

伪卫星信号的生成与应用研究*

王凯迪^{1,2}, 曹新亮^{1,2}

(1. 延安大学 物理与电子信息学院, 陕西 延安 716000;

2. 陕西省能源大数据实验室, 陕西 延安 716000)

摘要: 北斗 B1I 信号作为公开服务信号, 在全球范围内被广泛应用, 为了避免北斗信号被不正当使用, 需要对特定地区的特定卫星信号实施干扰。从生成式干扰角度出发提出了一种基于 Quartus II 平台, 以 Verilog 为硬件描述语言的北斗伪卫星 (B1I) 信号产生方法, 并对此伪卫星信号进行仿真测试, 结果显示: 伪信号使接收机三维定位产生显著偏差 ($X: -9.35 \times 10^4$ m、 $Y: +8.69 \times 10^5$ m、 $Z: +4.81 \times 10^5$ m), 钟差估计值从 -9.1 ms 变为 -1.7 μ s, 这为卫星导航欺骗干扰提供了有效的技术实现方法。

关键词: 卫星导航; 导航电文; 信号生成; 欺骗干扰; 可编程逻辑器件

中图分类号: V11; TN96

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.10.010

引用格式: 王凯迪, 曹新亮. 伪卫星信号的生成与应用研究 [J]. 网络安全与数据治理, 2025, 44(10): 59-65, 74.

The generation and application research of pseudo-satellite signals

Wang Kaidi^{1,2}, Cao Xinliang^{1,2}

(1. School of Physics and Electronics Information, Yan'an University, Yan'an 716000, China;

2. Shaanxi Province Energy Big Data Laboratory, Yan'an 716000, China)

Abstract: The Beidou B1I signal, as a public service signal, is widely used around the world. To prevent the improper use of Beidou signals, it is necessary to implement interference on specific satellite signals in specific regions. This paper proposes a method for generating Beidou pseudo-satellite (B1I) signals based on the Quartus II platform using Verilog as the hardware description language from the perspective of generative interference. A simulation test of this pseudo-satellite signal is conducted, and the results show that the pseudo signal causes significant deviation ($X: -9.35 \times 10^4$ m, $Y: +8.69 \times 10^5$ m, $Z: +4.81 \times 10^5$ m) in 3D positioning of the receiver, and the clock difference estimate changes from -9.1 ms to -1.7 μ s, which provides an effective technical implementation method for satellite navigation spoofing.

Key words: satellite navigation; navigation message; signal generation; spoofing interference; FPGA

0 引言

随着全球导航卫星系统 (Global Navigation Satellite System, GNSS) 的广泛应用, 伪卫星信号作为一种地面发射的模拟卫星信号, 它在导航欺骗干扰方面, 通过生成伪卫星信号, 可以对接收机产生误导, 进而拉偏其定位, 这在军事和安全领域具有重要的研究意义。现有的信号欺骗技术主要包括转发式欺骗和生成式欺骗^[1]。转发式欺骗通常是通过捕获真实卫星信号, 然后经过一定的处理后再发射给目标接收机, 这种方式虽然简单有效,

但容易被现代防欺骗技术检测到, 因为捕获和转发的过程不可避免地产生信号延迟及其他可感知的特征^[2-3]。相比之下, 生成式欺骗通过计算和合成生成与真实信号几乎无差的虚假信号, 从而更具隐蔽性^[4-5]。

目前, 国内外学者在伪随机信号生成及其抗欺骗检测方面展开了多方面的研究。传统伪随机序列 (如 m 序列、Gold 码) 由于可预测性强, 易被逆向分析, 为提高信号的不可预测性和抗欺骗能力, 文献 [6] 提出了一种基于混沌映射的伪随机序列生成方法, 通过非线性动力学系统增强序列复杂度, 有效提高了信号的抗分析能力; 文献 [7] 从硬件加速角度出发, 设计了基于现场可编程门阵列 (Field Programmable Gate Array, FPGA) 的并行

* 基金项目: 国家自然科学基金专项 (62141107); 延安大学研究生实践创新计划项目 (YSJ2025021)

线性反馈移位寄存器 (Linear Feedback Shift Register, LFSR) 优化结构, 通过动态反馈系数调整, 使伪随机序列的周期和随机性显著提升。文献 [8] 研究了高速伪随机数发生器的并行架构, 通过优化 LFSR 的反馈多项式, 在保证高随机性的同时, 降低了硬件资源消耗; 文献 [9] 则提出了一种基于物理不可克隆函数 (Physical Unclonable Function, PUF) 的随机种子生成方法, 结合 FPGA 的硬件熵源, 使生成的伪随机信号更接近真实噪声特性, 进一步增强了抗逆向分析能力。当前研究在伪随机信号生成优化、欺骗检测增强和 FPGA 硬件加速等方面取得了显著进展, 但仍需在信号动态可重构性等方面进一步探索, 以提高北斗民用信号的防御能力。

本文针对信号动态可重构性存在问题, 提出了一种基于 FPGA、以 Verilog 硬件描述语言为主要编程语言工具的北斗 B1I 伪卫星信号生成方法。通过使用 Modelsim 和 Quartus II 等 EDA 工具对所生成的信号进行仿真测试, 验证了信号的结构和携带信息的有效性。

1 B1I 信号结构及生成方法

1.1 B1I 信号结构及测距码特性

北斗 B1I 信号由测距码和导航电文一起调制在载波上生成^[10], 其信号表达式如式 (1):

$$S_{B1I}^j(t) = A_{B1I} C_{B1I}^j(t) D_{B1I}^j \cos(2\pi f_1 t + \varphi_{B1I}^j) \quad (1)$$

式中的 j 表示卫星的编号; A_{B1I} 表示信号的振幅; C_{B1I} 表示信号的测距码; D_{B1I} 表示调制在载波上面的数据码, 也就是导航电文; f_1 表示信号的载波频率; φ_{B1I} 表示信号的载波相位。

B1I 信号的测距码 (C_{B1I}) 的码速率为 2.046 Mcps, 码长为 2 046, 由线性序列 $G1$ 和 $G2$ 模二加产生平衡 Gold 后截短最后一码片生成^[11], 而 $G1$ 和 $G2$ 序列分别由 11 级线性移位寄存器生成, 其生成多项式分别为:

$$G_1(x) = 1 + X + X^7 + X^8 + X^9 + X^{10} + X^{11}$$

$$G_2(x) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^8 + X^9 + X^{11}$$

$G1$ 和 $G2$ 的初始相位为:

$G1$: 01010101010

$G2$: 01010101010

C_{B1I} 码发生器如图 1 所示。

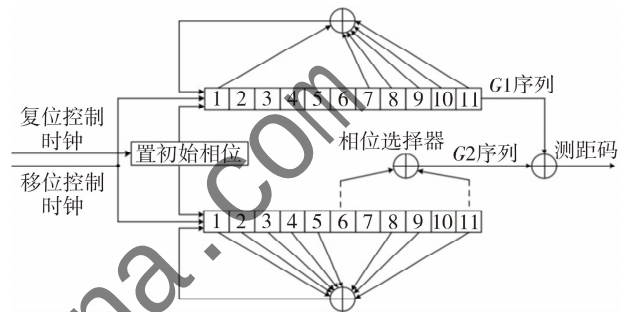


图 1 C_{B1I} 码发生器示意图

通过对产生 $G2$ 序列的移位寄存器不同抽头的模二加可以实现 $G2$ 序列相位的不同偏移, 然后与 $G1$ 序列模二加后可以生成不同卫星的测距码, 如图 1 所示为 6 号抽头和 11 号抽头进行模二加, 其所生成的测距码为编号 11 的测距码。表 1 是 $G2$ 序列不同相位分配表。

表 1 C_{B1I} 码的 $G2$ 序列相位关系表

PRN	卫星类型	C_{B1I} 编号	序列抽头	PRN	卫星类型	C_{B1I} 编号	序列抽头
1	GEO	1	1 $\oplus$ 3	21	MEO/IGSO	21	4 $\oplus$ 10
2	GEO	2	1 $\oplus$ 4	22	MEO/IGSO	22	4 $\oplus$ 11
3	GEO	3	1 $\oplus$ 5	23	MEO/IGSO	23	5 $\oplus$ 6
4	GEO	4	1 $\oplus$ 6	24	MEO/IGSO	24	5 $\oplus$ 8
5	GEO	5	1 $\oplus$ 8	25	MEO/IGSO	25	5 $\oplus$ 9
6	MEO/IGSO	6	1 $\oplus$ 9	26	MEO/IGSO	26	5 $\oplus$ 10
7	MEO/IGSO	7	1 $\oplus$ 10	27	MEO/IGSO	27	5 $\oplus$ 11
8	MEO/IGSO	8	1 $\oplus$ 11	28	MEO/IGSO	28	6 $\oplus$ 8
9	MEO/IGSO	9	2 $\oplus$ 7	29	MEO/IGSO	29	6 $\oplus$ 9
10	MEO/IGSO	10	3 $\oplus$ 4	30	MEO/IGSO	30	6 $\oplus$ 10
11	MEO/IGSO	11	3 $\oplus$ 5	31	MEO/IGSO	31	6 $\oplus$ 11
12	MEO/IGSO	12	3 $\oplus$ 6	32	MEO/IGSO	32	8 $\oplus$ 9
13	MEO/IGSO	13	3 $\oplus$ 8	33	MEO/IGSO	33	8 $\oplus$ 10
14	MEO/IGSO	14	3 $\oplus$ 9	34	MEO/IGSO	34	8 $\oplus$ 11
15	MEO/IGSO	15	3 $\oplus$ 10	35	MEO/IGSO	35	9 $\oplus$ 10
16	MEO/IGSO	16	3 $\oplus$ 11	36	MEO/IGSO	36	9 $\oplus$ 11
17	MEO/IGSO	17	4 $\oplus$ 5	37	MEO/IGSO	37	10 $\oplus$ 11
18	MEO/IGSO	18	4 $\oplus$ 6				
19	MEO/IGSO	19	4 $\oplus$ 8				
20	MEO/IGSO	20	4 $\oplus$ 9				

1.2 设计环境

在开发伪卫星信号的过程中，主要用到了 MATLAB、Quartus II、Modelsim 等开发软件，在软件开发平台上可以按照要求对信号的关键程序进行仿真分析、程序调试等，在程序开发完成后使用 Quartus II 将程序烧录入硬件板卡。

本设计的编程和程序运行均使用 Quartus II 软件进行，开发板选择 Cyclone IV GX 系列的 EP4CGX150DF31C7，代码编辑工具为 Notepad ++，该工具非常便捷且适用于 Verilog 语言的编辑。将数据码、导航电文、载波等部分程序在 Quartus II 中编译，通过后，再用 Modelsim 进行所有程序整合的仿真验证，产生伪卫星随机信号和导航电文原始信息。

Modelsim 中导出的导航电文为原始星历数据，用 MATLAB 将其转化为对应的十进制数，再乘以北斗官方文件给出的比例因子求解出伪卫星的星历信息，然后，通过位置解算公式求解出伪卫星定位接收机结果，进而获得其与实际位置的误差。

1.3 载波生成模块

载波生成的总体思路是通过 DDS 信号发生器来实现可调节相位、幅度和频率的余弦载波。首先，利用 MATLAB 生成一个余弦波的查找表，将该查找表存入 FPGA 的 ROMIP 核中，IP 核深度设置为 1 024，通过调用 IP 核将余弦波的波形通过 FPGA 输出。波形的频率、相位、幅度通过程序编码设计中的频率控制字、相位控制字和幅度控制字来控制。频率控制通过将查找表中的值进行抽取，从而实现倍频的效果，在代码编辑中一共给出了 7

个倍数。相位控制则是将相位控制字给出的初始相位存入相位累加器的寄存器中。然后，通过时钟信号将频率控制字送入相位累加器进行累加，幅度控制由幅度控制字与 ROM 实例输出的原始余弦波进行相乘得到，便实现了载波可调节。分别改变相位频率，在 Modelsim 中改变前后信号进行仿真和对比，波形如图 2 所示。

1.4 测距码生成模块

测距码是由 2 个 11 阶线性移位寄存器按照对应的生成多项式去移位^[12]，并且，根据不同抽头的模二加最后生成一位测距码，测距码一共有 2 046 位，在代码中加入计数器，并且使用 parameter 语句控制计数器的最大值为 2 046。该模块输出由时钟信号、复位信号、卫星编号控制字一起控制，北斗 B1I 播发在 MEO/IGSO 卫星上，通过前面提到的抽头关系表提前在代码中编写 5 ~ 37 号卫星不同抽头的异或，再通过编号控制字控制不同编号卫星所对应的不同测距码。图 3 为测距码 Modelsim 仿真图，其中抽头设置为 4 和 6，在编码中 Q_sel 对应的是寄存器 $g_2[4]$ 和寄存器 $g_2[6]$ 。

1.5 导航电文生成模块

根据前述的导航电文结构，在设计生成导航电文时，采用由下向上的设计思想，先从字 1 ~ 10 开始，字 1 的结构和其他 9 个字的结构是不同的，它包含了 11 bit 的同步码 11100010010，这是接收电文必不可少的一部分，因为接收机在接收电文之前会先确认搜索到同步码，完成子帧同步后开始正式接收。第一个字的 11 bit 同步码之后跟随的是 4 bit 的保留信息、3 bit 的子帧号和高 8 位的周内秒计数（SOW），加上 4 bit 的校验码，这些共同组成字 1。

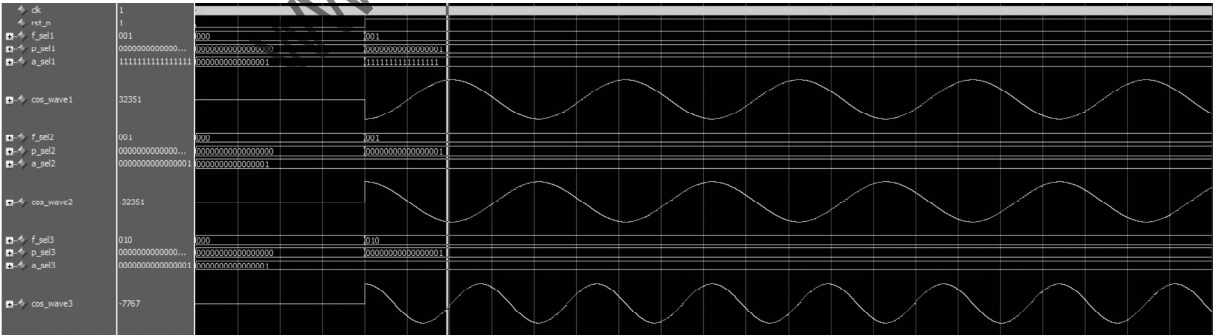


图 2 载波仿真

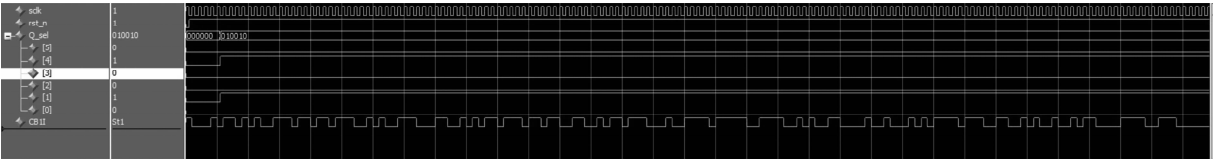


图 3 测距码仿真

子帧号也是通过计数器，每生成 10 个字子帧号就会加 1，一直到完成一段超帧后归零。

字 2~10 和字 1 不同的是没有同步码, 并且在 BCH 编码的时候有 8 bit 的校验码和 22 bit 的电文信息。在生成字 2~10 时, 使用 Verilog 编写伯努利二进制随机信号发生器, 先产生一段 22 bit 的随机信号, 将这段信息进行串并处理, 得到两个并行的 11 bit 序列, 通过 BCH 编码器对这两段序列进行编码, 产生两段 15 bit 的序列, 最后, 进行串并处理得到导航电文的字 2~10。

生成 10 个字后在子帧的生成过程中例化字 1 ~ 10, 组成一个完整的子帧, 再通过例化子帧实现一段完整的帧, 层层例化最终实现一个完整的超帧。图 4 为 Modelsim 的仿真结果。

1.6 整体信号的实现

信号整体的产生由载波、测距码和导航电文三部分组成，在这之前要对导航电文进行编码处理，再使用

BPSK 调制, 将其调制到载波上输出^[13]。

导航电文需要在 BCH 编码的基础上进行二次编码, 将拥有固定周期的 NH 码 00000100110101001110 使用 Verilog 编码存储到寄存器中, 再和电文的一个 bit 进行模二加, 扩频码一个周期对应 1 bit 的 NH 码, 一周期的扩频码和 1 bit 的 NH 码进行模二加, 最后, 输出的电文就是调制到载波上的电文。

将测距码和导航电文调制到载波上通过 Quartus II 综合布局布线产生的 RTL 电路, 如图 5 所示。

图 5 中, o_bli_1 为测距码输出; o_bli_2 为导航电文输出, 30 位为一个字直到产生完整的超帧停止; $o_carrier$ 是 DDS 信号发生器产生的余弦载波; o_BII 是载波、测距码和导航电文进行 BPSK 调制之后的最终信号。

代码编译通过之后使用 Modelsim 仿真, 观察到的信号如图 6 所示。

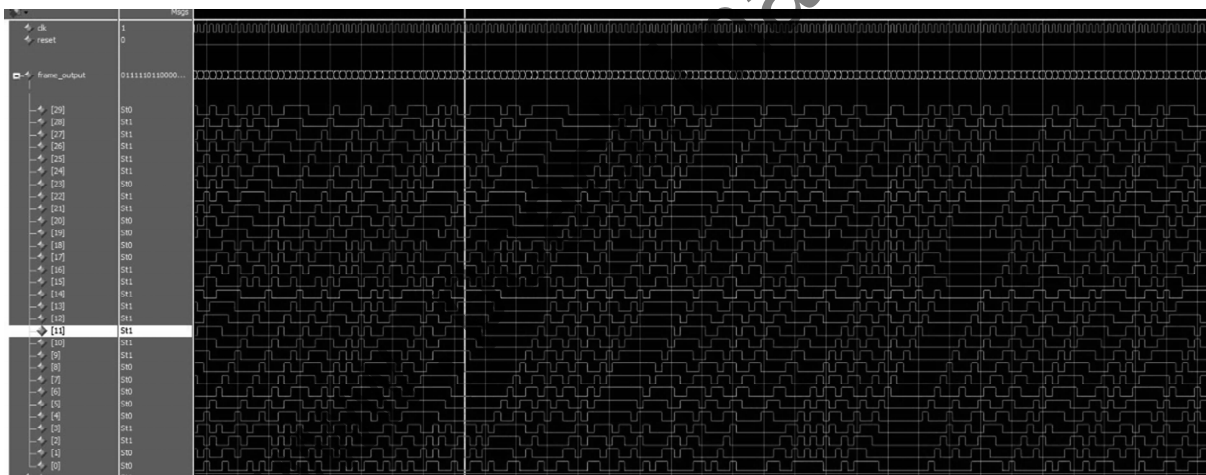


图4 导航电文仿真

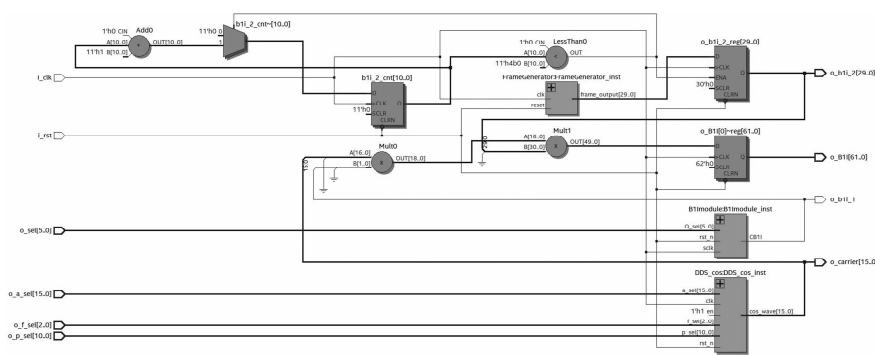


图 5 B1I 信号 RTL 电路图

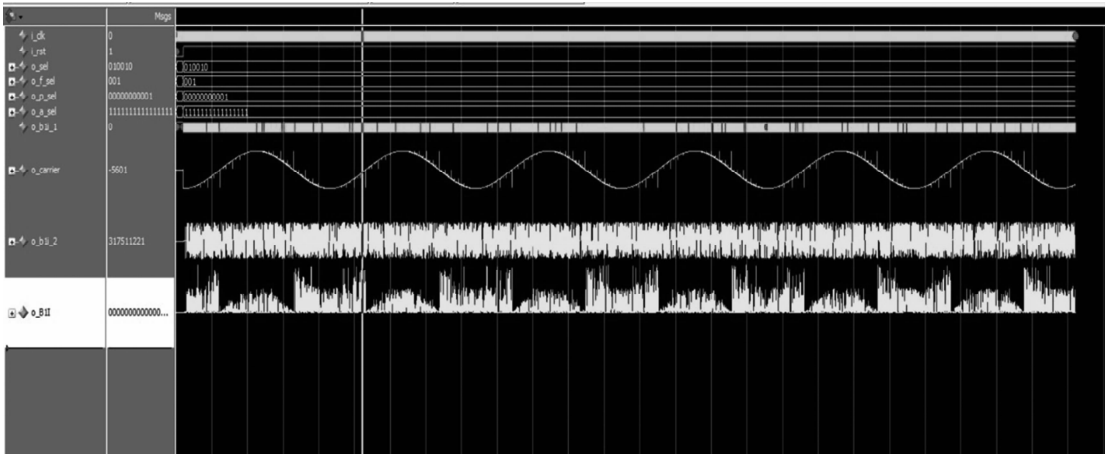


图6 B1I信号波形仿真图

2 干扰性能测试

2.1 卫星星历解算

欺骗信号在进入接收机环路之前一直保持低功率运行，当其成功进入接收机的跟踪环路之后，改变信号的幅值，使其码相位和载波相位都发生改变，从而实施定位信息篡改；当接收机开始解算伪卫星信号的时候，测试伪卫星携带的导航信息对接收机定位和授时的影响。

测试的主要方法是通过 Modelsim 将产生的导航电文原始数据打印出来，通过 MATLAB 程序和北斗实验室给出的星历对应的比例因子计算出原始数据中携带的星历信息，通过星历信息解算出伪卫星的空间位置，将接收机接收到的 IGSO 卫星编号找到并代入伪卫星的位置数据，解算出接收机的位置，观察接收机位置差异和钟差的变化。

从 1 220 ns 开始复位信号为高电平，程序开始运行，

B1I 信号逐渐输出。首先进行同步码的同步，同步完成后将原始数据导入 MATLAB 提取出携带星历信息的原始数据，如图 7 所示。

导出原始数据有原码和补码两种形式，需要将补码转变为原码，再统一转化为十进制，并乘以对应的比例因子得到伪卫星星历信息计算结果，如图 8 所示。

2.2 卫星位置解算

根据伪卫星的星历信息计算其在地心地固直角坐标系（China Geodetic Coordinate System 2000，CGCS2000）中的坐标^[14]。主要对归化时间、卫星平均运动速率、发射时刻的平近点角、偏近点角、真近点角、纬度幅角、摄动校正项、校正后的纬度幅角、轨道平面坐标、升交点经度和卫星在 CGCS2000 坐标系中的坐标进行计算，最终得到伪卫星坐标点。

GNSS Navigation Message Parameters			
Parameter	Bits (Hex)	Parameter	Bits (Hex)
1. Toa	0110 1100 0001 10110 (0x10C180)	Omega_0	0001 1001 0110 1010 0101 1010 1000 1101 (0x196A5ABD)
2. sqrt(A)	1100 1010 1110 1011 0010 1110 1111 (0xCAEB22DF)	Omega_dot	1111 1111 1110 1100 1010 0000 0 (0x1FFD940)
3. e	0000 0001 1000 1001 1000 1010 1010 1010 (0x0189380A)	I_0	0111 1010 1100 1100 1110 1011 1000 1111 (0x7ACCEB8F)
4. omega	1010 1111 1110 0111 1100 1001 0100 1000 (0xAFC7C948)	IDOT	1101 1110 1101 01 (0x1BDA)
5. Delta n	0000 1000 0101 1101 (0x0954)	C_uc	1111 1101 0001 1111 11 (0x1FD1FC)
6. M_0	1011 0001 1111 0100 0100 1010 1100 0111 (0xB1F44AC7)	C_us	0011 1011 1100 1001 00 (0x0EBC90)
7. C_(rc)	1110 1001 1111 1001 00 (0x1D3F50)	C_(re)	1111 1011 1101 1100 10 (0x1F7B72)
8. C_(ic)	0000 0001 0000 0100 10 (0x00412)	C_(is)	1111 1111 0010 1101 00 (0x1FF2D0)

图7 伪卫星星历原始数据

伪卫星星历参数 (Pseudo-Satellite Ephemeris)			
参数	数值与单位	参数	数值与单位
T_oe	447800 s	\Omega_0	0.19855815778 rad
\sqrt{a}	6493.3920269 m^{1/2}	\dot{\Omega}	-1.12777343019843 \times 10^{-4} rad/s
e	0.003000022145	I_0	0.95937866671 rad
\omega	-3.2514778897 rad	IDOT	-2.41357156482991 \times 10^{-4} rad
\Delta n	2.4340351956198 \times 10^{-5} 1/s	C_uc	-1.37137249112129 \times 10^{-4} rad
M_0	-0.60973229678 rad	C_us	2.8507784009 \times 10^{-5} rad
C_(rc)	-352.4375 m	C_(re)	-66.21875 m
C_(ic)	4.85219061374664 \times 10^{-4} m	C_(is)	-3.93018126487732 \times 10^{-4} m

注: T_oe - 星历参考时刻; \sqrt{a} - 轨道半长轴的平方根; 所有角度参数单位为弧度(rad), 时间参数单位为秒(s)

图8 伪卫星星历信息

(1) 计算归化时间, 通过卫星星历中的参考时间 T_{oe} 和 t 时刻值的差异, 解算出各个轨道参数在 t 时刻的值, 具体计算如式 (2) 所示:

$$t_k = t - T_{oe} \quad (2)$$

(2) 纠正后的卫星平均运动角速率用 n 表示, 如式 (3) 所示:

$$n = \sqrt{\frac{\mu}{A^3}} + \Delta n \quad (3)$$

其中, A 为卫星轨道长半轴, μ 为 CGCS2000 坐标系下的地球引力常数, 其值为: $\mu = 3.986\ 004\ 418 \times 10^{14} \text{ m}^3/\text{s}^2$ 。

(3) 信号发射时刻的平近点角用 M_k 表示, 将星历中的 M_0 代入式 (4) 线性模型中求解。

$$M_k = M_0 + nt_k \quad (4)$$

(4) 信号发射时刻的偏近点角用 E_k 表示, 根据星历中的 M_k 和 e 采用迭代法计算偏近点角。 E_k 的迭代初始值 E_0 可以设置为 M_k , 如式 (5) 所示:

$$\begin{cases} E_0 = M_k \\ E_{k+1} = M_k + e \sin E_k \end{cases} \quad (5)$$

当 E_k 前后两次的计算值小于预先设置的阈值 10^{-13} 时, 结束迭代输出精确解。

(5) 信号发射时刻的真近点角用 v_k 表示, 借由 E_k 和星历中的 e 来计算, 如式 (6) 所示:

$$\begin{cases} \sin v_k = \frac{\sqrt{1-e^2} \sin E_k}{1 - e \cos E_k} \\ \cos v_k = \frac{\cos E_k - e}{1 - e \cos E_k} \\ v_k = \arctan \frac{\sqrt{1-e^2} \sin E_k}{\cos E_k - e} \end{cases} \quad (6)$$

(6) 信号发射时刻的纬度幅角用 φ_k 表示, 根据求解出的真近点角 v_k 和星历中的 ω 来计算纬度幅角:

$$\varphi_k = v_k + \omega \quad (7)$$

(7) 信号发射时刻的摄动校正项分为纬度幅角改正项 δu_k 、地心距改正项 δr_k 、轨道倾角改正项 δi_k , 利用解算出的纬度幅角 φ_k 和星历参数中的 C_{uc} 、 C_{us} 、 C_{rc} 、 C_{rs} 、 C_{ic} 、 C_{is} 来计算, 如式 (8):

$$\begin{cases} \delta u_k = C_{us} \sin(2\varphi_k) + C_{uc} \cos(2\varphi_k) \\ \delta r_k = C_{rs} \sin(2\varphi_k) + C_{rc} \cos(2\varphi_k) \\ \delta i_k = C_{is} \sin(2\varphi_k) + C_{ic} \cos(2\varphi_k) \end{cases} \quad (8)$$

(8) 计算摄动校正后的纬度幅角 u_k 、卫星地心距 r_k 、轨道倾角 i_k , 将上一步得到的纬度幅角改正项 δu_k 、地心距改正项 δr_k 、轨道倾角改正项 δi_k 和星历参数中的 i 代入式 (9)~(11) 进行计算。

$$u_k = \varphi_k + \delta u_k \quad (9)$$

$$r_k = A(1 - e \cos E_k) + \delta r_k \quad (10)$$

$$i_k = i_0 + \dot{i} \cdot t_k + \delta i_k \quad (11)$$

(9) 在计算发射时刻的升交点经度 Ω_k 之前, 需要先计算卫星在轨道平面的坐标, 将极坐标 (r_k, u_k) 转换成平面直角坐标系中的坐标 (x'_k, y'_k) :

$$x'_k = r_k \cos u_k \quad (12)$$

$$y'_k = r_k \sin u_k \quad (13)$$

(10) 转换完成后进行升交点经度的解算, 针对 MEO/IGSO 卫星, 升交点经度的线性模型为:

$$\Omega_k = \Omega_0 + (\dot{\Omega} - \dot{\Omega}_e) t_k - \dot{\Omega}_e t_{oe} \quad (14)$$

代入星历数据中的 Ω_0 进行解算, 式 (14) 中的 $\dot{\Omega}_e$ 为 CGCS2000 坐标系下的地球自转角速度。

$$\dot{\Omega}_e = 7.292\ 115 \times 10^{-5} \text{ rad/s}$$

(11) 最后解算卫星在 CGCS2000 坐标系中的坐标, 针对 MEO/IGSO 卫星, 轨道平面直角坐标系需要先绕 X' 轴进行旋转 $(-i_k)$, 再绕旋转后的 Z' 轴旋转 $(-\Omega_k)$, 即通过式 (15) 可转换成 CGCS2000 地心地固直角坐标系。

$$\begin{cases} x_k = x'_k \cos \Omega_k - y'_k \cos i_k \sin \Omega_k \\ y_k = x'_k \sin \Omega_k + y'_k \cos i_k \cos \Omega_k \\ z_k = y'_k \sin i_k \end{cases} \quad (15)$$

经过上述步骤最终得出伪卫星位置坐标 (单位: m):
(x_k, y_k, z_k) = ($-1.469\ 9 \times 10^7, 3.232\ 1 \times 10^7, 2.254\ 5 \times 10^7$)

2.3 验证

当接收机有 4 颗或 4 颗以上可见卫星的伪距测量值时, 观测方程就由 4 个或 4 个以上方程式组成, 接收机就可以解算出方程组中的 4 个未知量, 包括: 三维位置和接收机钟差, 从而实现接收机的定位、授时。

此次验证过程采用的数据为线上数据, 接收机对 4 颗卫星在信号接收时刻 (2019, 3, 22, 3, 2, 42.990 989) 对 B1 频点的观测伪距如图 9 所示。

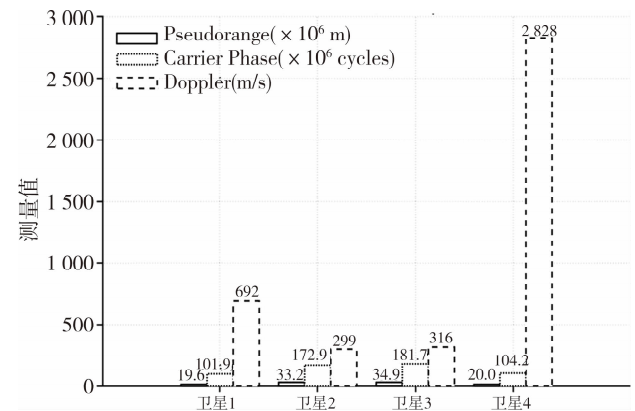


图 9 B1 频点观测量

经过地球自转改正后的卫星空间位置（单位：m）和误差校正后的伪距测量值（单位：m）如图 10 所示。

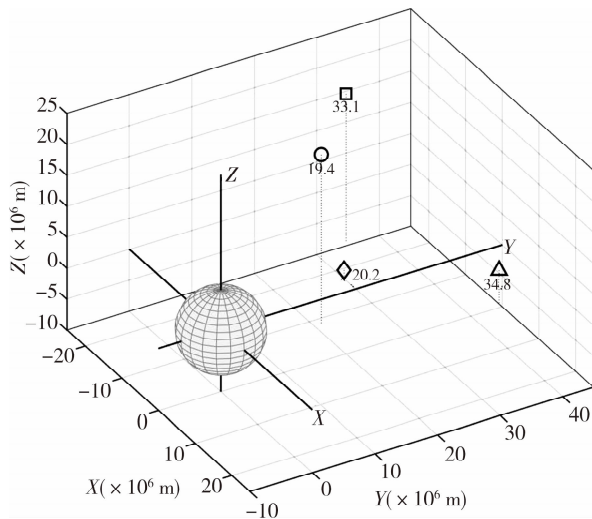


图 10 纠正后的空间位置和伪距

图 10 中 1 号卫星为 MEO 卫星，2 号卫星为 IGSO 卫星，3 号卫星为 GEO 卫星，4 号卫星为 MEO 卫星，伪卫星产生的信号为 IGSO/MEO 卫星播发的 B1I 信号，所以在此替换 2 号卫星的空间位置来进行计算，将伪卫星位置和表中数据代入伪距观测方程（16）中进行解算。

$$\begin{cases} \rho^{(1)} = \sqrt{(x^{(1)} - x_u)^2 + (y^{(1)} - y_u)^2 + (z^{(1)} - z_u)^2} + b_u + l^{(1)} \\ \rho^{(2)} = \sqrt{(x^{(2)} - x_u)^2 + (y^{(2)} - y_u)^2 + (z^{(2)} - z_u)^2} + b_u + l^{(2)} \\ \rho^{(3)} = \sqrt{(x^{(3)} - x_u)^2 + (y^{(3)} - y_u)^2 + (z^{(3)} - z_u)^2} + b_u + l^{(3)} \\ \rho^{(4)} = \sqrt{(x^{(4)} - x_u)^2 + (y^{(4)} - y_u)^2 + (z^{(4)} - z_u)^2} + b_u + l^{(4)} \end{cases} \quad (16)$$

式中， l 为卫星钟差、电离层延迟和对流层延迟计算的常数项，将该观测方程线性化之后，再通过最小二乘法进行解算，最终得到的接收机坐标（单位：m）和钟差（单位：s）为：

$$\begin{cases} X_k = (-2.2894 \times 10^6, 6.0468 \times 10^6, 3.4801 \times 10^6) \\ b_u = -1.6590 \times 10^{-6} \end{cases}$$

将计算后的接收机坐标、钟差与原始接收机进行可视化对比，如图 11 所示。

由图 11 中对比数据可知：X 轴出现非常规负向偏移（ -9.35×10^4 m + 4.26%），与 Y、Z 轴正向偏差形成非对称干扰模式，总空间相对误差达 23.61%，远超 GNSS 接收机典型容错阈值，而 -98.18% 的相对误差表明时钟系统几乎丧失基准保持能力。实验表明，该干扰量级足以造成 GNSS 接收机定位失效和授时系统失准。

3 结论

本文提出一种基于 FPGA 的北斗 B1I 伪信号生成方法。实验结果表明，当欺骗信号进入接收机环路时，伪信号导致接收机定位结果在 X、Y、Z 轴分别产生 -9.35×10^4 m、 $+8.69 \times 10^5$ m、 $+4.81 \times 10^5$ m 的偏差（相对误差达 4.26%、16.79%、16.05%），同时使钟差估计值从 -9.111×10^{-3} s 偏移至 -1.659×10^{-6} s（偏差达 99.98%）。这从生成式欺骗角度出发，为导航欺骗提供了一个新的手段。

当前，导航电文认证技术是检测生成式欺骗行为的有效手段^[15]。然而，这也引发了如何进一步为北斗部署导航电文认证方案的思考。后续研究将着重探索以国密算法为基础的北斗 B1I 电文认证，以应对生成式欺骗，确保北斗民用信号更加安全可靠。

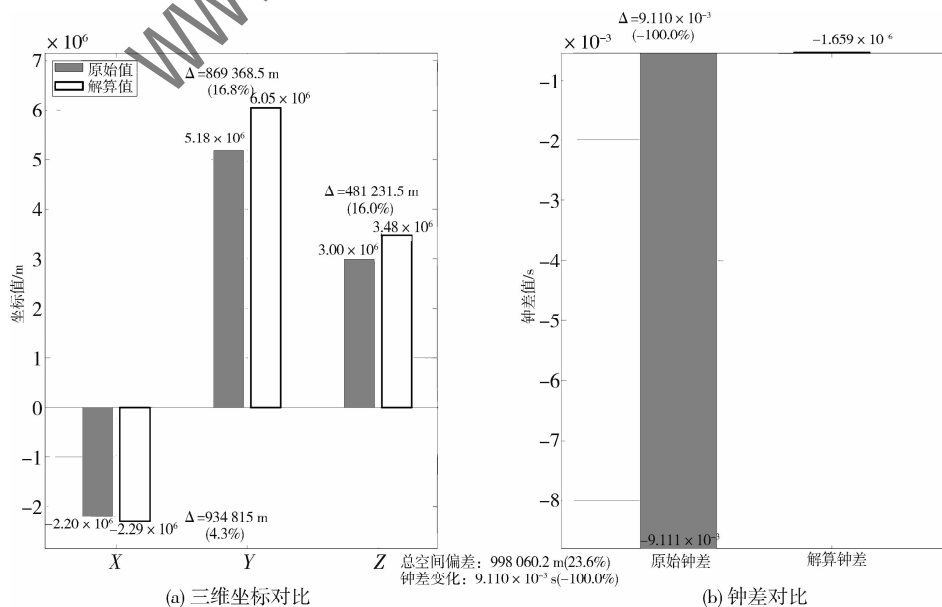


图 11 伪随机信号干扰下的接收机定位与钟差误差对比

（下转第 74 页）

- (3): 197–208.
- [11] 代闯闯, 栾海晶, 杨雪莹, 等. 区块链技术研究综述 [J]. 计算机科学, 2021, 48 (S2): 500–508.
- [12] LIU B, YU X L, CHEN S, et al. Blockchain based data integrity service framework for IoT data [C]//2017 IEEE International Conference on Web Services (ICWS). IEEE, 2017: 468–475.
- [13] XU Y, REN J, ZHANG Y, et al. Blockchain empowered arbitrable data auditing scheme for network storage as a service [J]. IEEE Transactions on Services Computing, 2019, 13 (2): 289–300.
- [14] 陈建伟, 王姝妤, 张美平, 等. 基于区块链且可验证的智能电网多维数据聚合与分享方案 [J]. 通信学报, 2024, 45 (1): 167–179.
- [15] LIN Y, LI J, KIMURA S, et al. Consortium blockchain-based public integrity verification in cloud storage for IoT [J]. IEEE Internet of Things Journal, 2021, 9 (5): 3978–3987.
- [16] 杨小东, 王秀秀, 李茜茜, 等. 基于区块链和雾计算的去中心化云端数据完整性审计方案 [J]. 电子与信息学报, 2023, 45 (10): 3759–3766.
- [17] 王子园, 杜瑞忠. 边缘环境下基于无证书公钥密码的数据完整性审计方案 [J]. 通信学报, 2022, 43 (7): 62–72.
- [18] ZHANG Q, SUI D, CUI J, et al. Efficient integrity auditing mechanism with secure deduplication for blockchain storage [J]. IEEE Transactions on Computers, 2023, 72 (8): 2365–2376.
- [19] WANG H, ZHANG J. Blockchain based data integrity verification for large-scale IoT data [J]. IEEE Access, 2019, 7: 164996–165006.
- (收稿日期: 2025–06–19)

作者简介:

赵雄伟 (1979–), 通信作者, 男, 博士, 主要研究方向: 信息系统、区块链和信息安全。E-mail: 3909082@qq.com.

滕威 (1999–), 男, 硕士, 主要研究方向: 云存储与信息安全。

楚鸿伟 (1989–), 男, 本科, 主要研究方向: 区块链应用。

(上接第 65 页)

参考文献

- [1] 倪淑燕, 陈世森, 付琦玮, 等. 卫星导航欺骗干扰检测与抑制技术综述 [J]. 电讯技术, 2024, 64 (5): 812–820.
- [2] HARTMANN K, GILES K. UAV exploitation: a new domain for cyber power [C]//Proceedings of 2016 8th International Conference on Cyber Conflict. Tallinn: IEEE, 2016: 205–221.
- [3] GREGORY P. EASA reports GNSS jamming/spoofing amid ukraine conflict [EB/OL]. (2022–03–18) [2023–08–08]. <https://www.ainonline.com/aviation-news/air-transport/2022-03-18/easa-reports-gnss-jamming-spoofing-amid-ukraine-conflict>.
- [4] MOSAVI M R, NASRPOOYA Z, MOAZEDI M. Advanced anti-spoofing methods in tracking loop [J]. Journal of Navigation, 2016, 69 (4): 883–904.
- [5] 马克, 孙迅, 聂裕平. GPS 生成式欺骗干扰关键技术 [J]. 航天电子对抗, 2014, 30 (6): 24–26, 34.
- [6] 王传福. 数字化混沌系统的动力学分析与伪随机序列生成算法设计 [D]. 哈尔滨: 黑龙江大学, 2020.
- [7] 束礼宝, 宋克柱, 王砚方. 伪随机数发生器的 FPGA 实现与研究 [J]. 电路与系统学报, 2003 (3): 121–124.
- [8] VOSTA K P, GHOLAMI M. Pseudo random bit generator in QCA for high speed communications [J]. Heliyon, 2024, 10 (22): e40238.
- [9] HOU S, GUO Y, LI S. A lightweight LFSR-based strong physical unclonable function design on FPGA [J]. IEEE Access, 2019, 7: 64778–64787.
- [10] 中国卫星导航系统管理办公室 (CSNO). 北斗卫星导航系统空间接口控制文件 公开服务信号 [S]. 2.1 版. BDS-SIS-ICD-2.1, 2016.
- [11] 王迪, 郝士琦, 朱斌. “北斗”2 代 B1I 信号导航电文分析 [J]. 航天电子对抗, 2013, 29 (6): 30–32.
- [12] 郭维. 北斗 B1I 信号的模拟与捕获算法研究 [D]. 太原: 中北大学, 2021.
- [13] 虞玲. 北斗二号导航信号软件模拟源的研究与实现 [D]. 西安: 西安电子科技大学, 2014.
- [14] 刘清, 谢坚, 王伶, 等. 卫星导航欺骗式干扰源高精度直接定位方法 [J]. 电子学报, 2022, 50 (5): 1117–1122.
- [15] 付晨罡, 陈潇, 刘婷, 等. 面向北斗导航电文认证的符号级欺骗方法研究 [J]. 导航定位与授时, 2024, 11 (4): 16–25.
- (收稿日期: 2025–06–27)

作者简介:

王凯迪 (2001–), 男, 硕士研究生, 主要研究方向: 卫星导航信号应用。

曹新亮 (1970–), 通信作者, 男, 博士, 教授, 硕士生导师, 主要研究方向: 综合电子系统设计与微波遥感。E-mail: caoxinliang874@163.com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com