针对GNSS授时接收机的转发式欺骗干扰技术研究*

黄 龙,龚 航,朱祥维,王飞雪
(国防科技大学 电子科学与工程学院,湖南 长沙 410073)

摘 要:授时接收机通过接收并处理卫星导航信号以获取高精度时间,为通信、电力及金融等系统提供精准的标准时间信号。提出了一种针对授时接收机的转发式欺骗干扰技术,通过对目标接收机的精密定位以及转发信号的精确时延控制,实现了对授时接收机的定时偏差控制,从而使其上层系统无法正常工作。通过建立仿真模型,验证了该欺骗干扰技术的有效性。

关键词:授时接收机;卫星导航;欺骗干扰;精密定位
中图分类号:TN958 **文献标志码**:A **文章编号**:1001-2486(2013)04-0093-04

Research of re-radiating spoofing technique to GNSS timing receiver

HUANG Long, *GONG Hang*, *ZHU Xiangwei*, *WANG Feixue*
(College of Electronic Science and Engineering, National University. of Defense Technology, Changsha 410073, China)

Abstract: To supply accurate stand time signal, timing receivers were used to acquire high precision time by processing satellite navigation signals. A re-radiating spoofing technique was proposed, which dealt with the target receiver's timing uncertainty by controlling the signal delays and positioning antenna precisely. Once the timing receiver was controlled by the spoofing signals, the host system could be collapsed. Simulation results validate the effectiveness of the proposed spoofing technique.

Key words: timing receiver; GNSS; spoofing interfere; precise positioning

随着科技的进步,人类社会对时间精度的要求越来越高。电力系统、通信系统、计算机网络等国家基础设施均需要高精度的时间同步才能正常运行。授时接收机作为时间同步系统中的关键设备,通过接收并处理卫星导航信号以获取高精度时间,为其上层系统提供精准的标准时间信号。针对关键基础设施中的授时接收机实施欺骗干扰,通过引入授时误差破坏系统时间同步,从而使其通信、电力、网络等核心系统瘫痪,以达到对敌软打击的目的。

本文通过卫星导航授时接收机原理的研究,提出了一种基于转发时延精密控制的欺骗干扰技术,可以在无需物理靠近的条件下实现对目标接收机定时偏差的控制,同时保证其定位结果不变,以防止被接收机察觉。仿真结果表明,该方法可以在保持定位结果不变的条件下,有效实现对目标接收机定时偏差的控制。

1 授时接收机工作原理

基于卫星导航系统的授时型接收机是在卫星接收机的基础上添加了授时模块。授时模块主要由本地钟、时刻比对、钟差计算、秒脉冲(1pps)合成和秒脉冲(1pps)合成控制等部分组成,如图1所示。

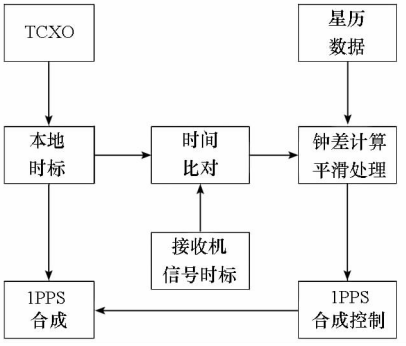

图1 授时接收机中授时模块原理框图
Fig. 1 Schedule of timing module in receiver

授时接收机首先比对接收信号中恢复出的时标信息与本地时标信息,得到伪距测量结果;再根据卫星星历、本地坐标、相关电离层/对流层修正参数以及接收机时延标定信息计算出本地时钟与卫星导航系统时钟的钟差,该钟差作为本地钟调整以及1pps合成的依据。

由以上授时原理可知,只要对目标接收机注

* 收稿日期:2013-01-24
作者简介:黄龙(1982—),男,重庆潼南人,博士研究生,E-mail: longhuang@nudt.edu.cn;
王飞雪(通信作者),男,教授,博士,博士生导师,E-mail: wangfeixue365@sina.com

入虚假的卫星导航信号,使其得到错误的伪距测量结果,即可实现对其最终授时结果的欺骗控制。

2 转发式欺骗干扰原理

转发式欺骗干扰是通过对真实卫星信号的接收和延迟,放大后再通过发射天线辐射出去。比如现在广泛用于测试和室内应用的 GPS 转发器(Re-radiator),其实质就是一个简单的欺骗干扰源,其应用模式如图 2 所示。

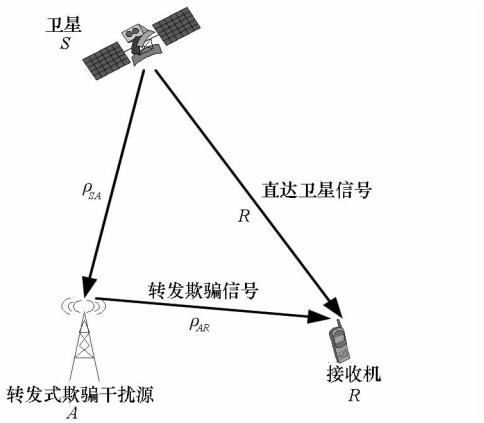

图 2 转发式欺骗干扰模型

Fig. 2 Model of re-radiating spoofing

由图 2 可以看出,经转发后,信号传输距离大于直达信号传输距离,从而使得目标接收机对欺骗信号的伪距测量值大于对真实直达信号,最终导致接收机的钟差计算错误。

3 针对授时接收机的转发式欺骗干扰系统

由于大部分授时接收机均安装于固定位置,且其接收天线相位中心坐标精确已知,因此授时接收机内部可能会采用位置校验的信号完好性监测手段,即将接收机的实时定位结果与已知位置坐标比对,若发现明显的位置偏移,则可判断当前接收信号异常,从而转入自主守时模式。

因此,为了能准确控制目标接收机的授时输出结果,针对这类授时接收机的欺骗攻击,需要着重考虑其位置校验的正确性。

假定在某时刻目标授时接收机接收真实卫星直达信号的定位解算方程为(不失一般性,假定接收机接收 4 颗卫星信号):

$$\begin{cases}\rho_1=\sqrt{(x_1-x_u)^2+(y_1-y_u)^2+(z_1-z_u)^2}+ct_u+ct_{s1}=R_1+ct_u+ct_{s1}\\ \rho_2=\sqrt{(x_2-x_u)^2+(y_2-y_u)^2+(z_2-z_u)^2}+ct_u+ct_{s2}=R_2+ct_u+ct_{s2}\\ \rho_3=\sqrt{(x_3-x_u)^2+(y_3-y_u)^2+(z_3-z_u)^2}+ct_u+ct_{s3}=R_3+ct_u+ct_{s3}\\ \rho_4=\sqrt{(x_4-x_u)^2+(y_4-y_u)^2+(z_4-z_u)^2}+ct_u+ct_{s4}=R_4+ct_u+ct_{s4}\end{cases} \tag{1}$$

式中 ρ_i 表示目标接收机对测距结果,(x_i,y_i,z_i) 为从星历获取的第 i 颗卫星的位置,t_i 为从星历获取的第 i 颗卫星的卫星钟差,R_i 为第 i 颗卫星与目标接收机间的真距,(x_u,y_u,z_u) 为目标接收机的定位解算位置,t_u 为目标接收机的定时解算钟差。

为了在定位结果(x_u,y_u,z_u)不变的情况下拉偏目标接收机的授时结果 t_u,实施转发式欺骗干扰时,需保证目标接收机得到的上述 4 个定位解算方程两边的增量相同,即

$$\begin{cases}\rho_1'=\rho_1+\Delta\rho=\sqrt{(x_1-x_u)^2+(y_1-y_u)^2+(z_1-z_u)^2}+ct_u'\\ \quad=R_1+c(t_u+t_1+\Delta t)\\ \rho_2'=\rho_2+\Delta\rho=\sqrt{(x_2-x_u)^2+(y_2-y_u)^2+(z_2-z_u)^2}+ct_u'\\ \quad=R_2+c(t_u+t_2+\Delta t)\\ \rho_3'=\rho_3+\Delta\rho=\sqrt{(x_3-x_u)^2+(y_3-y_u)^2+(z_3-z_u)^2}+ct_u'\\ \quad=R_3+c(t_u+t_3+\Delta t)\\ \rho_4'=\rho_4+\Delta\rho=\sqrt{(x_4-x_u)^2+(y_4-y_u)^2+(z_4-z_u)^2}+ct_u'\\ \quad=R_4+c(t_u+t_4+\Delta t)\end{cases} \tag{2}$$

转发式欺骗攻击系统需要保证各路转发信号与其直达信号的时延差相同,

$$\begin{cases}\rho_{SA1}+\rho_{AR}+\tau_1+\Delta\rho_1+ct_u=R_1+ct_u+ct_1+\Delta\rho\\ \rho_{SA2}+\rho_{AR}+\tau_2+\Delta\rho_2+ct_u=R_2+ct_u+ct_2+\Delta\rho\\ \rho_{SA3}+\rho_{AR}+\tau_3+\Delta\rho_3+ct_u=R_3+ct_u+ct_3+\Delta\rho\\ \rho_{SA4}+\rho_{AR}+\tau_4+\Delta\rho_4+ct_u=R_4+ct_u+ct_4+\Delta\rho\end{cases} \tag{3}$$

式中 ρ_{SAi} 表示第 i 颗卫星与干扰接收机间的距离,ρ_{AR} 表示欺骗干扰发射天线与目标接收机间的距离,τ_i 表示欺骗干扰系统各接收天线至发送天线的链路时延,$\Delta\rho_i$ 表示欺骗攻击系统对第 i 颗卫星链路的附加时延控制量,$\Delta\rho$ 表示欺骗攻击在目标接收机上最终体现出的时钟偏移。

将式(3)等号两边进行整理,即可得到

$$\begin{cases}\rho_{SA1}+\rho_{AR}+\tau_1+\Delta\rho_1=R_1+ct_1+\Delta\rho\\ \rho_{SA2}+\rho_{AR}+\tau_2+\Delta\rho_2=R_2+ct_2+\Delta\rho\\ \rho_{SA3}+\rho_{AR}+\tau_3+\Delta\rho_3=R_3+ct_3+\Delta\rho\\ \rho_{SA4}+\rho_{AR}+\tau_4+\Delta\rho_4=R_4+ct_4+\Delta\rho\end{cases} \tag{4}$$

上式中,目标接收机的星地距离 R_i 以及干扰接收机的星地距离 ρ_{SAi} 均随时间不断变化,因此欺骗攻击系统需要以一定的周期对各链路时间控制量进行更新,以保证最终攻击效果。

一个典型的转发式欺骗攻击系统如图 3 所示,不同的定向接收天线指向不同的可视卫星,各接收站信号经时延控制网络进行时延调整后,合

路经由同一面发射天线向目标接收机辐射。在式(4)中,在准确测定目标接收机天线位置的前提下,转发欺骗攻击系统发射天线与目标接收机接收天线距离 $\rho_{AR1}=\rho_{AR2}=\rho_{AR3}=\rho_{AR4}$ 且已知、欺骗干扰系统以及目标接收机接收天线星地距离 ρ_{SA1}, ρ_{SA2},ρ_{SA3},ρ_{SA4} 和 R_1,R_2,R_3,R_4 可精确测量计算,欺骗干扰系统各接收天线至发送天线的链路时延 τ_1,τ_2,τ_3,τ_4 可精确标定、因此,只需控制各路转发信号的时延 $\Delta\rho_1$,$\Delta\rho_2$,$\Delta\rho_3$,$\Delta\rho_4$ 即可在保证目标接收机定位结果为其预知值的同时,控制其钟差发生 $\Delta\rho/c$ 的偏移。

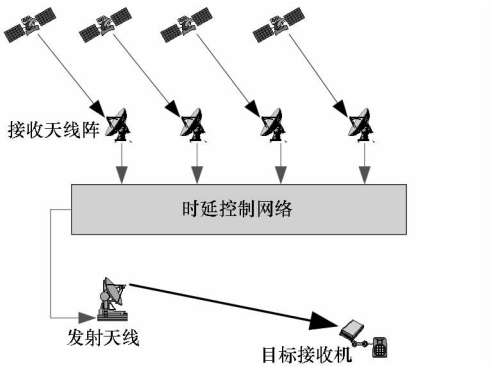

图 3　转发式欺骗干扰系统示意图

Fig. 3　Model of re-radiating spoofing system

4　转发式欺骗干扰误差源分析

在式(4)中,等式右边为目标接收机的测量结果,等式左边为转发式欺骗干扰系统控制参量,即欺骗干扰系统对其星地距离、发送天线与目标接收机接收天线的距离、链路时延以及信号时延的控制精度直接决定了对目标接收机的欺骗干扰性能。

4.1　星地距离测量

对卫星与欺骗干扰系统接收天线间星地距离采用高精度民用 GNSS 接收机进行实时测量,以保证欺骗干扰系统的机动性以及实时性。

由于采用同一台 GNSS 接收机对欺骗干扰系统各接收天线进行星地距离测量,其接收机钟差相同并可以归算只链路时延中,因此可以认为标定接收机对各天线测得的时延即为星地距离,其测量误差 $\sigma_1\approx0.3$ns。

4.2　收发天线间距离测量

应用于关键基础设施的授时接收机一般安装于安全防护较好的环境,无法对其进行接近式位置标定。但为了保证卫星可视性以及测量精度,授时接收机天线一般安装于视野较好的楼顶、塔顶等位置,从而为非接近式精密测量提供了条件。

测绘领域使用的非合作目标性全站仪(Reflectorless Total Station)是测量墙角、不可及目标、岩石表面、建筑物内部的顶部和墙面等对象的理想工具,也为无法接近的收发天线间距离测量提供了理想的手段。无合作目标性全站仪发射细小的激光束到测量目标上,并通过测相电路直接测定出光波在测线两端间往返传播的时间引起的相位差来计算距离,具有测量方便,测距精度高的特点。同时,在无合作目标工作模式下,无需在测量点放置放射棱镜,直接将测量激光束打到待测目标天线上,即可实现转发天线至目标接收机天线距离的精密测量,如图 4 所示。

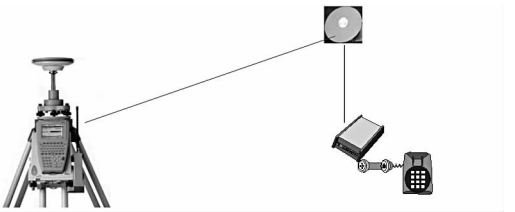

图 4　全站仪标定发射天线与接收天线距离

Fig. 4　Ranging with reflectorless total station

徕卡 TPS1200 系统全站仪即具备该无合作目标性测量能力,其无棱镜测程可达 1000m,测量精度 $\sigma_2\approx0.1$ns。

4.3　链路时延标定

由于转发式欺骗干扰系统一般不会长时间连续工作,因此其链路时延可以通过标准仪器进行离线标定,在工作过程中可认为其链路时延保持不变。链路时延标定精度一般为 $\sigma_3\approx0.3$ns。

4.4　信号时延控制

信号时延控制网络是转发式欺骗干扰系统的关键设备。由于转发信号链路中其他时延部分均不可控,因此只能通过对各路转发信号进行附加时延控制,才能实现对目标接收机定位定时结果的有效控制。

在转发式欺骗干扰系统中信号时延控制通过数控延迟线设备(Programmable Delay Line)来完成。目前市面上已有成熟的数控延迟线设备可以在宽频带范围内几乎无失真地实现皮秒量级的时延控制 $\sigma_4\approx0.001$ns,如图 5 所示。

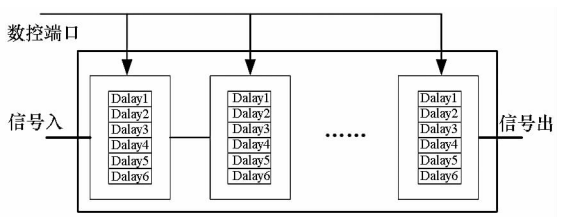

图 5　数控延迟线原理

Fig. 5　Programmable delay line instrument

综合以上转发式欺骗干扰系统误差源的分析,可以得到转发式欺骗干扰系统对目标接收机接收信号所产生的附加误差为:

$$\sigma = \sqrt{\sigma_1^2 + \sigma_2^2 + \sigma_3^2 + \sigma_4^2} \approx 0.436\text{ns} \quad (5)$$

5 欺骗干扰性能分析

假定授时接收机以无干扰信号存在时判定95%以上定位结果有效为依据设定欺骗干扰检测门限,那么当欺骗干扰导致定位结果发生明显偏移时,即可有效检测出欺骗干扰的存在,如图6所示。

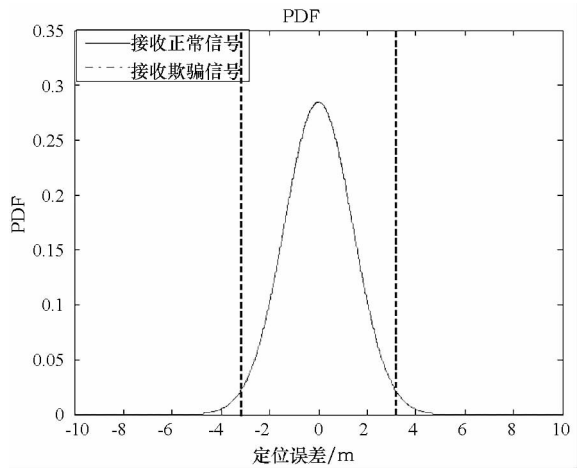

图6 定位误差概率分布函数(PDF)

Fig. 6 PDF of position errors

由文献[2]可知,授时接收机定位误差(RSS)一般为1.4m,由此可以得到95%概率下的欺骗干扰定位偏差判决门限为:

$$\text{Th} = 2.7439\text{m} \quad (6)$$

转发系统引入的附加误差为0.436ns,从而得到目标接收机接收上述转发式欺骗干扰信号时,定位误差为:

$$\sigma_m = \sqrt{1.4^2 + (0.436 \times 0.3)^2} = 1.4061\text{m} \quad (7)$$

即转发系统对接收机定位误差影响非常小。同时,对各路卫星信号的精确时延控制使得接收机定位误差的均值为0,从而可以得到上述转发式欺骗干扰系统对目标授时接收机实施有效欺骗干扰的概率:

$$P_{Spoof} = \int_{-Th}^{Th} p_{\mu(0,1.4061)}(x)\,\mathrm{d}x = 0.948994 \quad (8)$$

同时,由于授时接收机一般均采用时差平滑技术对测量得到的时差进行平滑降噪处理后再调整其最终输出时标信号(如图1所示),因此,欺骗干扰系统在授时接收机上引入的时差跳变同样会被平滑后才反映到输出时标信号上,从而更具隐蔽性,如图7所示。

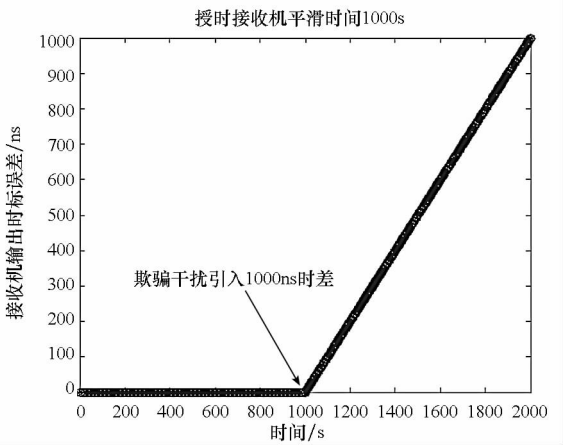

图7 平滑时标信号误差

Fig. 7 Time errors of averaging processing

6 结论

本文提出了一种针对授时接收机的转发式欺骗干扰系统设计方法。理论分析和仿真结果表明,通过对转发系统时延的精密控制以及对目标接收机天线位置的精确标定,可以以极大的概率对授时接收机时差进行有效控制,并且具有很高的隐蔽性,难以被对方检测。

参考文献(References)

[1] 李跃,邱致和. 导航与定位[M]. 2版. 北京:国防工业出版社,2008.
LI Yue, QIU Zhihe. Navigation and position[M]. 2nd Edition. Beijing: National Defense Industry Press, 2008. (in Chinese)

[2] Kaplan E D, Hegarty C J. Understanding GPS principles and applications[M]. 2nd Edition. Beijing: Publishing House of Electronics Industry, 2007.

[3] 黄龙,唐小妹,王飞雪. 卫星导航接收机抗欺骗干扰方法研究[C]. 第二届中国卫星导航学术年会, 上海,2011.
HUANG Long, TANG Xiaomei, WANG Feixue. Anti-spoofing techniques for GNSS receiver[C]. China Satellite Navigation Conference, Shanghai, May 18-20, 2011. (in Chinese)

[4] Pozzobon O. Keeping the spoofs out[J]. Inside GNSS, 2011, 6(3):55.

[5] Wesson K, Shepard D, Humphreys T. Straight talk on anti-spoofing[J]. GPS World, 2012, 23(1): 32-39.

[6] Jahromi A J, Nielsen J, Lachapelle G. GPS spoofer countermeasure effectiveness based on using signal strength, noise power and C/no observables[J]. International Journal of Satellite Communications and Networking, 2012, 30: 181-188.

[7] Daneshmand S, Jafarnia-Jahromi A, Lachapelle G. A low-complexity GPS anti-spoofing method using a multi-antenna array[C]//Proceeding of ION GNSS, 2012.

[8] Humphreys T E, Ledvina B M, Kintner P M, Assessing the spoofing threat: development of a portable GPS civilian spoofer[C]//Proceeding of ION GNSS, 2008:2314-2325.