GNSS欺骗攻击综述

郑辉根，张春磊，李子富，张　慧，王雪琴

（中国电子科技集团第三十六研究所，浙江 嘉兴 314001）

摘要： 全球导航卫星系统（GNSS）所提供的定位、导航、授时（PNT）能力已成为军用、民用领域内不可或缺的关键能力。随着电磁环境越来越呈现出复杂多变的特性，GNSS面临诸多现实威胁，其安全性问题备受关注。GNSS欺骗作为一种重要的电子攻击方式，具备隐蔽性强、破坏力大、技术成熟等特点，对GNSS安全性造成了很严重的影响。围绕GNSS欺骗这一主题，论述了GNSS的重要性和脆弱性，概述了GNSS电子对抗策略和GNSS欺骗基本原理，将GNSS欺骗大致分为3类，即信号处理级欺骗攻击、数据比特级欺骗攻击和基于预测的攻击，并对常见的GNSS欺骗类型进行了介绍，旨在形成对GNSS欺骗全面的理解和认识。

关键词： GNSS；GNSS欺骗；GNSS安全性；欺骗攻击

中图分类号： TN972^{+}.3　　**文献标识码：** A

DOI:10.16328/j.htdz8511.2020.04.008

An overview of GNSS spoofing

Zheng Huigen，Zhang Chunlei，Li Zifu，Zhang Hui，Wang Xueqin

（No.36 Research Institute of CETC，Jiaxing 314001，Zhejiang，China）

Abstract： The positioning，navigation and timing capabilities provided by GNSS have become indispensable in the military and civilian fields. With the electromagnetic environment becoming more and more complex，GNSS faces a lot of real threats. Security issues of GNSS have attracted much attention. As an important electronic attack method，GNSS spoofing is concealed，destructive and has mature technologies，which can heavily impact the security of GNSS. Focusing on the topic of GNSS spoofing，a comprehensive understanding of GNSS spoofing is introduced. The importance and vulnerability of GNSS are discussed. Strategy of GNSS electronic attack and fundamental principle of GNSS spoofing are outlined. GNSS spoofing is roughly divided into three categories：signal processing level spoofing attack，data bit level spoofing attack and attack based on prediction. In addition，common types of GNSS spoofing attack are introduced.

Key words： GNSS；GNSS spoofing；security of GNSS；spoofing attack

0　引言

全球导航卫星系统（GNSS）所提供的定位、导航、授时（PNT）能力已成为军用、民用领域内不可或缺的关键能力。正因如此，GNSS的安全性（包括物理安全性、电磁安全性、赛博安全性等）也成为各国在发展GNSS时重点关注的性能之一。而随着GNSS干扰（jamming）、欺骗（spoofing）、赛博攻击等技术不断扩散且成本不断降低，GNSS安全性问题越来越严重。

近年来，GNSS欺骗技术、方法不断涌现，欺骗事件也层出不穷，对GNSS安全性造成了很严重的影响。而GNSS欺骗具备隐蔽性强、破坏力大、技术成熟等特点，已成为攻击者最青睐的攻击方式之一。与GNSS欺骗相比，干扰、赛博攻击等方式“劣势”明显：干扰容易被检测到，隐蔽性差，被攻击者容易找寻替代方案；赛博攻击对技术要求较高，且效能不具备持续性。

1　GNSS发展意义

从1960年美国发射世界上第一颗导航卫星“子午仪”（transit）算起，GNSS已经发展了将近60年，目前已经形成了以美国GPS系统、中国“北斗”系统、俄罗斯“格洛纳斯”系统、欧洲“伽利略”系统、日本“准天

收稿日期：2020-05-14；2020-07-15修回。

作者简介：郑辉根（1961—），男，高工，主要研究方向为通信对抗技术。

顶”卫星系统、印度区域导航卫星系统(RNSS)等为代表的体系。

GNSS的PNT能力几乎已经渗透到了所有电子信息领域内,如果没有GNSS,很多正常的军事、商业活动都无法开展。2012年,美国国土安全部曾经开展过一项关于GPS依赖性的专项研究,并指出“美国19个关键基础设施、关键资源机构中,有15个都不同程度地利用GPS来提供授时信息”(如图1所示)。除了授时以外,GNSS所提供的定位、导航能力的应用领域实际上更为广泛。

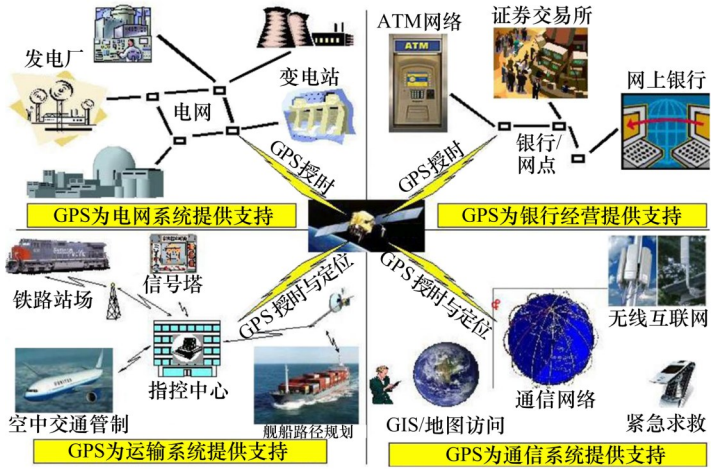

图1　美国关键基础设施等对GPS的依赖性

另外,从GNSS相关产业规模的不断扩大也可以看得出GNSS的重要性。根据相关研究,2025年GNSS产业规模(包括设备、增强服务、增值服务)或将达到近2800亿美元,如图2所示。

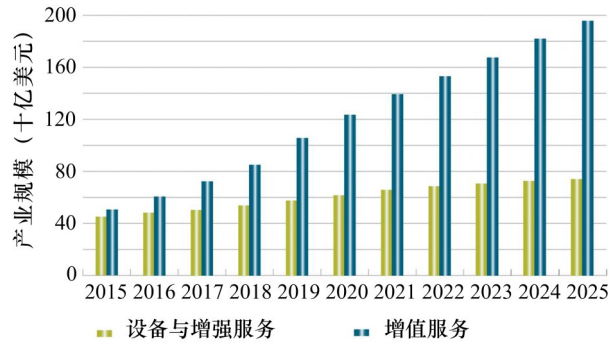

图2　全球GNSS产业规模发展预测

2　GNSS脆弱性分析

作为一种工作于开放式电磁环境中的用频系统,GNSS系统存在多方面脆弱性。除了可能遭受动能武器等的“硬杀伤”攻击以外,GNSS系统还可能遭受多种“软杀伤”攻击,包括电磁干扰、电磁欺骗、赛博攻击、多径衰落、大气活动影响等,如图3所示。其中,电磁欺骗事件近年来不断涌现,成为GNSS系统面临的主要威胁之一。

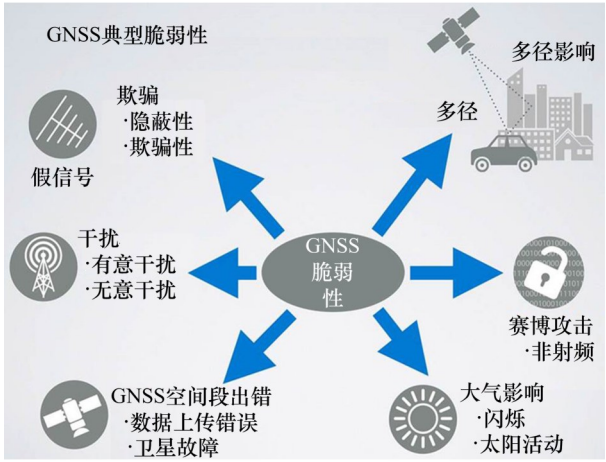

图3　GNSS典型脆弱性

3　GNSS对抗策略研究

GNSS欺骗属于GNSS电子攻击方式中的一类。关于GNSS欺骗与GNSS干扰之间的关系,有2种主流理解方式:其一,GNSS欺骗属于GNSS干扰的一类,称作欺骗式干扰,与GNSS拒绝服务式干扰并列;其二,GNSS欺骗与GNSS有意干扰(jamming)、GNSS无意干扰(interference)并列(本文即按照这一分类方法来介绍)。然而,不管从分类方面如何界定,从技术层面来讲,GNSS欺骗还是非常明确且清晰的。

目前,GNSS所面临的电子攻击威胁主要包括干扰和欺骗2类,而干扰则包括有意干扰与无意干扰2类。无意干扰指的是那些事实上阻止了GNSS信号接收的无意信号辐射,可以是带内干扰,也可以是带外干扰。有意干扰指的是旨在拒止GNSS接收机接收GNSS信号的有意信号辐射。欺骗(干扰)指的是旨在让GNSS接收机报告错误位置或时间信息的欺骗性活动。

上述三种攻击策略针对的都是GNSS接收机(通用框图如图4所示),而GNSS欺骗的前期环节重点针对GNSS信号的捕获与跟踪环节开展攻击。在遭受干扰的情况下,GNSS接收机主要会受到如下3方面影响:其一,由于载噪比(CNR)性能下降,导致跟踪丢失、可用观测量减少、出现周跳(Cycle Slips)现象;其二,编码与相位观测量中的噪声增加,导致定位、导航

与授时精度下降；其三，捕获时间变长，导致接收机启动到实现首次定位的时间变长。

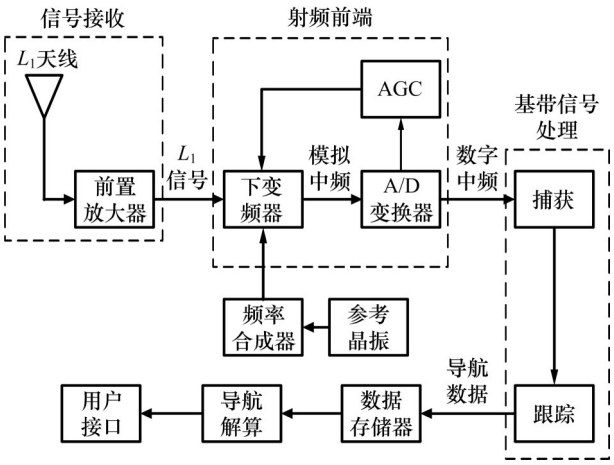

图4　GNSS接收机通用框图

3.1　GNSS欺骗基本原理

GNSS欺骗尚没有精准的定义，其中，“欺骗”(spoofing)借用的是信息安全领域(尤其是网络安全领域)中的“欺骗攻击”(spoofing attack)。在信息安全领域内，“欺骗攻击”指的是一个人或一个程序利用数据篡改成功伪装成另一个人或另一个程序的过程，其目的是获取情报。

GNSS欺骗攻击与信息安全领域内的欺骗攻击手段相类似，其最终目标是欺骗遭受攻击的GNSS接收机。具体方式包括：向GNSS接收机广播错误的GNSS信号，但这些信号经过了特殊设计，与正常的信号相似；向GNSS接收机转发从其他时间、其他地点截获的真实信号。遭受欺骗的GNSS接收机则会计算出一个错误的位置或错误的时间。典型的GNSS欺骗攻击设备如图5所示。

导航接收机的信号处理过程主要用到2方面信息，即调制的测距码(ranging code)和GNSS信号中所传递的导航数据信息。从这一角度出发，GNSS欺骗大致可分为如下3类。

1) 信号处理级欺骗攻击。民用GNSS信号的很多参数都是公开的，如，调制样式、伪随机码、发射频率、信号带宽、多普勒距离、信号强度等。因此，只要了解了某一GNSS接收机的通用结构和操作基础，欺骗干扰机就可以产生与真实GNSS信号类似的伪造信号，并可以通过改动目标接收机的各种参数(信号幅度、码延迟、多普勒频移、载波相位等)来对其实施有效的误导。

2) 数据比特级欺骗攻击。GNSS信号的帧结构是公开的，导航信号帧包含多种信息，如星历等。这类信息短期内不怎么变化，例如，尽管接收机在1 min之内即可捕获星历信息，但星历的持续时间却长达12.5 min。因此，欺骗干扰机可拥有足够的时间来伪造一个GNSS数据帧。

3) 基于预测的攻击。无论是信号处理级欺骗还是数据比特级欺骗，都基于这样一个前提，即，假定GNSS卫星发射的测距码和数据比特流已知。若信号采用了某些认证手段，则上述前提就不再具备。在这种情况下，欺骗干扰机就必须基于其接收到的包含噪声的信号来合成“近似的”测距码和比特流。要实现这一点，就需要用到基于预测的攻击。

3.2　GNSS欺骗常见类型综述

实际操作过程中，攻击者会综合利用上述攻击手段，以“引导”GNSS接收机计算出预期的“位置-速度-时间”(PVT)解。不同的组合会生成不同的GNSS欺骗类型。

3.2.1　信号处理级与数据比特级欺骗攻击

信号处理级欺骗攻击和数据比特级欺骗攻击这2种攻击手段的综合应用，可产生多种不同的攻击类型。

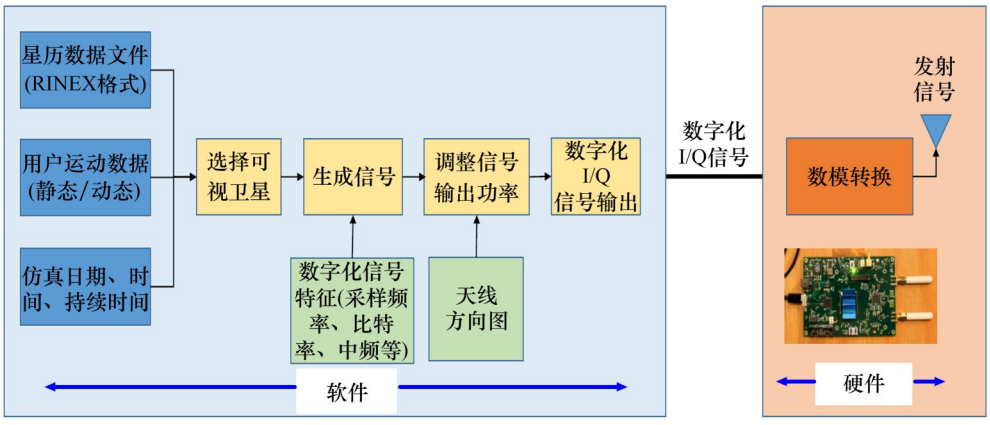

图5　典型的GNSS欺骗攻击设备

1) 延迟抬升(Lift-off-delay，LOD)欺骗攻击

延迟抬升(LOD)欺骗攻击过程中，欺骗干扰机通过如下方式伪造欺骗信号：一开始，欺骗信号幅度很小，且与实际信号之间存在相对延迟；然后，干扰机逐渐降低相对延迟，同时增加信号幅度；当欺

骗信号与实际信号之间没有延迟(相对延迟为零)且信号幅度相接近时,欺骗信号功率开始增加并逐渐超过真实信号功率,同时相对延迟也逐渐增加;最终,接收机的跟踪点离实际信号的参数越来越远(即,实现“抬升”)。这种欺骗干扰方式的原理与效果如图6所示,图中,欺骗攻击从$T2$开始发起。

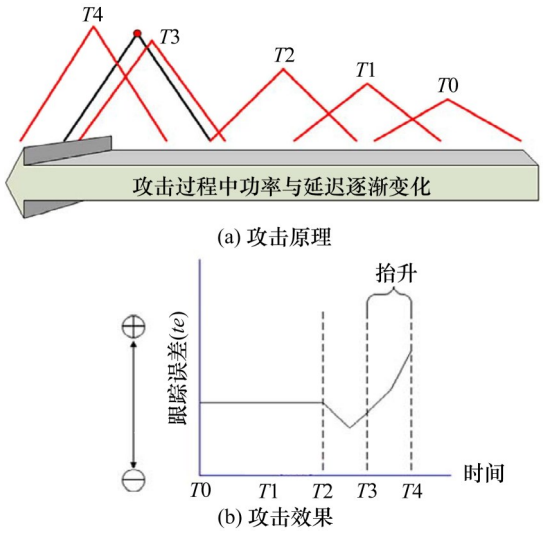

图6　LOD攻击原理与攻击效果

2) 对准抬升(Lift-off-aligned ,LOA)欺骗攻击

对准抬升(LOA)欺骗攻击攻击与“延迟抬升”攻击过程类似,只是在欺骗信号与真实信号幅度接近之前,欺骗信号与真实信号在时间上一直是对准的(相对延迟为零)。若这类欺骗信号突然出现,则会造成真实信号跟踪参数的剧烈变化。

对于处于信号捕获阶段的接收机而言,更容易遭受这种欺骗攻击。若这种欺骗攻击手段与自欺骗设备(self-spoofing device)搭配使用,则对于处于信号跟踪阶段的接收机也会造成很大影响。

3) 转发(MEAC)与选择性延迟(SD)欺骗攻击

转发(Meaconing)指的是首先利用接收设备记录下真实的GNSS信号,然后将该信号进行适当的延迟并放大以后再发射出去。这样,被攻击的接收机所定位的位置就是欺骗干扰机的位置。理论上说,这种欺骗方式对任何的GNSS信号都有效,即便是加密的军用信号亦是如此。转发欺骗攻击的原理如图7所示。

选择性延迟(selective delay)攻击可视作一种更加“高端”的转发攻击。欺骗干扰机利用多部接收天线并采用

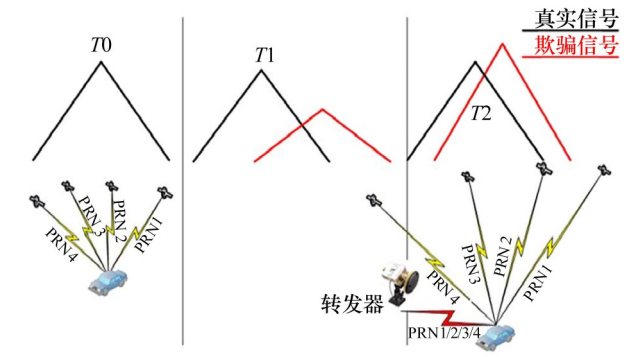

图7转发欺骗攻击原理图

相控阵信号处理技术来在单一信道中记录、转发每一颗导航卫星的信号。此外,欺骗干扰机也可以仅利用一部天线来接收,但通过跟踪不同的伪随机码来分离所接收到的多个信号。这种攻击方式可以独立操纵每一颗卫星的相对延迟,因此,理论上说可以产生任意的虚假位置。

实施选择性延迟攻击时,如果欺骗信号的幅度小于实际信号,则可产生“多径攻击”效果,因为此时欺骗信号看似是一个多径反射信号。这种情况下,尽管跟踪点仍在真实信号附近,但GNSS接收机的测距精确度会降低。

4) 干扰与欺骗(JAS)攻击

首先,欺骗干扰机通过大功率干扰迫使接收机进入信号捕获模式,并导致真实信号失锁,同时,干扰机还发射欺骗信号。然后,大功率干扰停止,以便目标接收机捕获到欺骗信号。

5) 非视距欺骗(NLOSS)攻击

在诸如城市等复杂环境下,接收机通常既无法跟踪到头顶所有卫星,也无法精确感知周边的障碍物情况,此时即有望对其发起非视距欺骗。此时欺骗干扰机发射的信号仅仅是那些可能被遮挡的卫星的信号,因此接收机很难发现欺骗信号的存在。非视距欺骗攻击原理如图8所示。

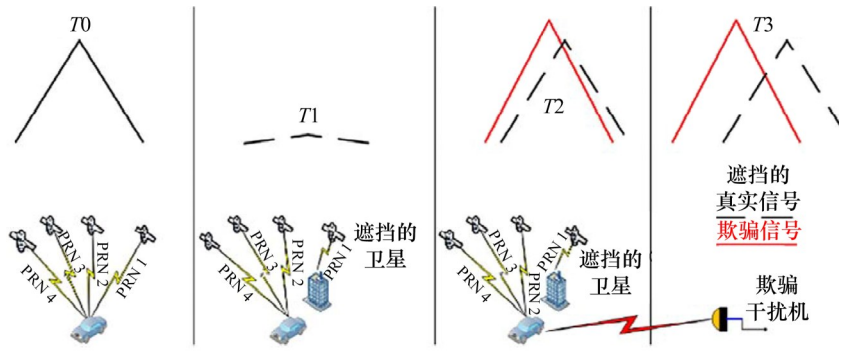

图8　非视距欺骗攻击原理图

6）轨迹欺骗攻击

除了转发欺骗以外，其它欺骗方式都可以独立生成多个欺骗信号，或者目标接收机利用这些信号还可以计算出同一个位置，后一种情况即称为轨迹欺骗。攻击者利用一套GNSS信号模拟器来沿着目标接收机的既定运行轨迹捕获其所有信道的跟踪点，这样，接收机用户就会沿着欺骗的轨迹移动。这种情况下，欺骗干扰机必须连贯产生特定轨迹所需的所有欺骗信号，以使得卫星距离连贯性技术失效。

7）调零欺骗攻击

欺骗干扰机发射的每个欺骗信号中都包含2个信号：一个信号用来欺骗目标接收机，以使其计算出错误的位置、时间；另一个信号用来抵消真实的信号。这样，就可以从目标接收机所接收的信号中彻底消除真实信号的所有痕迹。

8）多天线欺骗攻击

这种欺骗方式主要针对的是那些具备多天线接收能力的GNSS接收机，而这类接收机通常会具备很强的抗欺骗能力，如，基于信号到达方向的抗欺骗能力。实施欺骗时，每一部欺骗干扰机天线都对准接收机的某一部特定的天线，而且欺骗天线的定向性必须非常强以确保欺骗信号之间的方向隔离度。此外，欺骗天线与目标接收机天线之间的位置也必须精心计算，以确保欺骗信号的到达方向从物理上来看比较合理。

综合来看，多天线欺骗必须具备如下几方面前提：欺骗天线与接收机天线之间的相对位置需精心设计；欺骗干扰机距离目标接收机必须足够近；欺骗天线波束必须足够窄（定向性足够高）。总之，这种欺骗实施起来非常困难，需结合谍报人员才具备可行性。

3.2.2　基于预测的欺骗攻击

基于预测的欺骗攻击主要包括验证码估计与重放（SCER）攻击、前向估计攻击（FMA）、状态建模攻击（SMA）等。

1）验证码估计与重放（SCER）欺骗攻击

这种攻击方式通过观察所接收到的自由空间信号来估计验证码或加密数据比特。一旦攻击者得到了可靠的估计值，就立刻将其注入欺骗信号发生器中，并生成欺骗信号。

2）前向估计攻击（FMA）欺骗攻击

验证码估计与重放攻击关注的是从接收信号的一个个“片段”（如，一个个符号），并未充分利用这些片段之间的相关性。而前向估计攻击则主要利用某些GNSS信号中所采用的前线纠错编码（FEC）所带来的冗余度，以实现码字中后续符号的预测。

3）状态建模攻击（SMA）欺骗攻击

尽管攻击者可能预测出足够的导航信号符号来发起欺骗攻击，但无法预测所有的符号。因此，目标接收机可以利用这一点来实现抗欺骗，即，实施基于相关的信号验证。这种验证方法将接收到的符号与接收机中真实的安全相关符号进行相关运算，若收到的信号是真实信号，则相关运算会得出一个特定均值的高斯分布。

状态建模攻击则利用了这样一个事实：接收机无法区分是哪个符号内累计的能量。攻击者基于从此前接收到的符号中计算出的相关值先验知识，对每个欺骗符号的幅度进行调节，即可以产生欺骗效果显著的欺骗信号。

4　结束语

随着GNSS抗干扰技术的不断发展，GNSS的抗干扰性能得到了极大提高，同时，这也对GNSS干扰技术的发展提出了新的挑战。但不管GNSS系统如何发展，鉴于其运作环境复杂、信号不完善，总是存在脆弱性，存在着被欺骗干扰的风险。如何发展低成本、高效能的GNSS干扰技术，如何利用各种欺骗干扰技术，进行精确攻击，将是未来导航对抗的一项发展重点。■

参考文献：

[1] Yuan DB, Li H, Wang F, et al. A GNSS acquisition method with the capability of spoofing detection and mitigation[J]. Chinese Journal of Electronics, 2018, 27(1): 213-222.

[2] Perdue L, Sasaki H, Fischer J. Testing GNSS receivers to harden against spoofing attacks[C]//Kyoto, Japan: International Symposium on GNSS 2015, 2015.

[3] Psiaki ML. Techniques for spoofing and for spoofing mitigation[R]. Report on the ENAC/SIGNAV Nav. & Timing Symposium, 2015.

[4] Mahmood S. Critical infrastructure vulnerabilities to GPS disruptions[R]. Homeland Security Advanced Research Projects Agency, 2014.

[5] Psiaki ML, Powell S P, O'Hanlon BW. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data[C]//26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+), 2013.

（下转第45页）

建模仿真，通过研究同一分辨单元内的不同散射点的相对幅度变化情况，得出了调制系数和测角关系曲线以及调制系数和测角误差曲线，进一步描绘了调制系数和测角误差的相对关系。可为目标防护和材料的设计提供参考，对于提高目标战场生存能力具有一定的意义。■

参考文献：

[1] 黄虹.单脉冲雷达[M].北京：国防工业出版社，1974.

[2] 周颖，陈远征，赵峰.单脉冲测向原理与技术[M].北京：国防工业出版社，2013.

[3] 鲍卓如.有源频率选择表面关键技术研究[D].南京：南京航空航天大学，2012.

[4] 张厚，尹卫阳.频率选择表面在天线及微波技术中的应用[J].空军工程大学学报(自然科学版)，2019，20(5)：70-75.

[5] 黄培康，殷红成.扩展目标的角闪烁[J].系统工程与电子技术，1990(12)：1-17.

[6] 刘恩凯，何梅昕.相干双点源干扰下的单脉冲雷达测角误差研究[J].舰船电子对抗，2019(4)：20-23.

[7] 强宇，周东方，刘起坤，等.一种新型宽带吸收频率选择表面[J].强激光与粒子束，2019，31(10)：1-6.

[8] 郑万清.低RCS频率选择表面的分析与实现[D].成都：电子科技大学，2018.

(上接第10页)

[6] 通信辐射源瞬态特征提取和个体识别方法[J].西安电子科技大学学报(自然科学版)，2009，36(4)：736-740.

[7] 车金鸽.基于深度学习的雷达辐射源识别[D].西安：西安电子科技大学，2019.

[8] 田得雨.基于深度学习的通信信号调制类型识别研究[D].西安：西安电子科技大学，2019.

[9] 曹向海，刘宏伟，吴顺君.基于奇异值分解的双谱降维研究[J].宇航学报，2007，28(5)：1319-1322.

[10] Wang X，Huang G，Ma C，et al. Convolutional neural network applied to specific emitter identification based on pulse waveform images[J].IET Radar，Sonar & Navigation，2020，14(5)：728-735.

(上接第34页)

[10] 冉小辉，朱卫纲，邢强.电子对抗干扰效果评估技术现状[J].兵工装备工程学报，2018，39(8)：117-121.

[11] 汤广富，安红，焦志.基于层次分析法的协同干扰效能评估[J].电子信息对抗技术，2016，31(4)：58-62，78.

[12] 车飞.认知对抗中干扰效益评估与智能决策方法研究[D].哈尔滨：哈尔滨工程大学，2019.

[13] 马嘉呈，姚登凯，赵顾颢，等.基于离散粒子群算法的战术训练空域规划问题[J].火力与指挥控制，2018，43(12)：94-98.

[14] Gopal A，Sultani MM，Bansal JC. On stability analysis of particle swarm optimization algorithm[J].Springer Berlin Heidelberg，2020，45(2).

[15] Kennedy J，Eberhart R C.A discrete binary version of the particle swarm algorithm[C]//Proceeding of the World Multiconference on Systemics，Cybernetics and Informatics，New Jersy：Piscataway，1997：4104-4109.

[16] 董丽凤，陈阳，巫光福.动态学习混沌映射的粒子群算法[J].计算机应用研究，2019，36(5)：1319-1322.

[17] Dorota A. New discrete chaotic multiplicative maps based on the logistic map[J].World Scientific Publishing Company，2018，28(9).

[18] 印桂生，崔晓晖，董宇欣，等.面向离散优化问题的改进二元粒子群算法[J].哈尔滨工程大学学报，2015，36(2)：191-195.

[19] 陈曼，周凤星.改进粒子群算法的舰载武器目标分配[J].火力与指挥控制，2018，43(11)：72-76.

(上接第39页)

[6] Rügamer A，Kowalewski D. Jamming and spoofing of GNSS signals——an underestimated Risk?[C]//Sofia，Bulgaria：Wisdom of the Ages to the Challenges of the Modern World，2015.

[7] Frost T，Buesnel G. The vulnerability of GNSS timing receivers to spoofing attacks[R]//San Jose，CA，USA：Report on the Workshop on Synchronization and Timing Systems(WSTS 2016)，2016.

[8] Frost T，Buesnel G. Spoofing GNSS timing receivers[R]//Report on the 2015 International Telecom Sync Forum(ISTF 2015)，2015.

[9] Chiarello L. Security evaluation of GNSS signal quality monitoring techniques against optimal spoofing attacks[D]. Italy：Università degli Studi di Padova，2018.