文章编号:1002-0640(2016)07-0001-04

GNSS欺骗干扰技术研究*

庞 晶,倪少杰,聂俊伟,欧 钢
(国防科技大学电子科学与工程学院,长沙 410073)

摘 要:欺骗干扰是目前卫星导航设备面临的重要威胁,在欺骗干扰条件下,目标接收机接收到的欺骗信号功率大于真实信号,产生错误的定位或授时结果。根据干扰产生方式的不同将欺骗干扰源分为基于信号模拟器的自主产生式、基于接收机的接收产生式、基于转发器的转发式3类,其中基于接收机的产生式是目前真正实现欺骗攻击的干扰源。由于欺骗干扰实现形式的复杂多样性,对欺骗干扰的实施阶段、信号特性的影响和定位授时结果的影响进行了分析。

关键词:GNSS,欺骗干扰,诱导,抗欺骗
中图分类号:TN967.1 文献标识码:A

An Overview to GNSS Spoofing Technologies

PANG Jing,NI Shao-jie,NIE Jun-wei,OU Gang
(*School of Electronic Science and Engineering,National University of Defense Technology,Changsha* 410073,*China*)

Abstract:GNSS spoofing is an important threat to the current satellite navigation equipment. Under the condition of spoofing,the spoofing signal's power that target receiver received is greater than the real signal,and positioning errors or timing error are induced. According to the different methods of signal generating,spoofing source is divided into three categories: spoofer based on GNSS signal simulator,spoofer based on GNSS receiver and spoofer based on signal transponder re-radiator. The spoofer based on GNSS receiver is truly realizes the spoofing attack to receiver. Due to the complexity of spoofer realization forms,the implementation stage,signal characteristics and the influence to positioning and timing results are analyzed.

Key words:GNSS,spoofing,induce,anti-spoofing

0 引言

全球卫星导航系统(Global Navigation Satellite System,GNSS)在军民领域应用非常广泛,由于到达地面的信号微弱和民用信号格式公开的原因,容易被压制干扰和欺骗干扰[1]。

欺骗干扰是一种人为干扰,通过发射与真实卫星信号相同或相似的信号,使接收机跟踪到欺骗信号,从而获得错误的位置或时间信息[2]。与传统的以功率覆盖为主的压制干扰相比,欺骗干扰具有更大的危害性。成功的压制干扰导致被攻击目标定位或定时失败,转而启用备用导航手段。而被欺骗干扰攻击的目标接收机常常无法意识到被攻击,持续输出错误的定位或定时结果,从而诱导导弹攻击错误目标,或是瘫痪诸如电力系统、银行金融系统、无线通信系统等社会民用基础设施[3]。

目前一般的接收机尚未采用抗欺骗干扰措施,欺骗干扰逐渐成为卫星导航设备面临的潜在威胁。2011年,伊朗声称利用GPS欺骗技术俘获美军RQ-170无人机,2012年美国国防部在欺骗实验中,成功控制GPS无人直升机下降和爬升[4]。导航设备的欺骗干扰防护方案研究已成为研究热点。研

收稿日期:2015-06-12 修回日期:2015-07-07
* 基金项目:国家自然科学基金资助项目(61403413)
作者简介:庞 晶(1978-),女,山西新绛人,讲师,博士研究生。研究方向:卫星导航信号仿真模拟与接收机测试技术。

究欺骗干扰的实现机理有助于了解导航设备的弱点及制定抗欺骗干扰策略,是抗欺骗干扰技术研究的基础。

本文从欺骗干扰原理分析了实现对导航或授时型接收机进行欺骗干扰的约束条件,按欺骗干扰的产生方式对干扰模式进行分类介绍,并分析了欺骗干扰可实施时机、信号特性影响、信息处理结果影响等内容。

1　欺骗干扰原理

GNSS 接收机的定位原理是同时接收 4 颗或 4 颗以上的卫星信号,通过测量各个卫星信号到接收机的伪距,对方程联立求解,得出接收机的定位坐标 (x,y,z) 和钟差信息。

通过欺骗干扰 GNSS 接收机,使其测量得到错误的伪距,会得到错误的定位或定时结果。

本文介绍典型欺骗干扰原理,以 4 星定位为例,欺骗干扰原理示意图如图 1 所示,位于 S 点的欺骗干扰源发射欺骗干扰信号,将位于 A 点的目标接收机欺骗到虚拟点 B[5]。在欺骗干扰条件下,目标接收机接收到的信号同时来自卫星和干扰源,但干扰信号占据主导作用,分析时忽略卫星信号的影响。

欺骗干扰实施步骤如下:

1) 位于 S 点的干扰源接收 4 颗真实卫星 G1、G2、G3、G4 的信号,得到伪距 $(\rho_{S1},\rho_{S2},\rho_{S3},\rho_{S4})$;

2) 干扰源通过空域滤波或相关的方法分离各通道信号,根据适当的算法对各通道信号进行时延调整,并通过天线发射出去;

3) 位于 A 点的目标接收机接收欺骗信号,得到伪距 $(\rho_{B1},\rho_{B2},\rho_{B3},\rho_{B4})$,计算出定位解算结果为 B 点坐标 (x_B,y_B,z_B)。

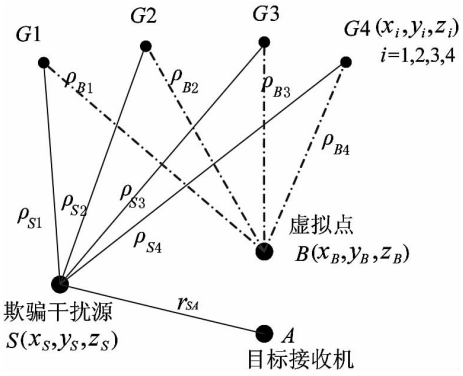

图 1　欺骗干扰系统示意图

由此可见,欺骗干扰的关键在卫星信号的通道分离和计算各通道信号的时延调整量。单接收天线的接收机会收到所有的可见卫星信号,因此,通道的分离通过数字解调实现,需要已知伪码,只能对公开信号进行欺骗。另一种通道分离方法是采用自动跟踪卫星信号的定向天线,通过空域滤波技术对多颗卫星信号进行分离处理,可实现对未知伪码信号的欺骗干扰。

2　欺骗干扰分类

文献 [5-7] 通常根据产生机理将欺骗干扰源分为产生式和转发式干扰源。国外一般根据信号的复杂度将欺骗干扰源分为 3 类[8-9]:简单干扰、中级干扰和高级干扰,简单干扰源利用目前市场的信号模拟器与天线组合实现;中级干扰源根据接收机获得的真实卫星信号参数估计当前目标参数,重新生成欺骗干扰信号;复杂干扰源为多个中级干扰源分布式协同工作,能使得到抗欺骗干扰到达角检测方法失效。

不论产生式还是转发式干扰源,都可以组成单一天线发射的单点干扰和多干扰源协同工作的分布式干扰两种模式。根据工程实现原理,将欺骗干扰源分为 3 类:基于信号模拟器的自主产生式、基于接收机的接收产生式、基于信号转发器的转发式干扰源。

2.1　基于信号模拟器的自主产生式

GNSS 信号模拟器是目前广泛应用于接收机测试设备,可以模拟各种真实环境中用户机接收的卫星导航信号。通过在一个 GNSS 信号模拟器,如 Spirent 公司的 GSS8000 上配置相应的功放和发射天线,即可制造一个简单的欺骗干扰源[10]。这种欺骗干扰源实现简单,所需的设备市场上均有成熟产品,从而成为目前全球卫星导航系统面临的最主要欺骗干扰威胁。

基于信号模拟器的欺骗干扰源完全自主产生信号,没有与真实卫星信号同步,因此,其产生的虚假信号会造成接收机失锁或重捕,这样就会使得目标产生警觉,即使能防止重捕,也会造成接收机 GPS 时间估计的巨大变化,很容易被检测出来。此外,信号模拟器体积庞大,价格高昂也是重要缺点。

2.2　基于接收机的接收产生式

基于接收机的欺骗干扰源以美国德州大学的 Todd Humphreys 团队研制的干扰源为代表[8],它是第一台真正意义上的 GNSS 欺骗干扰源。从图 2 可以看到,干扰源主要由接收和发射两部分组成。发射部分实质是 GNSS 信号产生器,其信号生成原理与自主产生式欺骗干扰类似,主要区别是生成信号的参数来源不同,前者自主设置,后者是根据前端

接收机真实卫星信号的估计结果,通过算法得到。

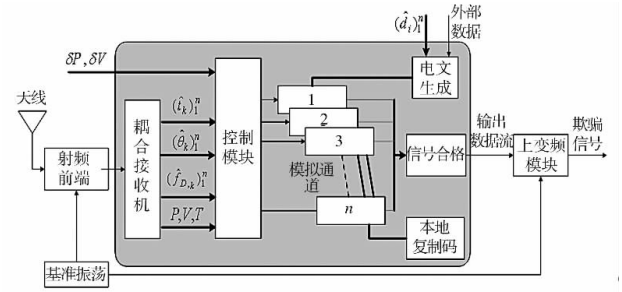

图 2　基于接收机的欺骗干扰源框图

Todd Humphreys 团队利用该干扰源发射伪造 GPS 信号,2012 年成功控制 GPS 无人直升机下降和爬升,2013 年诱导地中海游艇偏离航线且没有发出任何警报,欺骗干扰过程中信号没有失锁,具有很高的隐蔽性,具体实施步骤如下[1]:

1) 干扰源接收真实信号,估计目标接收机跟踪信号的码相位和载波频率;

2) 产生低功率欺骗信号,控制其码相位在目标接收机跟踪信号几个码片之外;

3) 逐步调整码相位接近真实信号,同时增大信号功率占据跟踪信号主导地位;

4) 利用欺骗信号的功率优势牵引相关峰离开真实信号,实现对目标接收机的控制,如图 3 所示。

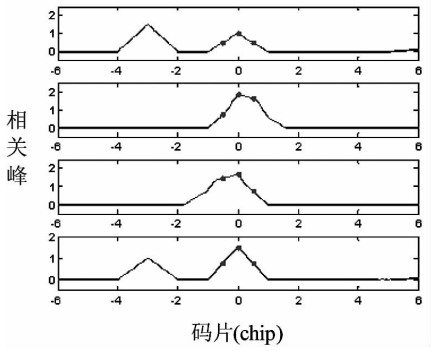

图 3　欺骗信号滑动牵引锁定信号相关峰

该方法需要精确测定目标接收机与欺骗干扰源天线之间的三维位置关系,实现难度较大[11],尤其当目标接收机处于运动状态时。演示试验中选取的目标接收机是处于静止状态的无人直升机和低速运动的游艇。

基于接收机的接收产生式与真实信号接近,可以滞后或提前发射信号,其缺点是需要了解信号结构,无法未知结构的军用信号实时干扰。

2.3 基于信号转发器的转发式

我国在 GPS 欺骗方面的研究主要集中在基于信号转发器的欺骗干扰。转发式欺骗不需要知道信号格式和伪码,其最大的优点是可以避免对军码进行解密的要求。由于技术的敏感性,国外较少有转发欺骗干扰研究的公开文献。

简单的转发方式为接收真实卫星信号,所有通道统一延时放大后再通过发射天线辐射出去,如现在广泛用于测试的 GPS 实时转发器 Re-radiator,可以实现精确重现真实 GNSS 信号的记录回放系统,如 Spirent 公司的 GSS6400。这类来源于接收机测试需求的信号播发方式,可以实现对一定范围内接收机欺骗,但接收机得到的定位解算结果始终为转发器接收天线的坐标,并不算真正意义上的欺骗干扰。

文献[12]提出一种通过对分布式转发器的干扰信号的时延控制,诱偏 GPS 制导的武器的转发式干扰系统。系统组成为在固定或悬浮在一定高度的平台上安放多颗延迟转发式干扰器,采用智能天线和空间滤波技术,对卫星信号进行分选,每颗干扰器分别转发一颗 G 星信号,如图 4 所示。

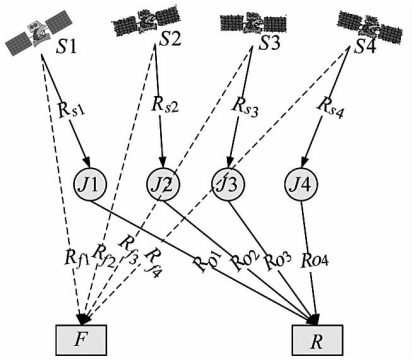

图 4　基于分布式转发器的欺骗干扰系统

文献[13-15]对该系统的诱偏时延算法、区域映射比例影响因素、诱导性能、系统平台优化布阵等问题研究,但仍处于理论和仿真研究阶段。

由于转发式欺骗放大转发,不需要知道伪码,并且信号到达目标接收机的时延一定大于真实信号到达目标接收机的时延,因此,存在一些固有的问题。

1) 接收天线需要采用智能天线阵或可以自动跟踪卫星信号的定向天线,通过空域滤波技术对多颗卫星信号进行分离处理,价格和体积限制应用;

2) 接收的卫星信号为低功率,转发的信号为高功率,且信号格式完全一样,收发隔离问题是实现难点;

3) 信号转发时连同接收噪声一起放大发射出去,会抬高目标接收机的噪声底,容易被检测;

4) 根据前面的分析,被攻击目标授时结果会发生跳变,容易被检测;

5) 时延难以控制在一个码片时间内,不易侵入被攻击目标的跟踪环路,需与压制干扰配合使用。

3 欺骗干扰影响分析

欺骗干扰在目标接收机不同工作阶段产生的

效果不同。此外目标接收机接收到的是欺骗信号与真实卫星信号的矢量和，占据功率主导地位的欺骗干扰信号与真实卫星信号和信息存在一定差异，如信号功率、信号功率变化率、信号来向等[16]。接收机可以利用这些特点进行抗欺骗干扰的检测[17]，这也是欺骗干扰的难点所在。

3.1 欺骗实施阶段

从被欺骗接收机的角度看，欺骗攻击阶段可以分为捕获阶段和跟踪阶段。

捕获阶段对应开机即有欺骗信号，或采用压制干扰方式强制接收机进入重新捕获阶段。此时接收机还未锁定信号，需要实施搜索，只要欺骗信号功率大于真实信号功率即可成功实现欺骗攻击。对于处于捕获阶段，未采取抗欺骗干扰措施的民用接收机，提到的 3 种产生方式的欺骗干扰源都可以通过其功率优势引导目标接收机对其进行捕获跟踪。

跟踪阶段对应已经跟踪上真实信号的接收机，要求在不导致接收机失锁的条件下，侵入并牵引跟踪环路，隐蔽性更强。文献 [8] 基于接收机的欺骗干扰实施方式，就是对接收机跟踪阶段的攻击。由于自主产生式欺骗干扰不与真实信号同步，转发式欺骗干扰滞后真实信号时间可能大于一个码片，实现侵入目标接收机的跟踪环路均存在一定困难，实际产生的干扰效果等同压制干扰中的宽带干扰。

3.2 信号特性的影响

在接收信号的空域特性上，采用单一天线发射欺骗的信号，多路欺骗信号到达接收机天线的方向角完全一致，而不同卫星的真实实际信号到达接收机天下的方向角是不同的。接收机通过多个天线对接收信号进行到达角检测是检测单一发射源欺骗信号的有效手段，只有多个欺骗干扰源协同工作的分布式欺骗干扰方式，可以避免被此方法检测。

在信号特性上，当存在欺骗信号时，目标接收机捕获的信号有以下特点：

1) 相关结果存在多个相关峰，欺骗信号相关峰和真实信号相关峰；

2) 信号绝对功率和信噪比发生变化，一般为增大；

3) 功率变化率与真实卫星信号变化存在差异。

因此，接收机可以采用绝对功率监测、相对功率监测、信号功率变化率监测、残留信号检测等方法进行抗欺骗检测[18-19]。

对于接收机跟踪环路，有两种欺骗信号载波生成策略[1]，一是载波与伪码相位同步调整，二是调整伪码，载波不同步调整。由于欺骗和真实信号的迭加，同步调整会引起载噪比测量结果的剧烈波动，一般选用第二种实现方式。但载波的不同步调整会影响载波环和码跟踪环输出结果的一致性，接收机可以通过一致性进行抗欺骗检测。

3.3 定位授时结果的影响

欺骗效果因目标种类而异，使接收机 PVT 解算结果错误，在欺骗 PVT 和真实 PVT 差异比较大时，接收机通过与惯性导航、高度计、测速器等传感器其他传感器测量结果对比，容易检测出被欺骗。这种情况下，需要逐渐拉偏 PVT 结果，保证变化结果在传感器误差范围内[20]。

4 结论

本文根据干扰产生方式的不同将欺骗干扰源分为基于信号模拟器的自主产生式、基于接收机的接收产生式、基于转发器的转发式等 3 类。针对未采用抗欺骗干扰措施的接收机，欺骗干扰很容易实施，有多个成功案例。如果考虑到接收机的抗欺骗措施，对欺骗实施条件有一些约束条件，欺骗有很多技术难点。欺骗干扰和抗欺骗干扰是“矛”和“盾”的关系，好的欺骗干扰方式可以提高接收机抗欺骗的代价。在欺骗与抗欺骗的攻防对抗中，欺骗技术将得到快速的发展。

参考文献：

[1] GAO Y,LI H,LU M Q,et al. Intermediate spoofing strategies and countermeasures [J]. Tsinghua Science and Technology,2013,18(6):599-605.

[2] ALI J J,ALI B,JOHN N,et al.GPS vulnerability to spoofing threats and a review of antispoofing techniques [J]. International Journal of Navigation and Observation,2012,2012:1-16.

[3] DANIEL P S,JAHSHAN A B,TODD E H. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks [C]//ION GNSS,2012.

[4] DANIEL P S, JAHSHAN A B, T E,H Drone hack:spoofing attack demonstration on a civilian unmanned aerial vehicle [J].GPS World 2012.

[5] 王伟，陶业荣，王国玉，等. GPS 欺骗干扰原理研究与建模仿真 [J].火力与指挥控制，2009，34(6):115-118.

[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 (信息科学版)，2011，11：1344-1347.

[7] 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)：67-70.

[8] TODD E H, BRENT M L, MARK L P, etal. Assessing the

(下转第 9 页)

由图 13 可以看出,当信干比大于 -15 dB 时,干扰效果不佳,仍然可以看出目标位置。当信干比小于 -15 dB 时,干扰效果明显,已无法找到目标的具体位置,主瓣难以辨别,达到干扰效果。

宽带多维信号是一种较好的低截获概率雷达信号。模糊函数近似为"图钉型",具有较好的距离 - 速度二维分辨力和测量精度,能够获得较大的脉冲压缩比,又因调制方式的复杂性,进一步增强了探测信号的隐蔽性,且兼具干扰性,有效地提升了雷达的"四抗"能力。

4　结论

宽带多维信号具有很好的隐蔽性,兼具探测和干扰功能,该信号设计方法具备开放性、可兼容特性,并具有优良的探测信号或干扰信号,且所设计的信号具备良好的"四抗"能力,为雷达与雷达对抗多维设计提供了一种信号设计方案,具有较强的实用价值。

参考文献:

[1] 杨丹丹,刘以安,唐霜天,等.噪声 - 相位编码复合调制一体化信号设计方法 [J].计算机工程与设计,2011,32(1):354-357.

[2] 杨丹丹.雷达干扰一体化设计的共享信号研究 [D].无锡:江南大学,2011.

[3] 钟璠.雷达探测与干扰一体化信号的研究 [D].成都:电子科技大学,2007.

[4] 邵春平,唐霜天.雷达干扰机一体化共享信号的优化设计研究 [J].微计算机信息,2010,26(10):208-210,238.

[5] MARIA G,FULVIC G.Radar detection and classification of jamming signals belonging to a cone class [J].IEEE Trans-Actions on Signal Processing,2008,56(5):1984-1993.

[6] 陈伯孝.现代雷达系统分析与仿真 [M].西安:西安电子科技大学出版社,2012.

[7] 帕波利斯·A.信号分析 [M].北京:海洋出版社,1981.

[8] ZHIQIANG G,PEIKANG H,WEINING L.Matched NLFM pulse compression method with ultra-low sidelobes [C]//Proceedings of The 5th European Radar Conference,2008:92-95.

(上接第 4 页)

spoofing threat [C]//ION GNSS,Savannah,2008:2314-2325.

[9] PAUL Y M, TODD E H,BRENT M L.A multi-antenna defense-receiver-au tonomous GPS spoofing detection [J]. Inside GNSS ,2009,march/april:40-46.

[10] SCOTT L. Anti-spoofing & authenticated signal architectures for civil navigation systems [C]//ION GNSS,Portland,2003:1543-1552.

[11] WANG J,ZHOU M,LI H,et al. On the requirements of GNSS intermediate spoofing [C]// China Satellite Navigation Conference,Nan Jing,2014:543-552.

[12] 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.

[13] 张颂,杨景曙,潘高峰,等. 诱偏暨导航一体化系统平台优化布阵及运动模型 [J]. 中国科学技术大学学报,2011,41(8):746-752.

[14] 张颂,杨景曙,潘高峰,等. 诱偏暨导航一体化系统中诱偏时延算法 [J].安徽大学学报(自然科学版),2011,35(1):64-68.

[15] 张颂,杨景曙,苗苗,等. 诱偏暨导航一体化平台位置误差补偿算法 [J].现代雷达,2012,34(2):37-40.

[16] DANIEL P S, TODD E H. Characterization of receiver response to spoong attacks [C]//ION GNSS,Portland,2011:2608-2618.

[17] FARINé,ALEKSANDAT J,BOTTERON C, et al. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers [C]//ION PLANS,monterey,2014:1258-1271.

[18] ALI J J,ALI B,JOHN N,et al.GPS spoofer countermeasure effectiveness based on signal strength,noisepower,and C/N0measurements [J].International Journl of Satellite Communications and Networking ,2012,30:181-191.

[19] KYLE D W, DANIEL P S, JAHSHAN A B,et al. Humphreys. an evaluation of the vestigial signal defense for civil GPS anti-spoofing [C]//ION GNSS,Portland,2011:1-11.

[20] SAMER K , NAEEM R , STEVEN L , etal.GPS spoofing detection using RAIM with INS coupling [C]//ION PLANS, Monterey,2014:1232-1239.