基于欺骗干扰技术的导航对抗新途径

和玉竹

（四川九洲电器集团有限责任公司，四川　绵阳　621000）

摘　要：导航对抗作为电子对抗中重要的一部分，其已成为热门研究，目前我国的导航对抗技术研究大部分处于压制式干扰、转发式欺骗干扰、异步生成式欺骗干扰技术，而同步生成式欺骗干扰技术相关研究相对薄弱，本文围绕同步生成式欺骗干扰技术进行论述、研究，实现了一种欺骗干扰技术导航对抗新途径的设计。此外，还利用设计的小型干扰源对目前市面上广泛使用的目标接收机和大疆民用无人机进行了静态、动态干扰测试，经过收集相关测试数据，不断优化设计，验证得出这种基于欺骗干扰技术的导航对抗新途径具有一定的合理性和科学性，可为研究此技术的相关人员提供一定帮助与借鉴，为促进导航对抗水平的提升作出贡献。

关键词：导航对抗；生成式欺骗干扰技术；同步

中图分类号：TN97　　**文献标识码：**A

0　引言

翻阅国内外公开的导航对抗相关的文献中发现，导航对抗中广泛使用的欺骗干扰技术有两种，分别为转发式干扰以及生成式欺骗干扰。转发式欺骗干扰的工作原理是将接收的真实导航信号进行延后转发，使得目标设备与导航系统之间产生一段信号的真空带，导致目标设备无法及时更新导航信息，从而达到干扰和阻断目标设备进行正常导航定位的目的。很多学者通过研究控制延时、改变钟差方式及多普勒频移控制来实现转发式欺骗干扰技术。生成式干扰是干扰源自主生成伪真度极高的欺骗信号，致使目标设备导航定位出现偏差，从而达到干扰的目的，其中，干扰源可以通过计算机调控干扰强度等相关干扰数据。生成式干扰还可以根据所生成的欺骗信号是否与目标设备应该接收到的正确信号在时间上同步细分为同步式生成欺骗干扰技术及异步式生成干扰技术。现阶段在军事导航对抗领域，使用最多的是异步生成式欺骗干扰技术，很多学者通过不同支路微型型号的应用，来进行异步生成式欺骗干扰技术中延时信号的释放，从而实现对目标设备正常工作的干扰。该项技术的适用范围较广，对于干扰源的设置要求不高，所以适合在条件复杂的战场中进行应用，异步生成式欺骗干扰技术主要通过以下两个环节干扰作业：①首先使用压制阻断干扰装备对目标设备的导航系统进行攻击，大量混凝数据流传输到目标设备系统中，阻断系统正常导航功能，使得目标设备导航系统不得不重新搜索接入信号；②利用目标设备导航系统重启的间隙，释放出干扰信号，使其锁定欺骗信号，改变原设航向、航线的目标。然而异步生成式欺骗干扰技术需要进行大功率压制，这意味着存在压制干扰源容易被敌方的观察机、信号接收机等设备所察觉的问题。而同步式欺骗干扰技术在应用的过程中，不需要过大的增加的功率，只需将欺骗信号散布出去，引导目标设备逐渐偏离预设轨迹。

我国在这些基础之上也在不断地对欺骗干扰的方法策略进行优化研究，设计相应试验进行导航对抗的模拟，从翻阅的文献来看，目前对于导航对抗技术的研发主要集中于转发式以及异步生成式两种，到目前为止，对于同步生成式欺骗干扰技术进行研究的相关文献多数停留在理论论证阶段，缺乏实验数据及试验检测工作支撑，未有成熟的经验可以借鉴和分析，针对此种情况，本文的研究核心思路是：首先建立欺骗信号模型，其次给出同步生成式欺骗干扰中的关键步骤，最后尝试使用DSP芯片以及FPGA设计一个小型的同步生成式欺骗干扰源，并进行相应的测试实验，验证能否将目标设备引导使其脱离真实的导航信号区域的功能。

1　信号同步设计

干扰源需要结合微型计算机使用，来实现对接收到的真实卫星导航信号的信号强度、信号码相位以及载波相位等等信息进行计算分析，从而推算出干扰源发送出欺骗信号的干扰数据，包括延时、发送时刻、功率大小及多普勒频移等，从而使干扰源所生成的欺骗

信号与目标设备接收信号之间的数据相一致，对目标设备进行同步干扰工作。

1.1 欺骗信号模型设计

设定为欺骗信号的发布时间为t，干扰源所发出的信号模型如公式一所示：

$$X_{RF}(t)=\sum_{j-1}^{N(t)}\sqrt{2P(t)}\,C^{j}\left(t-T^{j}(t)\right)$$

$$D^{j}(t-T^{j}(t))\cos(\theta^{j}(t))+n(t)$$

公式一：欺骗信号模型

在该公式中，$N(t)$所表示在干扰源工作的时刻可以向被干扰对象发射导航信号的卫星数，P_2^j表示在干扰源工作的时刻卫星j发射的导航信号强度，$C^{j}\left(t-T^{j}(t)\right)$表示卫星$j$所获取的目标设备的伪随机编码，表示干扰源在工作时刻卫星j伪随机码的传播延时情况，表示卫星j向目标设备所发送的导航信号强度，则表示在干扰源工作的过程中所产生的随机噪音。

1.2 信号同步方法

为了实现信号同步功能，其中，在本文中还使用了一种本地授时型接收机作为配合，该接收机被用作基准时钟以及接收1PPS信号脉冲。同步式欺骗信号生成的具体操作步骤如下述：①干扰源通过本地授时型接收机获取卫星时刻与目标设备系统中的时刻，在计算机中进行对比工作，如果对比数据一致则进行步骤二的操作；②干扰源将来自于授时接收机的1PPS信号和10MHz时钟作为FPGA的数字信号合成以及射频Agent信号数据的基准和时钟源，通过此操作实现对目标设备原本应该接收到的时间同步，然后根据欺骗信号模型公式进行欺骗信号相关参数的计算工作，则继续进行第三步；③通过DDS技术对欺骗信号进行载波调制，从而实现对欺骗信号状态的控制；④通过DDS技术中所带有的FPGA功能进行多级调整，以此来模拟对方导航卫星与目标设备之间的多普勒变化；⑤根据延时计算，控制数据码、伪码的码片播发及载波相位的播发时间[1]。

通过上述五个步骤的应用可以基本实现欺骗信号与真实信号的同步工作。

2 实验分析

2.1 小型干扰源整体设计

在实际的设计过程中参考了现阶段技术较为成熟的异步生成式欺骗干扰源的设计结构，并且根据前文所示的欺骗信号模型进行同步生成式欺骗干扰源的建设工作，该种干扰源主要包含有四个模块，分别是：接收模块、信号处理模块、上变频以及射频调整模块、主控模块。

每个模块的功能如下所述：接收模块使用常见的授时型接收机接收目标设备的授时信息，并传给信号处理模板，以便干扰源系统时间与卫星系统时间实现同步，保证干扰源产生的干扰信号能与原信号在时间信息、大小信息、位置信息等相关的参数相一致。信号处理模块是干扰源的核心组成部分，信号处理架构采用了DSP+FPGA，信号处理模块的主要任务是接收同步时间信息、延时信息、多普勒频移信息等，并根据这些信息生成相对应的同步欺骗中频信号。上变频以及射频调整模块主要是完成信号的调整工作，将原本的中频信号变为射频信号。上位机主控系统实现人机交互，并且控制系统中的气压构件质检完成数据的交换；目标侦察系统主要对目标设备进行速度、大小、机器型号等信息的分析工作，并且自动地匹配相应的干扰方法，将相关信息传输给上位机主控系统[2]。

2.2 进行干扰试验

为了验证设计同步式欺骗干扰方式的可行性，选择在空旷的区域使用某民用接收机和某型号的大疆无人机进行测试工作。

对民用接收机的干扰试验：在进行试验工作之前，首先设置相关的实验参数然后再进行干扰信号的释放工作，观察接收机的运行状态，从而进行干扰效果的分析。干扰源设定的初始位置与接收机的真实位置一致，以便于接下来对照实验的进行，接收机的初始速度与加速度均为0，在原地保持静止状态。实验开始后，首先为干扰源接通了电源，经过测量发现干扰源所发出的欺骗信号强度小于民用接收机接收全球定位系统真实信号的强度，说明欺骗干扰效果有待加强，在此基础上加大了干扰源的工作频率，欺骗信号以2dB/s的速度增强提升8s，最终干扰信号强度与接收信号强度相持平，民用接收机接收干扰信号。在民用接收机接收干扰信号之后，调整欺骗信号所仿真的导航信息，在ECFF坐标系下，调整x轴的加速度为0.2m，民用接收机完成相应动作。在民用接收机接收干扰信号之后测试欺骗信号与真实信号之间时间同步信息，具体的操作方法为：①使用两台接收机进行对照试验，一台接收欺骗信号，另一台接收真实信号，输入两个信号所带有的秒脉冲；②使用示波器对两个秒脉冲的对齐精度进行测试，经过多次对照实验，干扰源所发出的欺骗信号与真实信号之间的秒脉冲的误差能够小于1毫秒，这表明由干扰源所发出的欺骗信号能够与真实

信号保持时间上的同步，从而得出同步式欺骗干扰方式有其可行性。

需要对欺骗信号强度变化对接收机跟踪环路的影响进行研究，选择的试验区域所产生的热噪音情况较为稳定，在这样的背景之下可以选择使用射频信号的载噪比来体现接收机接受干扰信号的强度。所以在同步适应阶段，选择了通过测试接收机接收信号载噪比的变化数据进行记载分析，从而能够推断出欺骗信号强度变化对接收机跟踪环路的影响，方便进行下一阶段的研究工作，并且设计降低周围噪音干扰的技术。具体的数据收集方法步骤如下所示：①接收机的射频输入端同时开启，接收机为位置保持在干扰源的上方，可以使接收机连接卫星信号的天线与干扰源的信号输出，使干扰信号与真实导航信号同时输入到接收机系统内，进行载噪比的集聚。②关闭干扰源的电源，中断干扰信号的输出工作，从而使得接收机只接收真实卫星信号，此时记录干扰源关闭之后接收机载噪比的变化情况，数据的记录直至接收机输出真实位置信息。③接下来再次为干扰源接通电源，并且在开启电源的一瞬间进行数据记录工作，逐渐加大欺骗信号的强度，记录三组不同的载噪比数据。选择的目标接收机型号为w331，开启干扰电源五秒之后，欺骗性好的强度保持着每秒2dB的增长速度，增长的时间为8s，从所收集到的数据中心发现，在1-4s的阶段，欺骗信号强度低于真实信号强度时，接收机产生的载噪比比小于43dB·Hz，在第5s的时候，欺骗信号的强度开始逐渐拉升，但是由于其强度仍然略小于真实信号强度，因此此时接收机的载噪比没有产生较大的变化，当到第7s的时候欺骗信号的强度开始大于真实信号强度，这个时候接收机产生的载噪比明显增大，欺骗信号开始在接收机的系统内占主导地位。由此我们可以得知可以在欺骗信号的强度为4dB/s是最佳干扰强度，既能避免被对方观察机通过机器噪音的排查所发现，还能在机器的信号接收中占据主导地位，从而实现欺骗干扰作业[3]。

2.3 民用无人机的干扰试验

选择使用某型号的大疆民用无人机进行静止和预定飞行航线状态下的干扰效果测试。

静态干扰测试结果：在开启无人机电源飞行到指定位置之后，使其接受由自带控制器所释放的真实导航信号，等到其固定在干扰源上方5m的位置时进行干扰源的电源通电，通过大疆无人机所自带的调教参数软件来观察无人机定点飞行在干扰源介入的情况下是否会产生距离的变化，实际的变化情况如图1所示：

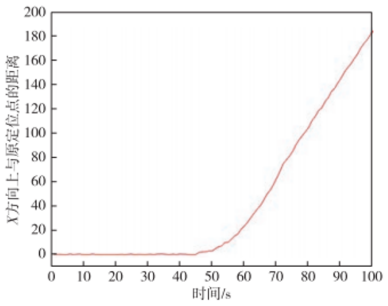

图 1　大疆无人机定点飞行接受干扰之后的检测轨迹

从图一所展现的数据中我们不难看出，在50秒之前干扰源并没有接入电源，所以在0-50s时大疆无人机一直处于干扰源上方5m的位置，并且定位点与原定位点的距离为0，这说明在这一段时间内大疆无人机在原本的位置上没有发生明显变化，大疆无人机能够在无干扰源的情况下，于同一位置保持定点静态飞行。而在50s之后开启干扰源，通过图一我们能够观察到在50s之后无人机的定位点产生了明显的变化，并且定位点与设定好的定位点之间的差距过大，这说明干扰源已经实现了对无人机的同步式欺骗干扰，并且对其输出的定位信息进行干扰，实验效果成功[4]。

在进行动态干扰实验之前首先简单地进行了动态干扰仿真实验，仿真基于MATLAB平台进行，仿真针对的是一段匀速运动的目标接收机，分别加入北向、东向的匀速干扰，并得出结论，通过仿真结果显示，实施干扰欺骗信号可以将目标接收机逐步拉向预设轨迹。如图2、图3所示。

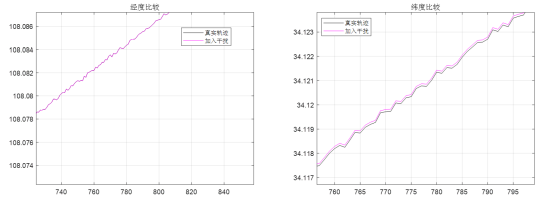

图 2　加入北向正向的干扰仿真图

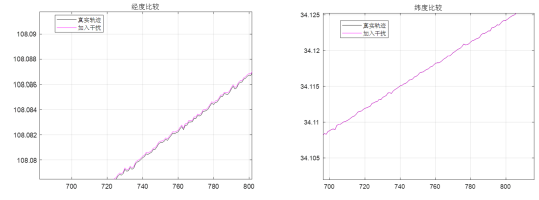

图 3　加入东向正向的干扰仿真图

动态干扰测试结果：为了能够进一步保证该实验进行的合理性，选择在同样的噪音环境中进行检测试验，并且使用同型号的大疆无人机，设定无人机将会从A点沿着直线匀速飞行到D点，航线的长度为100m，预设的无人机飞行的速度为1M/S，无人机从A点出发

（下转第30页）

求。另外，为了有效地缩短软硬件、计算机体系之间的差距，同样要对各类组件展开更新，满足基本的使用需求。承接各类软件的运营商要从自身出发，积极做好优化处理，而且还要及时地查找漏洞，避免软件受到侵害，这也能提高安全属性，为用户的操作带来保障。

4 结语

总之，大数据时代下做好网络计算机安全防护工作至关重要，这个关系到了人们的生活、工作与学习，其中要构建计算机安全网络体系，从不同的角度出发，避免计算机受到病毒、黑客所带来的侵扰，同时还要提高其安全属性，加强对软硬件的更新，实现病毒的查杀，选择各类加密技术与身份验证技术等，如此，能够真正减少网络安全问题的出现。

参考文献

[1] 胡美正.浅析大数据时代的计算机网络安全及防范措施[J].电脑知识与技术,2020,16(36):38-40.
[2] 陆欢荣.云计算环境下的计算机网络安全防范研究[J].网络安全技术与应用,2021(08):76-77.
[3] 齐红.大数据时代下计算机网络安全防范的研究[J].中小企业管理与科技(上旬刊),2021(10):104-106.
[4] 肖承望.中职院校计算机信息网络安全技术和安全防范策略探讨[J].网络安全技术与应用,2021(11):99-100.
[5] 刘雷,董超.大数据时代背景下计算机网络安全防范应用与运行[J].网络安全技术与应用,2019(06):51-53.
[6] 宋人愚.人工智能时代高校计算机网络信息安全问题研究[J].计算机产品与流通,2019(06):209.
[7] 葛小虎.关于计算机网络安全防范中防火墙技术的应用分析[J].网络安全技术与应用,2019(11):21-23.
[8] 吴欣妍,薛峰,刘琦.关于计算机网络通信安全问题分析与防范策略探讨[J].电脑知识与技术,2019,15(28):47-48+55.
[9] 王国庆,陈辉.试谈大数据时代的计算机网络安全及防范措施[J].IT经理世界,2020,23(3):102.

（上接第26页）

时，干扰源释放强度较低的干扰信号，通过观察发现无人机继续沿着设定好的航线飞行至AD线之间的B点处（详情如图4所示），说明该干扰信号并没有对无人机的正常飞行产生影响，当无人机飞行过B点时，开始进行欺骗信号强度的增强，每秒增加1dB，持续时间为10s。无人机仍然按照既定的航线进行飞行作业，不过通过载噪比的数据对比发现这个时候无人机已经接入了欺骗信号，并且在系统内占据主导定位，预设航线数据被影响。这个时候干扰源对无人机进行欺骗信号数据的改变，诱导无人机偏离原本预设的航线向西南方向飞行，并且干扰时间为5s，在这之后可以明显地观察到无人机偏离了原本的航线，说明欺骗干扰试验成功。

3 结论

在本文的论述中以欺骗干扰技术为基础进行了干扰型号模型的而设计，通过民用接收机以及大疆无人机作为实验对象进行可行性验证，结果表明，基于不需要对正确信号压制的情况，就可以成功实现对目标设备的

图 4 动态干扰测试中无人机航线的设定

干扰，从而使其偏离原本的航向，具有较高的可行性。

参考文献

[1] 马海宁，潘颜楠，孙志.基于欺骗干扰技术的导航对抗新途径[J].指挥控制与仿真，2021,43(4):67.
[2] 胡洪涛，李正杰，兰竹.基于卫星导航欺骗干扰的无人机诱捕技术[J].电子信息对抗技术，2020,35(2):16-17.
[3] 陈保豪，李任新.基于卫星导航欺骗干扰情况下的无人机管制技术研究[J].信息系统工程，2019(10):156.
[4] 施林，刘伟.基于卫星导航欺骗干扰的无人机管制技术[J].指挥信息系统与技术，2017,8(1):78-79.