MagDet:基于地磁的无人机GPS欺骗检测方法

魏晓敏 李兴华 孙 聪 张海宾 马建峰
(西安电子科技大学网络与信息安全学院 西安 710071)

摘 要 GPS是目前最为广泛使用的基于卫星的导航和定位系统,对于无人机而言,它是一个不可或缺的组成部分,提供了关键的精确位置数据,对导航和任务的成功至关重要.然而,GPS欺骗攻击已经逐渐演变成对GPS依赖系统不断增加的威胁.目前,针对无人机的GPS欺骗检测方法大多基于仿真数据提出、依赖于多个无人机或者需要专用设备(例如,软件定义无线电平台和高清摄像头).本文提出一种新颖的基于地磁场的无人机GPS欺骗检测方法——MagDet(Magnetic field-based Detection method),其基本思想是利用地球内部和周围金属建筑材料不均匀性引起的地磁场异常,通过真实飞行收集位置和磁场强度数据,包括正常和被攻击场景.应用各种机器学习算法来训练这些数据以选择最佳分类器,该分类器可以轻松部署在常见机载计算机中.该方法的检测率超过99.5%,平均错误率(Equal Error Rate,EER)为0.51%,优于现有检测方法.此外,评估了各种因素对MagDet的影响,以证明其鲁棒性.即使在未访问过的地点(距离6 km),准确率也高于95%,EER为0.49%.

关键词 GPS欺骗检测;地磁;无人机;GPS欺骗攻击;机器学习
中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2024.00877

MagDet: UAV GPS Spoofing Detection Based on the Geomagnetic Field

WEI Xiao-Min LI Xing-Hua SUN Cong ZHANG Hai-Bin MA Jian-Feng
(*School of Cyber Engineering, Xidian University, Xi'an* 710071)

Abstract GPS is currently the most widely used satellite-based navigation and positioning system. For unmanned aerial vehicles (UAVs), it is an indispensable component, providing crucial and precise location data that is essential for the success of navigation and missions. However, GPS spoofing attacks have gradually evolved into a growing threat to GPS-dependent systems. Most existing GPS spoofing detection methods for UAVs are proposed based on simulation data, and they depend on multiple UAVs or require dedicated devices (e.g., software-defined radio platform and high-definition camera). In this paper, we propose a novel GPS spoofing detection framework, MagDet, for a UAV based on the geomagnetic field. Our basic idea is to use the geomagnetic field anomalies due to inhomogeneities within the Earth's interior and surrounding metal material. We collect positions and the strength of magnetic field through real flights including normal and attacked scenarios. Various machine learning algorithms are applied to train with these data to choose the best classifier, which can be easily deployed in common companion computer. The detection rate is more than 99.5% and the equal error rate (EER) is 0.51%, which is better than existing methods. We also evaluate various factors on MagDet to demonstrate the ro-

收稿日期:2023-06-29;在线发布日期:2024-01-16.本课题得到国家自然科学基金(No.62125205,62272366,62232013)、中央高校基本科研业务费专项资金(No.ZYTS24141,ZYTS23165)和陕西省重点研发计划(No.2023-YBGY-371)资助.**魏晓敏**(**通信作者**),博士,讲师,中国计算机学会(CCF)会员,主要研究领域为GNSS欺骗检测、系统安全、嵌入式软件、无人系统.E-mail:xmwei@xidian.edu.cn.**李兴华**,博士,教授,国家杰出青年科学基金入选者,中国计算机学会(CCF)会员,主要研究领域为无线网络安全、隐私保护、应用密码学.**孙 聪**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为信息流分析、可信软件、程序分析与验证、无人系统安全.**张海宾**,博士,教授,主要研究领域为人工智能安全、工业互联网安全、可信计算.**马建峰**,博士,长江学者特聘教授,中国计算机学会(CCF)会员,主要研究领域为应用密码学、无线网络安全、数据安全、移动智能系统安全.

bustness. Even in an unvisited site (6 kilometers away), the accuracy is higher than 95% and the EER is 0.49%.

Keywords GPS spoofing detection; geomagnetic field; Unmanned Aerial Vehicle; GPS spoofing attacks; machine learning

1 引 言

全球卫星导航系统(Global Navigation Satellite System,GNSS)是世界上最常用的定位、制导和导航系统.全球导航卫星系统包括美国的GPS、中国的北斗、俄罗斯的格洛纳斯和欧盟的伽利略等几种类型.鉴于大多数无人机使用GPS,本文将重点关注针对GPS的欺骗攻击.

由于GPS在其最初设计时并未考虑对安全威胁的鲁棒性,因此依赖GPS进行无人机导航和定位时,面对安全威胁和攻击显得极为脆弱.尤其是民用GPS系统极易受到欺骗攻击的影响,这一问题在相关文献中得到了广泛关注[1-2].攻击者可通过生成并传输虚假的GPS信号,从而控制无人机导航系统,通过伪造位置信息欺骗无人机,导致其误入错误的目的地.大量研究表明,GPS欺骗攻击在各种应用场景中都得到了体现,包括操控无人机导航系统[3]、诱导游艇航向控制系统[4]、攻击道路导航系统[5-6]以及操纵自动驾驶汽车的多传感器融合系统[7].同时,用于发起GPS欺骗攻击的设备的成本逐渐降低,相应的技术手段也越来越普及.例如,软件定义无线电(Software-Defined Radio,SDR)设备和公共的GPS信号生成代码库(GPS-SDR-SIM[8])已成为实现GPS欺骗攻击的常见工具.有研究团队甚至使用了一种成本仅约200美元的便携式可编程欺骗器,即可轻松实施对GPS信号的欺骗[5].

为应对无人机GPS欺骗攻击威胁,研究人员已经提出了多种解决方案.然而,令人遗憾的是,大多数方法主要基于仿真数据进行设计与验证,而这些仿真数据与真实数据存在显著差异,可能忽略了真实飞行场景中的细节.由于仿真平台难以完全模拟真实环境的各种变化因素,这可能导致不同的控制参数和无人机姿态的出现.另外,一些异常检测的研究需要额外的外围设备,用于收集感知数据,例如图像(参见文献[9])和GPS信号特征(参见文献[10]和文献[11]).此外,有些研究利用多个无人机的协作来检测欺骗攻击[12-13].另一方面,一些研究人员试图通过建立各种传感器数据之间的理论关系来设计检测器[14].然而,这些传感器本身存在一些固有的缺陷,这些缺陷可能会降低测量数据的准确性.例如,加速度计数据具有累积误差,而陀螺仪则存在传感器漂移的问题.已有研究建议通过使用其他GNSS信号对GPS信号进行交叉检查,以提高检测的可靠性,但即便如此,被使用的GNSS信号也可能受到欺骗的威胁.

为实现一种健壮可靠的检测方法,本研究尝试解决以下关键挑战:(1)在确保机载传感器(加速度计和陀螺仪)固有缺陷不会降低检测准确率的情况下,如何在不需要任何额外设备而仅使用现有机载设备检测GPS欺骗攻击?(2)如何收集真实飞行数据来支持检测方法的设计、实现和评估?

本文提出一种利用磁场波动检测GPS欺骗攻击的方法.它基于地球内部不均匀性和周围金属材料所引起的地磁场异常[15].每个地理位置都可大致与一种地磁异常模式相关联,而这种模式被称为地磁指纹[16].利用地磁指纹与位置的映射关系,不仅可以辅助定位和导航系统,还可以在GNSS拒止环境中基于地磁进行定位和导航[16-18].依据无人机三维位置与地磁指纹之间的关系,本文提出一种基于地磁场的无人机GPS欺骗攻击检测方法——MagDet.由于MagDet仅依赖周围磁场和无人机三维位置,因此在不需要其他任何特殊基础设施或外部传感器的辅助下,依然可以准确完成无人机GPS欺骗检测.此外,大多数无人机已经配备用于收集磁场强度的磁力计、用于测算经纬度的GPS接收机和用于测量高度的气压计,这使得MagDet更加易于部署.

为分析GPS位置(正常或欺骗)和磁场强度的相关性,应通过无人机飞行收集真实数据,而非仅使用仿真.但根据政府无线电管理规定,禁止在室外环境实施GPS欺骗攻击实验.因此,本文设计并实现了一种基于软件注入技术的GPS欺骗攻击,可直接修改飞控固件中的真实GPS位置.通过实验已经成功收集了正常飞行和欺骗攻击飞行场景下的飞行数据.

无线卫星信号容易受到干扰和障碍物遮挡的影

响,且惯性测量单元具有累积误差,而磁场无处不在,其高可用性可以帮助避免这些问题、提高定位精度.当大型金属建筑物不变时,周围磁场随时间保持不变[16].因此,地磁导航技术可以辅助 GPS 进行定位和导航[19].然而,基于磁场的导航系统需要一个真实的地面磁场地图来确定位置[16,20-22].这张地图是通过记录磁异常模式及其对应的位置信息来构建的.建立这样一张地图是困难且耗时的,需要具有高灵敏度的专业设备(例如,光泵铯磁力计[23]),而 MagDet 不依赖于磁场地图.

为有效检测欺骗攻击,本文深入挖掘磁场强度、三维位置及其变化规律的数据特征.然后,使用多种机器学习算法进行训练并选择最佳分类器实现 GPS 欺骗检测.

据现有文献可知,MagDet 是第一个利用磁场对无人机进行 GPS 欺骗检测的方法.本研究的贡献如下:

(1)提出一种全新的无人机 GPS 欺骗检测方法,从理论和实验的角度分析基于地磁场强度识别无人机位置的可行性,并提高特征选择有效性.

(2)开发一种基于地磁场的检测方法——MagDet,通过实际飞行实验收集无人机真实数据,经过预处理、提取特征和模型训练生成欺骗检测器;部署于无人机的方式简单,无需额外设备.实验结果表明,MagDet 的检测准确率达到 99.5%,EER 为 0.51%.

(3)通过实验评估 MagDet 的多种影响因素(包括变化的飞行速度、高度和地点),从而验证 MagDet 的鲁棒性.即使在未访问过的地点,准确率也高于 95%,EER 为 0.49%.

本文的其余部分结构如下:第 2 节提供本研究的背景知识;第 3 节解释基于地磁场检测无人机 GPS 欺骗攻击的想法的可行性;第 4 节详细阐述 MagDet 的详细设计;第 5 节是实验评估、与现有方法的对比以及 MagDet 方法影响因素分析;其后是第 6 和 7 节中的讨论和相关工作;最后,在第 8 节中总结本文.

2　背景知识

2.1　地磁场和磁力计

地磁场是指分布在地球周围空间的磁场,近似于位于地球中心的磁偶极子的场.地磁场天然存在,不像 GPS 定位信号需要导航卫星做支撑,并且地磁场无处不在,不受天气和障碍物遮挡的影响.地球上不同地方的地磁场方向和强度各不相同.

磁力计由三个相互垂直的磁阻传感器组成,分别位于 XYZ 三轴上,每个传感器测量该方向地磁场的强度.几乎所有无人机系统都包含磁力计传感器,它将测量的地磁场强度 XYZ 三轴数据提供给无人机,进而无人机基于地磁场强度计算偏航角,确保无人机航向正确.

磁力计可以通过两种方式测量磁场强度:其一,可以采用具有晶体结构的合金材料设计,合金材料对外部磁场敏感,根据磁阻传感器的电阻值变化来测量磁场的强度.另外,可以应用洛伦兹力测量磁场,流经磁场的电流会产生一种力,电容等会产生变化,进而用以测量磁场强度.因此,磁力计不会出现类似于加速度计的累计误差和陀螺仪的漂移,可以准确地测量磁场强度,支持本文提出的基于地磁场的 GPS 欺骗检测方法.

2.2　安全威胁模型

在 GPS 欺骗攻击中,攻击者首先欺骗 GPS 接收机,使其从合法信号切换到伪造信号.然后,攻击者接管 GPS 接收机以生成位置信息,可以是暴力接管,也可以是平滑接管.在暴力接管中,以高功率传输虚假信号,导致 GPS 接收机在重新采集信号的过程中失去对卫星的跟踪,锁定更强的欺骗信号.暴力接管容易实现,但是,暴力接管可能会导致信号强度或时钟的异常跳变,这将很容易被检测到并丢弃.平稳接管更为隐秘,它首先发送与合法信号同步的信号,然后逐渐压制合法信号,导致 GPS 接收机迁移至欺骗信号,但是需要利用高成本的高级硬件设备对合法信号进行实时追踪和同步.

攻击者的目标是用伪造的位置欺骗无人机,并操纵导航系统中的位置估计.由于 GPS 欺骗攻击存在潜在的危害,政府无线电规定严格禁止在室外使用真实的欺骗器进行 GPS 欺骗攻击实验.本文假设攻击者能够成功欺骗并接管无人机的 GPS 接收机.实验中通过随机改变 GPS 接收机生成的纬度和经度来实现欺骗攻击.

3　可行性分析

在本节中,将探讨使用磁场作为基准来验证 GPS 信号可信性的可行性.地球磁场就像一根从磁南极到磁北极的磁铁.在磁极处,磁场垂直于当地水平面.在赤道处,磁场平行于当地水平面.在北半球,

磁场倾斜向地面.地球磁场的强度和方向随地理位置而变化.

地磁场是一个矢量,对于一个给定位置,可以分解为三个分量,包括两个与当地水平面平行的分量(X 轴和 Y 轴)和一个垂直于当地水平面的分量(Z 轴).如果磁力计保持与当地水平面平行,则磁力计的三个轴对应这三个分量.测量磁感应强度的单位是特斯拉或高斯(1 特斯拉=10000 高斯).无人机在任何位置都能感应磁场的三轴分量,磁场强度与无人机三维位置之间的关系可以用来判断信号是真实的还是欺骗的.

为了进一步说明无人机周围地磁场与其所在位置存在强相关性,通过实验说明它们之间的关联性.由于地磁场强度包含 XYZ 三轴磁分量,地理位置也包含三维坐标,难以直观地用一个图将地磁场强度和地理位置刻画出来,因此,简化地磁场强度和位置坐标:分别分析地磁场三维分量与位置之间的关系;对于直线飞行路径,以无人机与起始点的距离表示地理位置,该距离可以体现无人机的不同位置.本文设计了一条直线飞行路径,飞行速度设置为 2 m/s,飞行高度为 7 m,通过实验收集飞行日志并进行数据处理得到图 1,该图刻画了磁场强度与地理位置之间的关系.以图 1(a)为例,每个无人机位置对应一个地磁场强度 X 轴分量.此外,Y 轴和 Z 轴分量也能分别与无人机位置一一对应,分别如图 1(b)和 1(c)所示.进一步,通过组合 XYZ 三轴分量可以使用每个不同的地理位置对应不同的地磁场强度.由此可以说明无人机位置与磁场强度之间具有很强的相关性,而无人机水平位置是通过 GPS 信号计算得到,从而可以利用磁场强度检测 GPS 欺骗攻击.

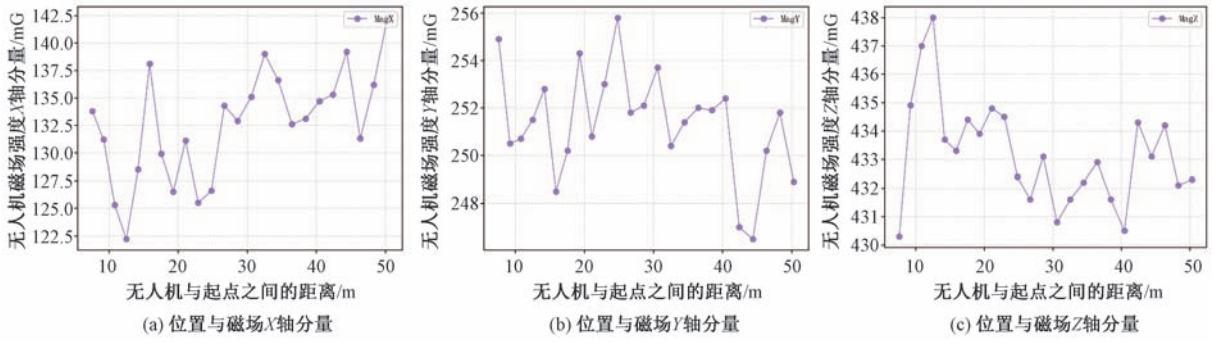


图 1 无人机位置与磁场强度之间的对应关系

4 MagDet 方法设计

本文提出基于地磁场的无人机 GPS 欺骗检测系统——MagDet,如图 2 所示.MagDet 由以下几个模块组成:数据收集模块、数据预处理模块、特征抽取模块和攻击检测模块。本节将详细介绍每个模块.

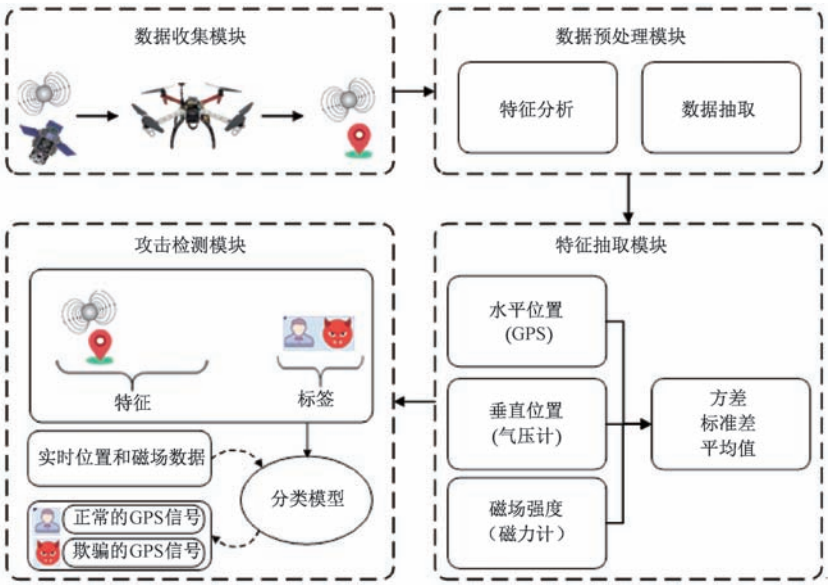


图 2 MagDet 方法

4.1　数据收集

通常,开源飞行控制器允许用户从飞行日志中获取飞行数据.但是,大多数商用无人机已禁用日志接口或加密日志数据.因此,本文使用开源飞行控制器(Pixhawk[24])和开源飞行控制软件(Ardupilot[25])作为无人机的核心.无人机正常飞行和欺骗飞行数据都是分析和建立欺骗检测模型所必需的.

首先,要收集正常的飞行数据.为了增强数据多样性,规划的飞行路径应覆盖不同的位置(包括纬度、经度和高度)和不同的磁场三轴分量.因此,为无人机设计多种飞行路径,包括直线飞行、垂直向上与向下飞行和曲线飞行.这些路径包含改变三维位置、磁场强度和磁场方向的不同方式.

其次,必须收集无人机受到欺骗的飞行数据.收集正常数据的飞行路径可以重复使用以获取欺骗数据.难点在于如何在实际飞行中利用伪造的 GPS 数据欺骗无人机飞行,并保证实验安全.本文通过将位置数据伪造程序注入到飞行控制软件来设计和实现欺骗攻击.该程序用随机值更新正常的纬度和经度,其中,随机值必须满足给定的取值范围.通过实验,本文已经验证了该取值范围能够欺骗无人机偏离计划路径飞行.欺骗程序的详细说明请参见章节 5.1.

4.2　数据预处理

4.2.1　特征分析

无论身在何处,地磁场总是可用的,而磁力计能够测量磁场强度,这确保了无人机始终可以获取其所在位置周围的磁场,包括 X 轴、Y 轴和 Z 轴分量.由第 3 节可行性分析可知,无人机所处不同位置对应不同的地磁场强度,因此有必要将磁场强度三轴分量选取为数据特征.

磁场异常使得不同位置的磁场不同.无人机使用 GPS 接收机和气压计获取其位置(纬度、经度和高度).从位置到磁场的映射关系可以用来识别 GPS 接收机是否接收到 GPS 欺骗信号.因此,还要选择无人机三维位置为数据特征,再做进一步的数据预处理和特征提取.

4.2.2　数据抽取

本研究从飞行日志中提取原始飞行数据.无人机控制系统通过 GPS、BARO(气压计)和 MAG(磁力计)日志消息分别记录水平位置(纬度和经度)、垂直高度和磁场强度.

本文实验使用的无人机的 GPS 接收机、气压计和磁力计的采样频率分别为 5 Hz、10 Hz 和 10 Hz.为保持数据量一致,以 GPS 数据的数量为基准.对于气压计或者磁力计数据,每两个相邻的数据以平均值的方式组合为一个数,从而统一数据采样频率为 5 Hz,与 GPS 数据一致.例如,气压计一秒钟测量得到 10 个高度数据,每两个相邻数据合并为一个,那么得到 5 个高度数据,可与一秒内的 5 个 GPS 数据一一对应;磁力计数据使用同样的方式统一采样频率.由此,基于 GPS 接收机的采样频率,建立 GPS 数据与磁力计和气压计数据三者之间的对应关系.但是,低采样频率可能会增加欺骗检测时间.

4.3　特征抽取

无人机飞行速度快,位置变化迅速.然而,由于风等外部环境因素的干扰,无人机无法不抖动地保持位置固定.无人机也不可能在不超出其位置区域的情况下到达航路点.通常,存在一个航路点半径,用来确定无人机是否到达该航路点.因此,仅使用单一时刻的数据来分析是否受到欺骗攻击是不合理的.MagDet 每隔一段短时间(τ 秒)检测一次攻击,用 τ 秒内的数据进行检测.为考虑空间距离变化,要计算 τ 秒内每两个位置之间的距离.为分析位置的变化模式和趋势,位置相关的特征选定为位置(纬度、经度和高度)和距离各自的均值、方差和标准差,如表 1(从第 1 个到第 12 个)所示.与其他无人系统相比,本实验采用无人机自带的传感器收集数据,其采样频率较低,这将限制 τ 的大小,进一步将限制 MagDet 的检测速度,但是不需要为无人机添加额外的设备.

表 1　特征列表

序号	特征
1～3	纬度{方差,均值,标准差}
4～6	经度{方差,均值,标准差}
7～9	高度{方差,均值,标准差}
10～12	距离{方差,均值,标准差}
13～15	Mag_x {方差,均值,标准差}
16～18	Mag_y {方差,均值,标准差}
19～21	Mag_z {方差,均值,标准差}
22～24	$MagXY$ {方差,均值,标准差}
25～27	$MagXYZ$ {方差,均值,标准差}

磁场的三轴分量不仅受无人机位置的影响,还受磁力计方向的影响.其中,方向由无人机姿态决定.然而,无人机姿态不断变化,因为它必须沿着规划的路径到达航点或抵抗外部干扰以保持飞行稳定.MagDet 每次使用一段时间内的磁力计数据进行分析,以减少瞬时数据误差.此外,两个水平磁分量融合成一个标量 $MagXY$,三轴磁分量融合成一个标量 $MagXYZ$,使得它们不再受磁力计方向的

影响[16]. $MagXYZ$ 是无人机周围磁场强度总量,但是相比垂直方向,无人机水平移动范围更大,同时,水平方向上位置变化速率也更大,所以有必要将水平方向的磁场强度 $MagXY$ 独立出来,将其综合到数据集中. 水平磁场强度 $MagXY$ 和总强度 $MagXYZ$ 可以分别使用公式(1)和(2)计算,其中 Mag_x、Mag_y 和 Mag_z 是三轴磁分量. 因此,选择三轴磁分量、$MagXY$ 和 $MagXYZ$ 各自的均值、方差和标准差作为磁场相关的特征,如表 1(从第 13 个到第 27 个)所示,其涵盖了磁场状态及其变化过程.

$$MagXY=\sqrt{Mag_x^2+Mag_y^2} \tag{1}$$

$$MagXYZ=\sqrt{Mag_x^2+Mag_y^2+Mag_z^2} \tag{2}$$

4.4 攻击检测

在从飞行日志中生成特征数据后,采用支持向量机(Support Vector Machine,SVM)、K 最近邻(K-Nearest Neighbor,KNN)、随机森林(Random Forest,RF)、多层感知器(Multiple Layer Perceptron,MLP)、梯度提升决策树(Gradient Boosting Decision Tree,GBDT)、决策树(Decision Tree,DT)和 XGBoost(Extreme Gradient Boosting)算法进行机器学习模型训练. 各种算法各有优缺点,本文的目标是以最高的检测率识别 GPS 欺骗攻击. SVM 适用于小样本和非线性数据集,以及高维模式识别问题,但是不适合多分类问题,并且对缺失数据较敏感;KNN 适用于多标签问题,具有较高的准确率,但其预测速度较慢,可解释性较差;RF 在许多实际任务中具有较低的计算开销和强大的性能,然而,对于某些具有高噪声的分类或回归问题,它会过拟合;MLP 具有较好的识别率和较快的分类速度,但是可能会丢失像素之间的空间信息,只接受矢量输入;GBDT 具有较高的预测精度,可以处理非线性数据,灵活地处理包括连续值和离散值在内的各种类型的数据,但是,由于弱学习器之间的依赖性,使得数据的并行训练变得困难;DT 可以处理多个输出问题,然而,它容易过拟合,决策树的生成不稳定,数据的微小变化可能导致生成的决策树不同;XGBoost 可以同时解决线性分类和逻辑回归问题,但是预排序过程的空间复杂度太高,要消耗较高的内存.

本文使用多种模型,以便选择最佳检测器. 为了比较这些算法的性能,首先,使用五折交叉验证和网格搜索方法[26]调整算法参数以获得最佳性能;其次,特征提取产生的数据集作为算法的输入,划分为训练集(70%)和验证集(30%). 在模型训练后,评估这些算法以选择一个最佳分类器来检测正常 GPS 数据和欺骗 GPS 数据.

无人机通过 GPS 接收机和气压计测量三维位置,包括经度、纬度和高度;通过磁力计传感器测量周围的磁场强度;通过输入实时采集的位置和磁场数据,分类器判断 GPS 信号是否正常. 如图 2 攻击检测模块所示,从而实现 GPS 欺骗攻击检测.

5 实验评估

5.1 实验设置

(1)硬件设置

使用一架四旋翼无人机进行飞行实验,无人机型号为 F450,该无人机采用 Pixhawk 2.4.8[24]作为飞行控制器,Adupilot 4.0.5[27]作为飞行控制软件;采用树莓派 raspberry 4B[28]作为机载计算机,用以支持 MagDet 运行,其所需的飞行数据通过与飞行控制器之间的有线传输实现,通信过程遵循 MAVLink 协议[29]. 在实验中,使用的传感器包括 GPS 接收机、MPU-6000、HMC-5883 和 MS5611. GPS 接收机接收卫星信号并向飞行控制器提供纬度和经度. MPU-6000 由加速度计和陀螺仪组成,支持姿态估计和位置估计. HMC-5883 作为磁力计,用于测量磁场三轴分量,支持计算无人机偏航角. MS-5611 是一种气压计,用于测量无人机高度.

(2)GPS 欺骗攻击设置

现有的针对无人机的 GPS 欺骗检测方法大多数是基于仿真数据提出. 只有少数研究人员利用真实数据验证他们的方法,但是大多数真实数据没有公开分享. 当前没有适合的开源数据可用于评估本文提出的方法. 收集正常飞行数据很容易,具有挑战性的在于收集由 GPS 欺骗攻击产生的欺骗数据. 考虑到 GPS 欺骗的潜在危害,无线电法规严格禁止在室外使用真实欺骗器进行 GPS 欺骗攻击实验. 为确保实验伦理性和合法性,将通过在飞行控制软件中注入欺骗软件(SpoofSW)来实现 GPS 欺骗攻击. 假设欺骗器已成功欺骗了无人机,SpoofSW 为正常纬度和经度增加或减少一个随机值. 这个随机值可以诱导无人机到虚构位置,并且已经在实验中验证了 SpoofSW 的有效性. 本文使用随机值而不是常数值来修改经度和纬度,因为纬度或经度的线性变化很容易被识别,而随机变化的值可以代表各种情况(每次欺骗位置的不同方向和距离),并且更难以检测.

$$m=randN\%50,\quad randN\%50>20 \tag{3}$$

$$lngChSum=\begin{cases}lngChSum+m, & randN\%10\geqslant 5\\ lngChSum-m, & randN\%10<5\end{cases} \tag{4}$$

$$spoofedLongitude=longitude+lngChSum \tag{5}$$

SpoofSW 修改真实 GPS 数据以实现欺骗攻击的方式,如公式(3)、(4)和(5)所示,展示了经度值修改方法.纬度值修改方法相同,这里不再列出.公式 3 中,$randN$ 为整型随机值,m 是由 $randN$ 得到的经度修改中间量;公式(4)中,$lngChSum$ 为经度修改量,初始值为 0;公式(5)中,$longitude$ 为真实的经度,$spoofedLongitude$ 为欺骗的经度值. SpoofSW 的详细工作流程如算法 1 所示.其输入由 GPS 接收机产生,即真实且正确的经度和纬度.第 2 行定义的静态变量 $lngChSum$ 和 $latChSum$ 分别用于记录每次修改经度和纬度的更改值(随机值)的累加值.更改值必须不断变化,不断增加或减少,因为如果一直使用相同的常数值作为更改值,那么无人机可以检测到欺骗攻击,然后忽略该常数值.每次变大或变小且值小于 50(如第 8、10、17 和 19 行所示)的变化值可以逐渐诱使无人机到欺骗位置.此外,在第 3—11 行计算 $lngChSum$ 的值,在第 12—20 行计算 $latChSum$ 的值,最后在 21—22 行修改真实的经度和纬度.

算法 1.　SpoofSW 算法.

输入:$longitude$, $latitude$

输出:$spoofedLongitude$, $spoofedLatitude$

1. BEGIN
2. 定义 $lngChSum$ 和 $latChSum$ 为静态浮点数并初始化为 0;
3. $randN \leftarrow rand()$;
4. WHILE $randN\ \%50 < 20$ DO
5. 　$randN \leftarrow rand()$;
6. END
7. IF $randN\ \%10 \geqslant 5$ THEN
8. 　$lngChSum \leftarrow lngChSum + randN\ \%50$;
9. ELSE
10. 　$lngChSum \leftarrow lngChSum - randN\ \%50$;
11. END
12. $randN \leftarrow rand()$;
13. WHILE $randN\ \%50 < 20$ DO
14. 　$randN \leftarrow rand()$;
15. END
16. IF $randN\ \%10 \geqslant 5$ THEN
17. 　$latChSum \leftarrow latChSum + randN\ \%50$;
18. ELSE
19. 　$latChSum \leftarrow latChSum - randN\ \%50$;
20. END
21. $spoofedLongitude \leftarrow longitude + lngChSum$;
22. $spoofedLatitude \leftarrow latitude + latChSum$;
23. RETURN $spoofedLongitude$, $spoofedLatitude$
24. END

(3)数据收集设置

在数据收集过程中,规划的飞行路径包括直线路径、曲线路径、转弯路径、上升线路径和下降线路径.速度设为 2 m/s、4 m/s 和 6 m/s,高度设在 6 m 到 15 m 之间.首先,无人机按照每个规划的路径飞行,不受 GPS 欺骗攻击的影响,以便生成并获得正常飞行数据.其次,在无人机飞行过程中发起 GPS 欺骗攻击,使其偏离预期路径.然后,可以从飞行日志中获得欺骗飞行数据.根据第 4.2 节介绍的数据预处理和第 4.3 节介绍的特征抽取,每一小段时间内的数据被提取为一个样本.通过实验共创建了 12386 s 的有效数据,包括 6534 s 正常数据和 5852 s 欺骗数据.

5.2　性能评估

评估指标本文选择了多种评估指标来评估 MagDet,包括准确率(accuracy)、假接受率(False Acceptance Rate,FAR)、假拒绝率(False Rejection Rate,FRR)、真阳性率(True Positive Rate,TPR)、假阳性率(False Positive Rate,FPR)、F1 度量(F1-measure)和等错误率(Equal Error Rate,EER).其中,(1)准确率表示 GPS 欺骗攻击的正确检测率;(2)FAR 表示在所有被接受样本(判定为正常的 GPS 信号)中,欺骗样本被错误接受为正常样本的比率;(3)FRR 表示在所有被拒绝样本(判定为欺骗的 GPS 信号)中,正常样本被错误拒绝的比率;(4)TPR 表示系统正确拒绝的欺骗样本在所有拒绝样本中的百分比,FRR 和 TPR 的总和为 1;(5)FPR 是系统错误接受的欺骗样本在所有接受样本中的百分比,FPR 等同于 FAR;(6)F1 度量用于评估分类模型的质量;(7)EER 是当判别阈值调整到 FRR 等于 FAR 时的比率.EER 越低,说明系统越精确.准确率、FAR/FPR、FRR 和 TPR 用于评估 MagDet 方法的性能,F1 度量值用于评估训练得到的模型的质量.

不同数据长度的性能比较为确定飞行数据选取的最佳数据长度,将不同时间长度(1 s、2 s、3 s、4 s 和 5 s)内的数据合并为一个数据检测点,进而训练分类器.采用 XGBoost 算法评估在不同数据长度下的系统性能.不同时间长度下的 GPS 欺骗攻击的检测率如图 3(a)所示,可以看到,各时间长度下的检

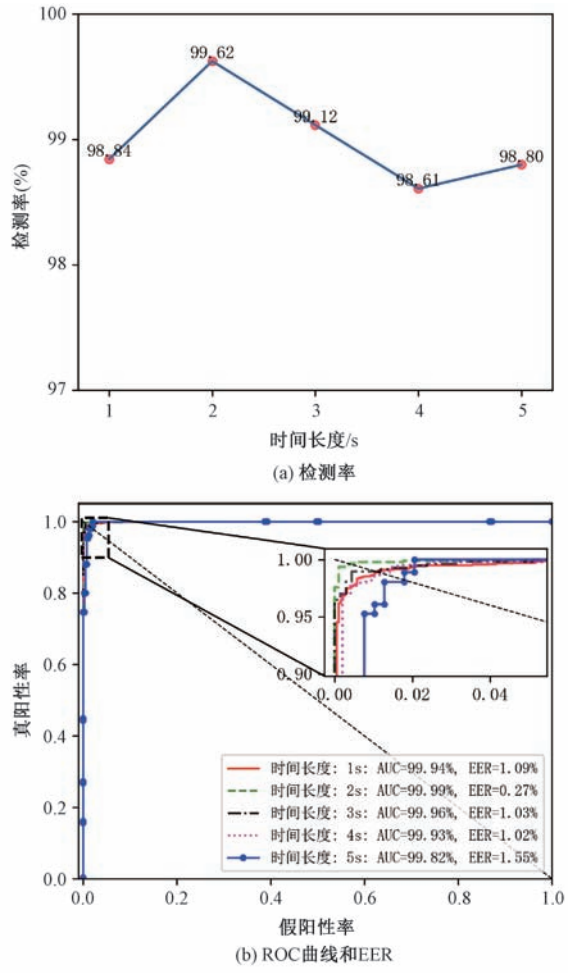


图 3 不同时间长度的检测性能对比

测率都高于 98.6%，这证明了 MagDet 在检测 GPS 欺骗攻击方面的有效性. 当时间长度为 2 s 时，检测率是最高的，为 99.62%. 此外，使用 ROC 曲线评估分类器性能，并计算不同时间长度的曲线下面积(Area Under Curve，AUC)和 EER，如图 3(b)所示. 与检测率一致，当时间长度为 2 s 时，EER 值是最低值，为 0.27%. 基于以上观察，可以得出结论：以 2 秒的时间长度选取数据点，对于分类器的训练和测试是最优的.

(1)算法调参

在检测欺骗攻击之前，MagDet 需要使用提取和处理过的飞行数据进行训练. 首先使用五折交叉验证和网格搜索方法调整 SVM-rbf、KNN、RF、GBDT、DT、MLP 和 XGBoost 算法的参数. 以 XGBoost 为例，预先构建了参数的值范围. 其中，γ 和 *learning_rate* 被设置为一组值，其中包含 6 个从 10^{-3} 到 10^{2} 的对数间隔的值；*max_depth* 的取值为从 2 到 6，间隔为 1；*n_extimators* 是估计器数量，取值为从 200 到 500，间隔为 50. 在遍历参数值范围后，为了达到最佳性能，参数 γ、*learning_rate*、*max_depth* 和 *n_extimators* 分别选定为 0.001、0.1、2 和 450. 算法参数调优花费的总时间为 6198 s.

(2)总体性能评估

首先，训练 MagDet 并生成实验结果，如表 2 所示. XGBoost 的准确率、FAR/FPR 和 F1 度量最高，分别为 99.57%、0.21%和 99.55%. XGBoost 是最好的模型，具有最佳的检测能力. 其次，生成 ROC 曲线来评估性能，如图 4 所示. 此外，还计算了不同分类器对应的 AUC 和 EER，如图 4 中所示. RF、GBDT 和 XGBoost 的性能良好. 它们的 AUC 超过 99%，EER 小于 1.4%. XGBoost 表现最佳：其 AUC 为 99.99%，EER 为 0.51%.

表 2 各种分类器的实验结果

分类器	准确率	FAR/FPR	FRR	TPR	F1 度量
KNN	80.17%	20.62%	18.97%	81.03%	79.65%
SVM-rbf	78.40%	35.46%	6.51%	93.49%	80.56%
RF	98.12%	1.13%	2.69%	97.31%	98.02%
MLP	79.58%	26.19%	14.14%	85.86%	80.10%
DT	96.83%	2.27%	4.15%	95.85%	96.66%
GBDT	99.25%	0.72%	0.79%	99.21%	99.21%
XGBoost	**99.57%**	**0.21%**	**0.67%**	**99.33%**	**99.55%**

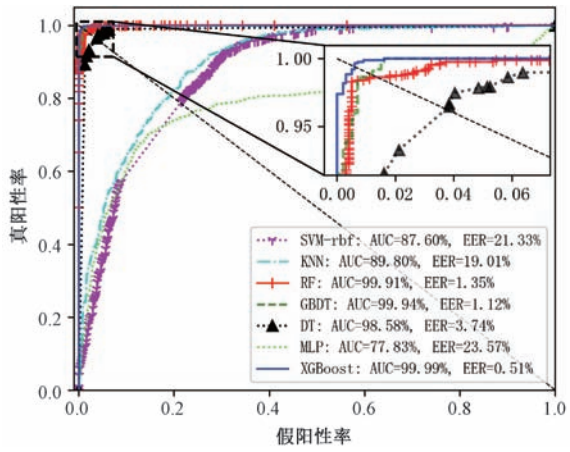


图 4 不同分类器的分类性能

(3)模型部署

鉴于 XGBoost 模型的优异表现，将其部署于无人机. 飞行控制器计算资源有限，为了不影响无人机核心控制系统的实时性，已在树莓派 raspberry 4B[28]中实现 MagDet. raspberry 4B 作为一个机载计算机与飞行控制器相互协作，使用 MAVLink 协议通过串口连接进行通信[29]. 为进一步说明 MagDet 的可用性，在校园场地测试已部署 MagDet 的无人机，飞行速度设置为 2 m/s，飞行高度范围为 7 m—22 m. 通过实施无人机 GPS 欺骗攻击实时检

测实验,记录飞行数据和检测结果,累计获得 1852 s 正常飞行数据和 1626 s 欺骗攻击数据. 实时检测 GPS 欺骗攻击的准确率为 88.50%,F1 度量值为 85.97%. 机载计算机上的实时检测性能低于台式机上的飞行日志数据检测性能,因为机载计算机与飞控之间通过串口实时通信,可能导致接收数据不完整,同时数据传输存在延时.

5.3　相关工作性能比较

进一步将 MagDet 的性能与现有相关工作进行比较,以证明磁场特征的优越性. 由于已有的方法使用的数据集与 MagDet 不同,且一些工作没有公开共享他们的数据集,因此本文复现了这些方法,并使用本文的数据集对它们进行评估. 使用相同的数据集可以提供更准确的性能比较,相较于直接比较各论文的欺骗检测准确率更为公平. 对比结果如表 3 所示. 在所有评估指标中,MagDet 的表现均优于 JSA[30]、PerDet[31] 和 ConstDet[32] 方法. JSA 的准确率最低,只有 82.25%,因为 JSA 仅使用角速度、加速度和基于 GPS 位置数据计算的距离,而对于这三种数据,存在以下缺点:陀螺仪测得的角速度存在漂移、加速度计测得的加速度存在累计误差,这些不精确数据会导致结果不准确;另外,无人机位置不仅包含 GPS 测得的水平位置,还应包含垂直高度,以准确计算无人机距离变化. JSA 方法的作者还提出了用于无人机 GPS 欺骗攻击的 DATE[33] 和 TECS[14] 方法,他们已经声明 JSA 方法优于 DATE 和 TECS 方法,因此可以进一步推断 MagDet 的性能也优于 DATE 和 TECS 方法.

表 3　与现有工作(已复现)的性能对比

相关工作	准确率	FAR/FPR	FRR	TPR	F1 度量
JSA[30]	82.25%	15.56%	20.17%	79.83%	81.03%
PerDet[31]	91.78%	8.38%	8.06%	91.94%	91.52%
ConstDet[32]	96.87%	3.05%	3.23%	96.77%	96.77%
MagDet	99.57%	0.21%	0.67%	99.33%	99.55%

表 4　与现有工作的检测率对比

相关工作	检测率	数据集
Wang 等人[34]	78%	仿真数据
Jansen 等人[12]	75%	真实数据和仿真数据
Liang 等人[13]	98.6% (>4 UAVs) 96.7% (≤4 UAVs)	仿真数据
Xue 等人[9]	94.8% (地面站检测) 89% (机载检测)	真实数据
MagDet	99.57%	真实数据

此外,还有一些工作提供了 GPS 欺骗攻击的检测率,但由于它们是基于多传感器数据[34]、多飞机位置数据[12]、多无人机位置数据[13]或卫星图像[9]提出的,因此它们不能与 MagDet 使用相同的数据集. 通过表 4 比较各种方法的检测率. 可以观察到,MagDet 是基于真实数据提出的,并且具有最高的检测率.

5.4　各种因素对 MagDet 的影响

本小节将评估各种因素(例如速度、高度和地点)变化对 MagDet 的影响.

需要注意,先前的研究表明天气的影响可以忽略不计[35]. 此外,一般情况下,地磁信号在白天和晚上并未呈现明显的周期性变化. 地磁场源于地球内部的运动,相对于地球的自转周期,白天和晚上的时间尺度相对较小,因此这两个时间段内地磁场的基本结构没有显著差异. 然而,在特定的地理位置和特殊的条件下,可能存在一些微小的影响. 例如,在白天,太阳辐射可引起大气电离层的变化,这种变化可能对一些高频地磁信号产生一定影响,尽管这一影响通常与地磁导航和传感应用的相关性较小. 总体而言,一天中的时间变化通常对地磁信号整体特性的影响相对较小. 地磁传感器通常能够在白天和晚上都稳定地测量地磁场. 然而,在一些特殊的应用场景中,可能需要考虑这些微小的变化,尤其是在磁场传感应用中,特别是对于需要极高测量精度的情况. 值得注意的是,MagDet 方法采用常见且廉价的磁力计,不属于高精度传感器,因此其测量结果受一天中的时间变化的影响较小. 尽管如此,未来将通过实验评估 MagDet 是否受白天或晚上的差异影响大小.

(1)速度变化的影响

相同时间长度的飞行数据在不同速度下会有不同的方差、标准差和均值. 本文通过在三种情况(飞行速度分别为 1 m/s、3 m/s 和 5 m/s)下飞行无人机来评估 MagDet 在不同速度下的性能. 这些速度不包含于第 5.2 节中描述的训练数据集中. 正常飞行和欺骗飞行的有效数据量如表 5 所示. 使用第 5.2 节中最好的分类器来检测这些数据. MagDet 在三种情况下的准确率和 F1 度量分别高于 98% 和 97%,显示了它对速度变化的适应性. 此外,通过绘制 ROC 曲线并计算相应的 AUC 和 EER 来评估性能,如图 5(a)所示,AUC 大于 99.8%,EER 小于 1.5%.

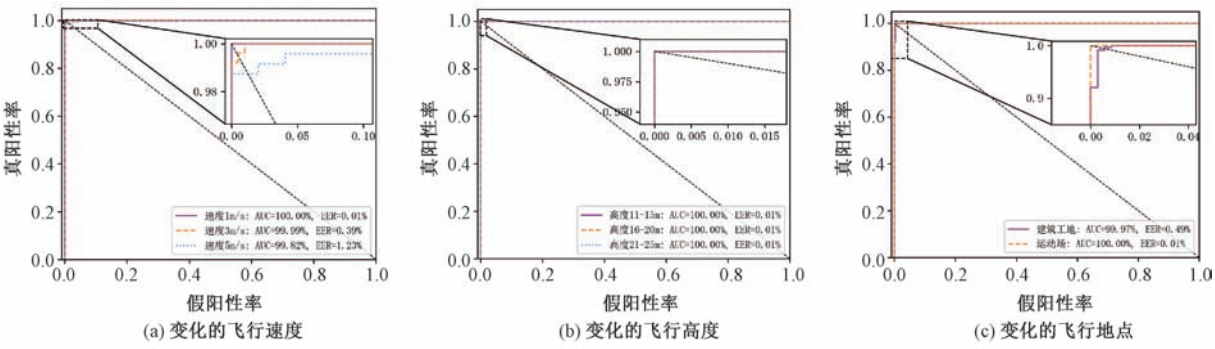
(2)高度变化的影响

磁场强度随高度变化而变化. 本实验通过在 11 m－15 m、16 m－20 m 和 21 m－25 m 三个高度

范围内飞行，对 MagDet 在不同高度下的性能进行了评估. 测试数据包括正常飞行和欺骗飞行数据，如表 6 所示. 当使用第 5.2 节中的分类器时，检测准确率大于 99.50%，F1 度量大于 99%. 另外，还绘制了 ROC 曲线并计算了 AUC 和 EER，如图 5(b)所示，其表现几乎是完美的. 这些结果表明，当无人机在不同高度飞行时，MagDet 可以检测 GPS 欺骗攻击.

表 5 不同飞行速度的性能对比

速度	1 m/s	3 m/s	5 m/s
正常时间(s)	596	397	296
欺骗时间(s)	420	508	478
准确率	98.03%	99.12%	98.71%
F1 度量	97.56%	99.21%	98.96%



(a) 变化的飞行速度 (b) 变化的飞行高度 (c) 变化的飞行地点

图 5 不同因素影响下的检测性能对比

表 6 不同飞行高度的检测性能对比

高度范围	11－15 m	16－20 m	21－25 m
正常时间(s)	520	465	525
欺骗时间(s)	386	344	329
准确率	99.78%	99.75%	99.53%
F1 度量	99.74%	99.71%	99.40%

(3)地点变化的影响

部署了 MagDet 的无人机可能飞往未曾到过的地点，但是不同地点的磁场环境存在差异. 为了评估不同的飞行地点对 MagDet 的影响，本实验通过在建筑工地(construction site)和运动场(sports field)收集飞行数据来评估 MagDet 在不同地点的性能，这两个地点相距 6 km. 飞行数据包括正常和欺骗攻击飞行场景. 飞行速度和高度与第 5.2 节中描述的训练数据集相同. 使用第 5.2 节中训练的分类模型进行欺骗攻击检测. 测试数据、准确率和 F1 度量如表 7 所示. 由结果可知，即使在新的地点，准确率和 F1 度量分别为 95.24%和 94.92%. 此外，还绘制了 ROC 曲线并计算了 AUC 和 EER，如图 5(c)所示. 这些结果表明，MagDet 不仅可以在训练区域内工作良好，而且还可以在未访问过的地点以高准确率工作.

表 7 不同实验地点的检测性能对比

飞行地点	建筑工地	运动场
正常时间(s)	706	631
欺骗时间(s)	680	611
准确率	95.24%	100%
F1 度量	94.92%	100%

6 讨 论

本节讨论了 MagDet 可能存在的局限性，并为将来的改进提供了一些方向.

(1)建筑物对地磁信号的干扰

建筑物可以对周围地磁信号产生影响. 首先，建筑结构中含有铁、钢等磁性物质，可能引起周围磁场的偏转，从而导致地磁场的畸变. 这种畸变可能使地磁传感器测量到错误的磁场方向和强度. 其次，建筑物的结构可能会阻挡地磁信号的传播，导致信号在穿过建筑物时衰减，特别是对于低频磁场信号. 这可能导致建筑物内或周围某些区域的地磁信号较弱. 在需要高精度地磁信号测量的应用中，必须考虑并纠正建筑物对地磁信号的影响，以确保准确地测量. 尽管 MagDet 方法并非以精确地磁信号为基础，但未来有必要进一步确认建筑物对 MagDet 的影响. 通过在建筑物周围进行正常飞行和 GPS 欺骗攻击飞行实验，收集地磁信号数据和无人机位置数据，以评估 MagDet 方法的健壮性. 在实际应用中，如果无人机飞行高度较高，建筑物对无人机测量的地磁信号影响较小. 在收集磁场信号数据后，如果飞行地点周围的建筑物没有太大变化，地磁信号不会有显著的差异. 这些因素需要在未来评估和使用 MagDet 方法时考虑，以确保其在各种环境条件下的可靠性和准确性.

(2)地磁欺骗

在通常情况下,地磁信号容易受到干扰,但实施地磁欺骗相对较为困难.地磁欺骗是指通过技术手段对地磁场进行操控或伪装,以达到欺骗或误导磁场感应设备的目的.在无人机导航系统中,磁力计传感器作为关键组件之一,尤其是在惯性导航系统中起着至关重要的作用.攻击者通过改变周围的地磁场,有可能欺骗这些传感器,从而导致导航系统生成错误的位置信息.这种攻击行为同样可能对 MagDet 方法检测 GPS 欺骗攻击的有效性产生负面影响.未来的研究需要着重评估地磁欺骗对 MagDet 方法检测性能的具体影响,并进一步探讨如何改进 MagDet 方法以减轻这种潜在威胁.这涉及到解决技术挑战,包括提高 MagDet 方法的抗干扰能力,确保其在面对地磁欺骗时仍能准确可靠地检测 GPS 欺骗攻击.这方面的研究将有助于加强对无人机导航系统的安全性,面对不断演变的威胁,提供更为可靠的解决方案.

(3)不同的无人机机架类型

磁力计安装在无人机上,其磁场分量会随着无人机的姿态变化而相应变动.由于无人机机架的重量和结构各异,不同类型的机架表现出不同程度的抖动.同时,每一类型的无人机机架均匹配着相应的电池,从而导致无人机的整体重量差异.在未来的研究中,我们计划利用多种无人机机架进行飞行数据的收集,以用于模型的训练和评估.

(4)GPS 欺骗攻击方式

为了合法地对无人机进行 GPS 欺骗攻击,本实验放弃了真实的无线电欺骗攻击,而是将攻击注入飞行控制软件中.本文将它们实现为随机欺骗攻击,并验证了它们能够欺骗无人机.未来,有必要通过将随机欺骗位置改进为指定欺骗位置,从而改变 GPS 欺骗攻击的方式,这样就可以获得不同的欺骗飞行数据,并且可以增加模型训练的数据多样性.此外,将提出一种欺骗路径规划算法,以支持通过攻击控制受害无人机并使其到达指定的任何位置.

(5)数据多样性

出于安全原因,实验在运动场上进行.受到 GPS 欺骗攻击的无人机飞行极其危险.许多靠近地铁站、建筑物或铁塔的地点,会对磁场产生巨大干扰.这些地点的磁场强度变化模式与运动场不同.但是,在具有强磁干扰的地点收集飞行数据是困难的.因此,计划通过精确的位置欺骗方式来改进欺骗攻击软件,以便于将无人机引诱到期望的位置.这种方式可以支持在“危险”地点附近进行实验,可以收集更多的不同场地飞行产生的数据.

7　相关工作

与现有工作进行对比,如表 8 所示,可知本文提出的 MagDet 方法不需要额外的专用设备,易于部署;基于真实数据提出,具有更高的应用价值;只需要单个无人机自身的数据便可以实现,不需要其他无人机、地面站或飞机协同实现.尽管表 8 倒数第二行的文献[14,30-33]也具体这些优点,但是由表 3 基于相同数据集的实验比较可知,MagDet 方法的检测率最高.此外,由表 4 可知,MagDet 方法同样优于其他方法,如 5.3 节所述.

表 8　无人机 GPS 欺骗检测方法对比

相关工作	专用设备	数据真实性	数据来源
文献[10-11]	需要	仿真	单机
文献[12]	不需要	真实+仿真	多机
文献[9,36]	需要	真实	单机
文献[13,37]	不需要	仿真	多机
文献[34,38-42]	不需要	仿真	单机
文献[14,30-33]	不需要	真实	单机
MagDet	不需要	真实	单机

针对无人机的一些欺骗检测方案需要额外的设备,如 SDR 接收机.Calvo-Palomino 等人[10]使用 SDR 设备收集 GPS 多普勒频移测量值,并训练长短期记忆(Long Short-Term Memory,LSTM)算法进行 GPS 欺骗检测.Khoei 等人[11]使用高级 GPS 接收机,如 SDR 设备,收集 GPS 信号的各种特征并训练机器学习算法.一些基于图像的检测方法依赖于安装在无人机上的高清摄像头来捕获图像和视频流[9,36].本文提出的方法不需要额外的硬件设备,可方便地在配套计算机上实现.

许多欺骗检测方案需要多架无人机协作并共享位置数据.Jansen 等人[12]提出了 Crowd-GPS-Sec 方法,一种使用众包监控无人机或飞机广播的 GPS 数据来检测 GPS 欺骗攻击和定位 GPS 欺骗器的方法.Crowd-GPS-Sec 使用真实数据和仿真数据进行评估.Liang 等人[13]提供了一种使用多架无人机的位置检测无人机 GPS 欺骗攻击的解决方案,这些位置由地面控制站(Ground Control Station,GCS)收集和计算,该方法在仿真实验中得到了证明.Eldosouky 等人[37]以附近多架无人机协同定位为前提,开发了一种对抗机制.本文提出的方法使用单架无人机的感知数据检测欺骗攻击.

许多用于无人机的欺骗检测方案都是使用仿真数据提出和评估的. Kim 等人[38]提出了一个基于 MLP 的框架,使用陀螺仪、加速度计和 GPS 数据来检测传感器欺骗,并利用生成对抗网络(Generative Adversarial Networks,GANs)来更好地训练模型. Wang 等人[34]利用 LSTM 模型与无人机在 X 轴方向和 Y 轴方向上的速度、加速度、纬度和经度进行训练,以预测位置,然后将其与基于 GPS 的位置进行比较,以确定无人机是否遭受 GPS 欺骗攻击. Panice 等人[39]使用惯性导航数据训练 SVM 模型生成位置,用于通过与基于 GPS 的位置比较进行欺骗检测. 上述方法都使用无人机仿真平台获取实验数据. 一些基于 GPS 信号特征的检测方法也只使用了仿真数据[10-11]. 一些基于多架无人机的检测方法[13,37]也使用仿真进行验证. 然而,本文进行了大量真实飞行实验进行数据收集,以支持 MagDet 的设计与验证.

一些用于无人机的欺骗检测方案只是理论框架,没有得到实际验证. Eldosouky 等人[37]介绍了一个数学框架来保护无人机免受 GPS 欺骗攻击. Elena 等人[40]应用 Kullback-Leibler 散度来检测无人机的 GPS 欺骗攻击,并使用泊松分布描述参数的随机变化,然而,这种方法对异常行为的鲁棒性较低. Meng 等人[41]介绍了一种基于线性回归(Linear Regression,LR)的无人机 GPS 欺骗检测方法,用于预测经度和纬度,以便与基于 GPS 的位置进行比较. Bada 等人[42]提出了一种基于策略的检测方法,用于检测飞行自组织网络(Flying Ad hoc Networks,FANETs)中合谋的无人机 GPS 欺骗攻击. 但是,这些方法仅基于仿真数据进行评估.

还有一些基于图像和视频流的无人机欺骗检测方案. Xue 等人[9]提出了一种基于卫星图像与无人机拍摄的图像之间的图像匹配的无人机 GPS 欺骗检测方法,即 DeepSIM. Barak 等人[36]应用线性回归模型,使用从摄像机的视频流中收集的位置和帧来预测位置,用于与基于 GPS 的位置进行检测,然而,这种方法受不同地形、环境光和高度的影响. 基于图像的方法也需要大量计算能力,而这对于无人机来说是缺乏的. 本文提出的方法仅依赖于常见的机载设备,例如,NVidia TX1[43]、NVidia TX2[44]和 Raspberry[28]等.

还有一些基于传感器数据之间的理论关系的无人机欺骗检测方法. Feng 等人[33]通过比较加速度计和 GPS 接收机分别计算的加速度来检测无人机 GPS 欺骗攻击. 他们还利用 GPS 计算的偏航角,通过与阈值比较来确定无人机是否遭受攻击[14]. 然而,传感器数据可能导致累积误差和数据漂移,从而降低检测准确率. 本文提出的检测方法智能地区分正常和欺骗数据,以减轻这些影响. Wei 等人[32]提出了一种基于无人机水平控制过程和高度控制过程中使用的参数的控制语义检测方法. Wei 等人[31]基于加速度计、陀螺仪、磁力计、GPS 和气压计产生的感知数据之间的关系来检测欺骗攻击. Feng 等人[30]提出了一种 JSA 方法,它使用角速度、加速度和 GPS 数据训练 XGBoost 模型进行欺骗检测,并声明 JSA 方法优于他们的 DATE[33]和 TECS[14]方法. 本文已经实现了 JSA 方法,用于与本文提出的方法进行比较,如第 5.4 节的对比实验.

8 结 论

本文提出了一种新的基于地磁场的检测方法——MagDet,该方法使用飞行控制器上的内置磁力计,通过感知磁场异常来识别无人机上的 GPS 欺骗攻击. 实验表明,MagDet 可以在不同的高度、速度和位置条件下有效地检测 GPS 欺骗攻击,并对环境噪声具有鲁棒性.

未来将在距离更远的区域进行实验(例如,不同的城市),收集正常的和欺骗的飞行数据,进一步验证 MagDet 在未访问过的地点的工作性能. 另外,将改进飞行控制系统,支持在地磁场强干扰区域飞行,从而收集磁场干扰严重区域的飞行数据进行模型训练,进一步在强干扰区域进行实际飞行测试. 此外,为了提高无人机实时检测 GPS 欺骗攻击的能力,将改进飞控与机载计算机之间的通信方式,以提高数据传输速率和准确率.

参 考 文 献

[1] Tippenhauer N O, Pöpper C, Rasmussen K B, et al. On the requirements for successful GPS spoofing attacks//Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS). Chicago, USA, 2011, p. 75-86

[2] Westbrook T. The global positioning system and military jamming: Geographies of electronic warfare. Journal of Strategic Security, 2019, 12(2): 1-16

[3] Kerns A J, Shepard D P, Bhatti J A, et al. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 2014, 31(4): 617-636

[4] Bhatti J, Humphreys T E. Hostile control of ships via false

GPS signals: Demonstration and detection. NAVIGATION: Journal of the Institute of Navigation, 2017, 64(1): 51-66

[5] Zeng K C, Liu S, Shu Y, et al. All your GPS are belong to us: towards stealthy manipulation of road navigation systems//Proceedings of the 27th USENIX Security Symposium (USENIX Security). Baltimore, USA, 2018: 1527-1544

[6] Narain S, Ranganathan A, Noubir G. Security of GPS/INS based on-road location tracking systems//Proceedings of the IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2019: 587-601

[7] Shen J, Won J Y, Chen Z, et al. Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing//Proceedings of the 29th USENIX Conference on Security Symposium. Berkeley, USA, 2020: 931-948

[8] gps-sdr-sim, https://github.com/osqzss/gps-sdr-sim, 2023, 1, 5

[9] Xue N, Niu L, Hong X, et al. DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching//Proceedings of the Annual Computer Security Applications Conference (ACSAC). Austin, USA, 2020: 304-319

[10] Calvo-Palomino R, Bhattacharya A, Bovet G, et al. Short: LSTM-based GNSS spoofing detection using low-cost spectrum sensors//Proceedings of the IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks(WoWMoM). Cork, Ireland, 2020: 273-276

[11] Talaei Khoei T, Ismail S, Kaabouch N. Dynamic selection techniques for detecting GPS spoofing attacks on UAVs. Sensors, 2022, 22(2): 662

[12] Jansen K, Schafer M, Moser D, et al. Crowd-GPS-Sec: leveraging crowdsourcing to detect and localize GPS spoofing attacks//Proceedings of the IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018: 1018-1031

[13] Liang C, Miao M, Ma J, et al. Detection of GPS spoofing attack on unmanned aerial vehicle system//Proceedings of the International Conference on Machine Learning for Cyber Security. Xi'an, China, 2019: 123-139

[14] Feng Z, Guan N, Lv M, et al. An efficient UAV hijacking detection method using onboard inertial measurement unit. ACM Transactions on Embedded Computing Systems (TECS), 2018, 17(6): 1-19

[15] Heirtzler J, Dickson G, Herron E, et al. Marine magnetic anomalies, geomagnetic field reversals, and motions of the ocean floor and continents. Journal of Geophysical Research, 1968, 73(6): 2119-2136

[16] Wang C C, Chen J C, Chen Y, et al. MVP: Magnetic vehicular positioning system for GNSS-denied environments//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. New Orleans, USA, 2021: 531-544

[17] Pasku V, De Angelis A, De Angelis G, et a. Magnetic field-based positioning systems. IEEE Communications Surveys Tutorials, 2017, 19(3): 2003-2017

[18] Canciani A, Raquet J. Absolute positioning using the earth's magnetic anomaly field. NAVIGATION: Journal of the Institute of Navigation, 2016, 63(2): 111-126

[19] Howard K, Ludwigson J. Defense navigation capabilities DOD is developing positioning, navigation, and timing technologies to complement GPS. Washington, USA: United States Government Accountability Office, Technical Report, GAO-21-320SP, 2021

[20] Yang C, Strader J, Gu Y, et al. Cooperative navigation using pairwise communication with ranging and magnetic anomaly measurements. Journal of Aerospace Information Systems, 2020, 17(11): 624-633

[21] Brzozowski B, Kaźmierczak K, Rochala Z, et al. A concept of UAV indoor navigation system based on magnetic field measurements//Proceedings of the IEEE Metrology for Aerospace (MetroAeroSpace). Florence, Italy, 2016: 636-640

[22] Brzozowski B, Kaźmierczak K. Magnetic field mapping as a support for UAV indoor navigation system//Proceedings of the IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace). Padua, Italy, 2017: 583-588

[23] Grosz A, Haji-Sheikh M J, Mukhopadhyay S C. High sensitivity magnetometers. Springer, 2017, 19

[24] Pixhawk overview, https://ardupilot.org/copter/docs/common-pixhawk-overview.html, 2023, 1, 5

[25] Copter home, https://ardupilot.org/copter/index.html, 2023, 1, 5

[26] Syarif I, Prugel-Bennett A, Wills G. SVM parameter optimization using grid search and genetic algorithm to improve classification performance. Telkomnika (Telecommunication Computing Electronics and Control), 2016, 14(4): 1502-1509

[27] Ardupilot, https://github.com/ArduPilot/ardupilot/tree/Copter-4.0.5, 2023, 1, 5

[28] Raspberry pi 4, https://www.raspberrypi.com/products/raspberry-pi-4-model-b/, 2023, 1, 5

[29] Communicating with raspberry pi via mavlink, https://ardupilot.org/dev/docs/raspberry-pi-via-mavlink.html, 2023, 1, 5

[30] Feng Z, Guan N, Lv M, et al. Efficient drone hijacking detection using two-step GA-XGBoost. Journal of Systems Architecture, 2020, 103: 101694

[31] Wei X, Wang Y, Sun C. PerDet: Machine-learning-based UAV GPS spoofing detection using perception data. Remote Sensing, 2022, 14(19): 4925

[32] Wei X, Sun C, Lyu M, et al. ConstDet: Control semantics-based detection for GPS spoofing attacks on UAVs. Remote Sensing, 2022, 14(21): 5587

[33] Feng Z, Guan N, Lv M, et al. Efficient drone hijacking detection using onboard motion sensors//Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE). Lausanne, Switzerland, 2017: 1414-1419

[34] Wang S, Wang J, Su C, et al. Intelligent detection algorithm against UAVs' GPS spoofing attack//Proceedings of the IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). Hong Kong, China, 2020: 382-389
[35] Griffiths D J. Introduction to electrodynamics. 2005
[36] Davidovich B, Nassi B, Elovici Y. Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream. Sensors, 2022, 22(7): 2608
[37] Eldosouky A, Ferdowsi A, Saad W. Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing. IEEE Internet of Things Journal, 2019, 7(4): 2840-2854
[38] Kim K H, Nalluri S, Kashinath A, et al. Security analysis against spoofing attacks for distributed UAVs//Proceedings of the Decentralized IoT Systems and Security. San Diego, USA, 2020
[39] Panice G, Luongo S, Gigante G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV//Proceedings of the 23rd International Conference on Automation and Computing (ICAC). Huddersfield, UK, 2017: 1-11
[40] Basan E, Basan A, Nekrasov A, et al. GPS-spoofing attack detection technology for UAVs based on kullback-leibler divergence. Drones, 2021, 6(1): 8
[41] Meng L, Yang L, Ren S, et al. An approach of linear regression-based UAV GPS spoofing detection. Wireless Communications and Mobile Computing, 2021, 2021: 1-16
[42] Bada M, Boubiche D E, Lagraa N, et al. A policy-based solution for the detection of colluding GPS-spoofing attacks in FANETs. Transportation Research Part A: Policy and Practice, 2021, 149: 300-318
[43] Nvidia TX1 as a companion computer, https://ardupilot.org/dev/docs/companion-computer-nvidia-tx1.html, 2023, 1, 5
[44] Nvidia TX2 as a companion computer, https://ardupilot.org/dev/docs/companion-computer-nvidia-tx2.html, 2023, 1, 5

WEI Xiao-Min, Ph. D., assistant professor. His research interests include GNSS spoofing detection, system security and safety, embedded software and unmanned systems.

LI Xing-Hua Ph. D., professor. His research interests include wireless network security, privacy protection and application cryptography.

SUN Cong Ph. D., professor. His research interests include information flow analysis, trusted software, program analysis and verification, and unmanned system security.

ZHANG Hai-Bin Ph. D., professor. His research interests include artificial intelligence security, industrial Internet security and trusted computing.

MA Jian-Feng Ph. D., professor. His research interests include application cryptography, wireless network security, data security and mobile intelligent system security.

Background

Satellite-based navigation and positioning systems, with the GPS at the forefront, play a pivotal role in guiding UAVs through precise location data. The integration of GPS is essential for the success of UAV navigation and mission execution. However, the widespread reliance on GPS introduces a significant vulnerability, as the system was not originally designed to withstand deliberate security threats.

Particularly in the realm of civilian GPS applications, susceptibility to spoofing attacks poses a noteworthy concern. Spoofing attacks involve the generation and transmission of counterfeit GPS signals with the intent to manipulate the UAV's navigation system. This manipulation leads to the dissemination of falsified location data, subsequently diverting the UAV to unintended destinations without its awareness.

Past research has shed light on instances of GPS spoofing attacks across various applications. These include taking control of UAV navigation systems, and manipulating sensor-fusion algorithms in self-driving cars. The implications of such attacks extend beyond mere inconvenience, encompassing potential security breaches and safety hazards.

Compounding the issue is the increasing accessibility and affordability of devices and techniques employed for launching GPS spoofing attacks on UAVs. The escalating sophistication and accessibility of tools for GPS spoofing highlight the urgency of developing robust countermeasures. Addressing these security vulnerabilities is crucial to ensuring the integrity and reliability of UAV navigation systems, safeguarding against unauthorized control.

In this paper, we propose the use of magnetic field fluctuations for detecting GPS spoofing attacks. It is based on geomagnetic field anomalies due to inhomogeneities within the Earth's interior and surrounding metal material. Each location can roughly associate with a pattern of anomalies. We put forward MagDet, a UAV GPS spoofing attack detection method based on the magnetic field. In MagDet, detec-

tion mechanism can be implemented in a UAV without requiring any additional sensors. Because MagDet relies solely on the surrounding magnetic field and UAV three-dimensional position, it does not require any special infrastructure. Moreover, most UAVs are already equipped with magnetometers for collecting magnetic field strength, GPS receivers for calculating longitude and latitude, and barometers for measuring altitude. This characteristic makes MagDet easy to deploy.

This work is supported by the National Natural Science Foundation of China (No. 62125205, No. 62272366 and No. 62232013), the Fundamental Research Funds for the Central Universities (No. ZYTS24141 and No. ZYTS23165) and the Key Research and Development Program of Shaanxi Province (No. 2023-YBGY-371).