欺骗信号功率高于真实信号功率,可调整 BLWN 干扰功率,使真实信号载噪比低于接收机锁相环(PLL)的跟踪门限,同时真实信号载噪比高于跟踪门限。

该干扰模式的主要优势在于两方面:一是,拒止环境对欺骗信号捕获概率的影响小于真实信号的影响,有利于捕获欺骗信号。一旦接收机捕获到欺骗信号,其载噪比满足跟踪条件,接收机转入对欺骗信号的跟踪状态;二是,即使接收机搜索捕获到真实信号,其载噪比不能满足信号跟踪,致使接收机再次进入搜索状态。因此,基于拒止环境实现注入的欺骗干扰模式有较高的成功率。

1.2 干扰系统组成

干扰系统由转发干扰器 R_i、BLWN 干扰源和主控站组成,见图 1。图中只显示了对一颗可见卫星的转发,实际工作中则根据具体需要确定转发卫星的数量和卫星序号。其中,转发干扰器接收并转发真实 GPS 信号 S_T 形成欺骗信号 S_F;BLWN 干扰源负责发射一定功率的 BLWN 干扰信号 S_J 以形成拒止环境;主控站负责协调干扰系统,包括控制干扰源位置、转发增益、转发时延以及 BLWN 功率等。

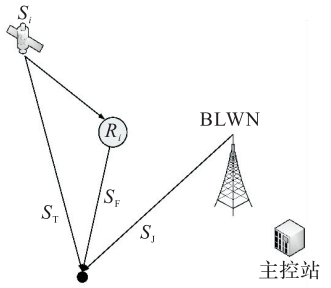

图 1 干扰系统示意图

Fig.1 The schematic diagram of GPS jamming system

2 可行性分析及参数设定

2.1 拒止环境下载噪比分析

GPS 接收机信号捕获和跟踪的性能取决于接收机中信号的载噪比和带宽。拒止环境下,真实信号与欺骗信号的等效载噪比降低。设到达接收机前端的 BLWN 干扰信号为:

$$J(t)=\sqrt{2C_J}n(t)\cos(2\pi ft+\theta) \tag{1}$$

式中:C_J 为 BLWN 干扰信号功率;$n(t)$ 为基带白噪声信号;f 为 GPS 载波频率;θ 干扰信号初始相位。下面分析由该干扰信号所构建的拒止环境下真实信号和欺骗信号的等效载噪比。

当受到 BLWN 干扰,接收机前端信号载噪比 C/N_0 与等效载噪比 $(C/N_0)_{eq}$ 的关系为[7]:

$$\frac{1}{(C/N_0)_{eq}}=\frac{1}{C/N_0}+\frac{C_J/C}{QR_c} \tag{2}$$

式中:C 为待捕获跟踪信号功率;R_c 为码速率;Q 为抗干扰品质因数,可近似表达为[8]153-300:

$$Q\approx B_n/R_c\int_{f-B_n/2}^{f+B_n/2}S(f)\mathrm{d}f \tag{3}$$

式中:B_n 为 BLWN 干扰信号带宽;$S(f)$ 为归一化到无穷带宽上的待捕获信号功率谱密度,由于转发欺骗信号与真实 GPS 信号格式相同,欺骗信号的功率谱密度以及码速率与真实信号的相等。考虑到 GPS 信号 90%以上功率集中在零点至零点主瓣带宽内,因此式(3)中选择零点至零点带宽作为 B_n。此时 $B_n/R_c=2$ 且 $\int_{f-B_n/2}^{f+B_n/2}S(f)\mathrm{d}f=0.9$,即 $Q=\frac{20}{9}$。

根据式(2)、(3)分别计算拒止环境下真实信号和欺骗信号的等效载噪比 $(C_T/N_0)_{eq}$、$(C_F/N_0)_{eq}$:

$$(C_T/N_0)_{eq}=20R_cC_T/(20R_cN_0+9C_J) \quad (4)$$

$$(C_F/N_0)_{eq}=20R_cC_F/(20R_cN_0+9C_J) \quad (5)$$

式中：C_T 为 GPS 真实信号功率；C_F 为转发欺骗信号功率；N_0 为 1 Hz 带宽内热噪声功率。欺骗信号与真实信号载噪比的相互影响也可以由式(2)和(3)式计算，但是由于此时 Q 值很大，当转发时延超过一个码元且干信比小于 30 dB 时，欺骗信号与真实信号间的相互影响可以忽略[9]。

可见，随着 C_J 的增大，$(C_T/N_0)_{eq}$ 和 $(C_F/N_0)_{eq}$ 逐渐变小，直至趋近于 0。因此，通过构建拒止环境，可以人为降低到达接收机的真实信号和欺骗信号的信号质量，为下一步欺骗信号的注入做好准备。

2.2　欺骗信号捕获性能分析

GPS 信号捕获就是在信号跟踪之前粗略确定可见卫星信号的载波频率和码相位。在每个搜索方格的滞留时间 T 期间，对 I 和 Q 信号进行积分和清零，并比较包络 $V=\sqrt{I^2+Q^2}$ 与门限来判定信号存在与否。当不存在卫星信号时，V 呈瑞利(Rayleigh)分布，通过对概率密度函数积分可以求得信号捕获虚警概率 P_{fa} 为[10]350-393：

$$P_{fa}=\int_{V_t}^{\infty}\frac{v}{\sigma_n^2}e^{-\frac{v^2}{2\sigma_n^2}}\mathrm{d}v \quad (6)$$

存在卫星信号时，V 呈莱斯分布，通过对概率密度函数积分可得信号检测概率 P_d 为：

$$P_d=\int_{V_t}^{\infty}\frac{v}{\sigma_n^2}e^{-\frac{v^2+a^2}{2\sigma_n^2}}I_0\left(\frac{va}{\sigma_n^2}\right)\mathrm{d}v \quad (7)$$

式中：V_t 为判决门限值；σ_n^2 表示 I 支路与 Q 支路上均值为零且互不相关的正态噪声功率；a^2 为信号相干积分后的功率；$I_0(\cdot)$ 为第 1 类零阶修正贝塞尔函数[11]。通常，信号捕获首先给定一个虚警概率 P_{fa}，根据式(6)计算门限值 $V_t=\sigma_n^2\sqrt{-2\ln P_{fa}}$，最后根据式(7)计算单次检验信号捕获概率。

由于 GPS 欺骗干扰，尤其是转发式欺骗干扰所用干扰信号格式与真实 GPS 信号格式相同，其欺骗信号很容易进入信号捕获电路，此时欺骗信号的捕获概率可根据式(7)推导计算。通过分析式(7)可知，在确定判定门限值 V_t 后，莱斯概率密度函数的积分值实际上是相干积分后信噪比(SNR) K 的函数。为简化下文推导，将噪声功率归一化处理即令 $\sigma_n^2=1$，设相干积分后真实信号 SNR 为 K_T；相干积分后欺骗信号 SNR 为 K_F。在不计基带数字信号处理损耗时，信号的载噪比、信噪比和相干积分时间的关系为[10]350-393：

$$(C/N_0)=K/T \quad (8)$$

并由式(4)、(5)得欺骗信号的 SNR 为：

$$K_F=MK_T \quad (9)$$

式中：M 为欺骗信号与真实信号的功率之比。

因此，欺骗干扰下接收机捕获真实信号概率 P_1 和捕获欺骗信号概率 P_2 可以分别表示为：

$$P_1=\int_{V_t}^{\infty}ve^{-\frac{v^2}{2}-K_T}I_0\left(\sqrt{2K_T}v\right)\mathrm{d}v \quad (10)$$

$$P_2=\int_{V_t}^{\infty}ve^{-\frac{v^2}{2}-MK_T}I_0\left(\sqrt{2MK_T}v\right)\mathrm{d}v \quad (11)$$

对于一般接收机认为 GPS 信号 C/N_0 小于 28 dB 为弱信号，大于 40 dB 时为强信号[10]350-393，噪声频谱功率密度典型值 N_0 为 −205 dBW/Hz。设相干积分时间 T 为 10 ms，P_{fa} 为 1%，根据式(8)、(10)计算真实信号捕获概率，其中典型载噪比值对应的捕获概率由表 1 给出。

表 1　典型载噪比下 GPS 信号捕获概率

Tab.1　Acquisition probability of GPS signal under representative CNR

$(C/N_0)_{eq}$ /dB	26	28	29	30	32	34	40	45
K /dB	6	8	9	10	12	14	20	25
P_1/%	47.86	74.27	85.72	93.66	99.29	99.77	99.97	99.99

从表中可以看出，随载噪比增加，捕获概率非线性增加，对于强信号而言，其捕获概率接近于 1，可以认为当搜索方格对齐真实信号的载波频率和码相位时，即可对其捕获。因此，通过 BLWN 干扰降低等效载噪比，可以同时降低 P_1 和 P_2 的值，且 P_1 下降较快，以减少很小的 P_2 为代价提高欺骗信号的相对捕获概率(接收机监测到信号时，该信号为欺骗信号的概率)。欺骗信号相对捕获概率表达式为：

$$P=bP_2/(aP_1+bP_2) \quad (12)$$

式中：a 为信号搜索算法的搜索单元对齐真实信号的概率；b 为信号搜索算法的搜索单元对齐欺骗信号的概率。对于处于搜索状态的民用 GPS 接收机，通常采用线性搜索 C/A 码的方法，而对于处于搜索状态的军用接收机，一般也是首先搜索 C/A 码进而引导 P(Y)码捕获。因此可以认为(12)式中 $a=b$。下面以 P 为衡量标准分析欺骗信号捕获性能。

当 C_T 为 −160 dBW；R_c 为 1.023 MHz；相干积分时间 T 为 10 ms；虚警概率 P_{fa} 为 1%；噪声频谱功率密度典型值 N_0 为 −205 dBW/Hz；为防止欺骗信号功率过大而被接收机抗干扰措施识别，仿真 4

种干信比情况，M 分别取 2、5、10 和 20 倍，即 3 dB、7 dB、10 dB 和 13 dB。在不同干信比下 P 与 $(C_T/N_0)_{eq}$ 曲线见图 2。

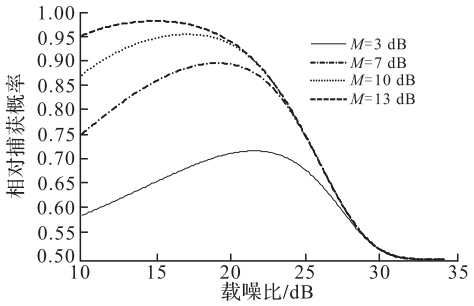

图 2 相对捕获概率与载噪比的关系

Fig.2 The relationship between relative acquisition probability and CNR

从图 2 可见，在相同 $(C_T/N_0)_{eq}$ 下，P 值随 M 增加而增加；在不同 M 下存在最佳等效载噪比使 P 取最大值，该载噪比记为 $(C_T/N_0)_{eq,M}$，且 $(C_T/N_0)_{eq,M}$ 是 M 的一元函数，表示为：

$$(C_T/N_0)_{eq,M}=f(M) \tag{13}$$

$(C_T/N_0)_{eq,M}$ 是 P 曲线的极大值点，对式(12)求导并令导数为 0，得 $P_1'P_2=P_1P_2'$，由于该式求解过于复杂，实际应用中可从图 2 程序的仿真结果中寻找 P 的最大值点，其对应的横坐标即 $(C_T/N_0)_{eq,M}$，利用式(4)计算为达到该载噪比所需的带限白噪声信号功率 C_J，所得结果见表 2。

表 2 不同干信比下最佳等效载噪比

Tab.2 Preferential equivalent CNR under different JSR

M /dB	3	7	10	13
$(C_T/N_0)_{eq,M}$ /dB	21.4	19.0	17.0	14.9
C_J /dBW	−117.85	−115.44	−113.44	−111.34
P /%	71.29	88.42	94.04	96.63

可见，基于拒止环境实现注入的欺骗干扰，一方面可适当提高干信比 M，进而提高 P 值；另一方面 BLWN 干扰可以降低 $(C_T/N_0)_{eq}$ 至 $(C_T/N_0)_{eq,M}$，进而使 P 取到最大值。当干信比 13 dB 等效载噪比 14.9 dB 的时侯，欺骗信号相对捕获概率可以达到 96.63%。因此，该干扰模式具有很高的欺骗信号捕获性能。

2.3 欺骗信号跟踪性能分析

当接收机搜索到某颗卫星的真实信号或是欺骗信号时，相应的接收通道就从捕获阶段进入跟踪阶段。PLL 跟踪误差的 3 倍标准差 $3\sigma_{PLL}$ 必须小于 PLL 鉴相器相位牵引范围的 1/4，载波环才会锁定信号[7]，其中 σ_{PLL} 与信号载噪比有关。载波上调制有数据且使用二象限反正切相位鉴别器时，信号跟踪门限满足[8]：

$$\sigma_{PLL}=\sqrt{\sigma_{tPLL}^2+\sigma_v^2+\theta_A^2}+\frac{\theta_e}{3}=15^\circ \tag{14}$$

式中：σ_{tPLL} 为 1σ 热噪声；σ_v 为 1σ 由振动引起的振荡器颤动，这里取 1.42°；θ_A 为阿仑偏差引起的振荡器颤动；θ_e 为动态应力误差，对于 10 Hz 的 2 阶 PLLθ_e 为 14.3°[7]。σ_{tPLL} 与 θ_A 的计算公式为：

$$\sigma_{tPLL}=\frac{360^\circ}{2\pi}\sqrt{\frac{B_L}{(C/N_0)_{eq}}\left[1+\frac{1}{2T(C/N_0)_{eq}}\right]} \tag{15}$$

$$\sigma_A=360^\circ fT\sigma_A(\tau) \tag{16}$$

式中：B_L 为载波环噪声带宽；$\sigma_A(\tau)$ 为短期阿仑标准差。

当 B_L 为 10 Hz；T 仍取 10 ms；$\sigma_A(\tau)$ 取 10^{-10}；f 取 GPS L1 载波频率 1 575.42 MHz。通过仿真，2 阶载波环 PLL 跟踪误差标准差与等效载噪比关系见图 3。

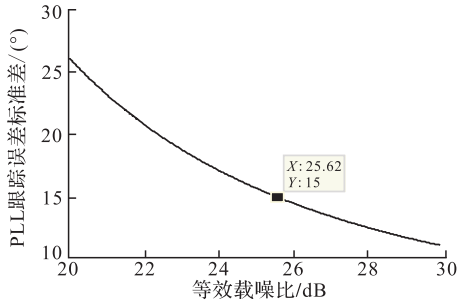

图 3 PLL 跟踪误差标准差与等效载噪比关系

Fig.3 The relationship between standard deviation of tracking error and CNR of PLL

可见，以上条件下 PLL 跟踪门限为 25.62 dB。为达到真实信号失锁、欺骗信号跟踪，真实信号等效载噪比应满足不等式：

$$(C_T/N_0)_{eq}\leqslant(C/N_0)_{Th}\leqslant(C_F/N_0)_{qe} \tag{17}$$

式中：$(C/N_0)_{Th}$ 为 PLL 跟踪载噪比门限。即拒止环境下真实信号等效载噪比小于 25.62 dB，且欺骗信号等效载噪比大于 25.62 dB 时，更有利于欺骗信号的跟踪。在 2.2 节中设置的 4 种干信比中，M 取 7 dB、10 dB 和 13 dB 时可满足上述要求，欺骗信号等效载噪比分别为 26.0 dB、27.0 dB 和 27.9 dB，且 M 越大，越易满足载噪比门限要求。

因此，基于拒止环境实现注入的欺骗模式，通过构建拒止环境压制 $(C/N_0)_{eq}$，使真实信号等效载噪比低于跟踪门限；同时在压制下，欺骗信号等效载噪比仍高于跟踪门限。这样的限定更有利于欺骗信号的跟踪。

以上为提高欺骗信号捕获跟踪性能所计算的参数(干信比、BLWN 功率)是在给定具体情况下得出的。结合式(4)、(13)和(17)，可将该模式 BLWN 干扰功率以及干信比限定条件一般化，即：

$$\begin{cases} C_J = \dfrac{20R_c[C_T - N_0 f(M)]}{9f(M)} \\ f(M) \leqslant (C/N_0)_{Th} \leqslant Mf(M) \end{cases} \tag{18}$$

3　结语

通过拒止环境实现注入的欺骗干扰模式，需要 BLWN 干扰与转发增益协同工作，两者配合将接收机前端的等效载噪比限定在一定范围内。在该范围内，虽然欺骗信号捕获概率和真实信号捕获概率较未施加拒止时都有所降低，但是由于欺骗信号捕获概率下降幅度更大，因此拒止环境提高了欺骗信号的相对捕获概率。其次，合理设置的拒止环境可以致使真实信号即使被捕获也不能满足信号跟踪条件，并且欺骗信号仍满足跟踪条件。因此该模式具有一定的可行性，其中干信比与带限白噪声干扰功率的设置则需要根据实际情况计算得出，在工程实现中的一些问题和解决问题的方法，有待于下一步研究。

参考文献(References)：

[1] 石斌斌，程翥，钱林杰，等.基于循环平稳的级联空时 GPS 抗干扰方法[J]. 西安电子科技大学学报，2010，37(4)：743-749.
SHI Binbin，CHENG Zhu，QIAN Linjie，et al. Cyclostationarity Based Cascaded Space-Time Anti-Jamming Processor Designed to Appeal to GPS Receivers [J]. Journal of Xidian University，2010，37(4)：743-749. (in Chinese)

[2] 刘海波，吴德伟，董成喜，等.GPS 抗干扰技术发展趋势[J].火力与指挥控制，2011，33(1)：1-4.
LIU Haibo，WU Dewei，DONG Chengxi，et al. Development Trend of GPS Anti-Jamming Technique [J]. Fire Control & Command Control，2011，33(1)：1-4. (in Chinese)

[3] 潘延明，卢艳娥，骆艳卜，等.稳健的 GPS 干扰抑制方案研究[J]. 重庆邮电大学学报：自然科学版，2012，24(3)：330-334.
PAN Yanming，LU Yan′e，LUO Yanbo，et al. A Research of Robust GPS Anti-Jamming Scheme [J]. Journal of Chongqing University of Posts and Telecommunications：Natural Science Edition，2012，24(3)：330-334. (in Chinese)

[4] 杨景曙，曾芳玲，盛琥，等.通过区域映射实现诱导的 GPS 干扰系统[J]. 电子学报，2005，33(6)：1036-1038.
YANG Jingshu，ZENG Fangling，SHENG Hu，et al. A Jamming System Through Section Mapping for GPS Navigation [J]. Acta Electronica Sinica，2005，33(6)：1036-1038. (in Chinese)

[5] 闫占杰，吴德伟，刘海波，等. GPS 转发欺骗式干扰时延分析[J]. 空军工程大学学报：自然科学版，2013，14(4)：68-70.
YAN Zhanjie，WU Dewei，LI Haibo，et al. Analysis of Time-Delay in GPS Repeater Deception Jamming [J]. Journal of Air Force Engineering University：Natural Science Edition，2013，14(4)：68-70. (in Chinese)

[6] 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 Yanbin，SU Wuxing，YAN Shusheng. Effectiveness Analysis of Repeater Deception Jamming Signal upon GPS Receiver[J]. Journal of Air Force Radar Academy，2004，18(4)：4-6.(in Chinese)

[7] Ward P W. GPS Receiver RF Interference Monitoring，Mitigation，and Analysis Techniques[J]. Journal of Navigation，1994，41(4)：367-391.

[8] Elliiott D. Kaplan，Christopher J Hegarty. Understanding GPS：Principles and Applications[M]. Boston Artech House，2006.

[9] Humphreys T E，Ledvina B M，Psiaki M L. Assessing the Spoofing Threat：Development of a Portable GPS Civilian Spoofer [C]//ION GNSS，Georgia，USA，September 16～19，2008.

[10] 谢钢.GPS 原理与接收机设计[M]. 北京：电子工业出版社，2011.
XIE Gang. Principles of GPS and Receiver Design [M]. Beijing：Publishing House of Electronics Industry，2011.(in Chinese)

[11] DING Yong，LI Ran. An Integral Estimate of Bessel Function and Its Application [J]. Science in China (Series A：Mathematics)，2008，51(5)：879-906.

(编辑：姚树峰)