计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(5):371−376 [doi: 10.15888/j.cnki.csa.008603]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于基站辅助的电力 5G 终端 GPS 欺骗检测①

龚亮亮[1,2], 陈振昂[3], 张　影[1,2], 吕　超[1,2], 何莉媛[1,2], 罗先南[1,2], 秦中元[3]

[1](南瑞集团有限公司 (国网电力科学研究院有限公司), 南京 211106)
[2](南京南瑞信息通信科技有限公司, 南京 211106)
[3](东南大学 网络空间安全学院, 南京 211189)
通信作者: 秦中元, E-mail: zyqin@seu.edu.cn

摘　要: 电力能源的安全在国家安全中占有重要的地位. 随着电力 5G 通信技术的发展, 大量电力终端产生定位需求. 传统 GPS 定位方法存在易受欺骗的问题, 如何有效提升 GPS 定位的安全性成为一个亟待研究的问题. 本文提出了一种基于基站辅助的电力 5G 终端 GPS 欺骗检测算法, 利用安全性较高的基站定位来检验可能被欺骗的 GPS 定位, 并且引入了一致性因数用来描述 GPS 定位结果和基站定位结果的一致性. 通过计算一致性因数, 如果大于设定的阈值则判断发生欺骗, 反之则 GPS 工作正常. 实验表明, 在使用本论文模型情况下, 本算法的准确率为 99.98%, 优于传统机器学习分类算法. 此外, 本方法在运行速度上相较于传统机器学习分类算法也有一定程度的提升.

关键词: 5G 终端; 基站定位; GPS 定位; GPS 抗欺骗; 一致性因数; 机器学习; 电力能源安全; 物联网

引用格式: 龚亮亮,陈振昂,张影,吕超,何莉媛,罗先南,秦中元.基于基站辅助的电力 5G 终端 GPS 欺骗检测.计算机系统应用,2022,31(5):371–376. http://www.c-s-a.org.cn/1003-3254/8603.html

GPS Spoofing Detection with Base Station Assistance in Power 5G Terminals

GONG Liang-Liang[1,2], CHEN Zhen-Ang[3], ZHANG Ying[1,2], LYU Chao[1,2], HE Li-Yuan[1,2], LUO Xian-Nan[1,2], QIN Zhong-Yuan[3]

[1](NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China)
[2](NARI Information & Communication Technology Co. Ltd., Nanjing 211106, China)
[3](School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China)

Abstract: The security of electric energy plays an important role in national security. With the development of power 5G communication, a large number of power terminals have positioning demand. The traditional global positioning system (GPS) is vulnerable to spoofing. How to improve the security of GPS effectively has become an urgent problem. This study proposes a GPS spoofing detection algorithm with base station assistance in power 5G terminals. It uses the base station positioning with high security to verify the GPS positioning that may be spoofed and introduces the consistency factor (CF) to measure the consistency between GPS positioning and base station positioning. If CF is greater than a threshold, the GPS positioning is classified as spoofed. Otherwise, it is judged as normal. The experimental results show that the accuracy of the algorithm is 99.98%, higher than that of traditional classification algorithms based on machine learning. In addition, our scheme is also faster than those algorithms.

Key words: 5G terminal; base station positioning; GPS positioning; GPS anti-spoofing; consistency factor (CF); machine learning; security of electric energy; Internet of Things (IoT)

① 基金项目: 国家电网有限公司总部管理科技项目 (SGZJXT00JSJS2000455)
收稿时间: 2021-09-26; 修改时间: 2021-10-25; 采用时间: 2021-12-08; csa 在线出版时间: 2022-03-31

电力是国计民生的支柱产业, 优质可靠的电力供应是现代化持续稳定发展的重要保证. 随着电力终端日益增多, 全国各地分布了大量电力终端, 定位服务的需求日益迫切. 如何对电力终端进行定位, 提供准确、安全、可靠的定位信息, 成为管理调度电力系统的关键问题之一[1,2].

目前采用 GPS 授时技术和定位技术是对电力终端进行定位的常用手段. 然而, 由于 GPS 并不安全, 存在多种欺骗式攻击方法[3,4], 使得 GPS 接收机解算出虚假的定位结果. 从攻击手段上来讲, GPS 欺骗式攻击可以分为两类: 一类是转发式欺骗, 这种攻击利用了 GPS 通过传播时延计算伪距的原理, 通过一台接收机设备接收真实卫星信号, 经过延迟、功率放大后转发至攻击目标, 使得攻击目标接收机计算得到错误的位置[5]. 此类攻击类似于传统的重放式攻击, 仅需转发信号, 实现难度低. 另一类是生成式欺骗, 该攻击利用了 GPS 民用波段信号格式公开的特点, 通过伪造真实信号发送至攻击目标, 使得导航接收机最终解算出错误的定位结果. 伪造者需要具备 GPS 信号编码、导航电文等相关知识, 实现难度相对较高[6].

自 2001 年以来, 美国国家运输中心在其提交给美国国家运输部的技术报告中首次评估了欺骗式攻击对全球定位系统的危害性[7], 随后, 众多学者开始对 GPS 的欺骗式干扰进行了系统研究. Wesson 等人研制了生成式 GPS 欺骗器, 并成功攻击了一架无人机[8]. Kerns 等人通过建立无人机欺骗攻击的必要条件, 探讨了欺骗信号的作用范围, 研究了捕获欺骗信号与真实信号的过程[9]. Liang 等人提出了一种基于协同式网络 GPS 认证方法用于检测 GPS 攻击[10]. 在国内, 史鹏亮等人对转发式欺骗干扰的选星方法进行了研究, 提出了一种基于常用 GNSS 定位选星方法和对卫星位置精度因子的贡献值选择被转发卫星的选星方法[11]. He 等人在建立多天线转发式攻击数学模型的基础上, 研究了影响攻击结果的关键因素和主要参数, 并设计开发了 GPS 欺骗攻击仿真系统进行欺骗原理进行验证[12]. 梁高波等人从不同的角度研究了转发式欺骗攻击对接收机的影响[13]. 有学者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, 实现对授时接收机的定时偏差控制. 还有研究者通过分析伪距定位原理, 研究修改信号的导航电文信息实现转发式欺骗攻击, 并进行仿真研究[14,15].

基站定位技术由于其覆盖范围广, 可用于室内定位, 所以基站定位也是目前常用的定位技术. 根据基站定位所采用的特征值, 可以分为基于增强小区 ID (E-CID) 定位、到达时间差 (TDOA) 定位、到达角度 (AOA) 定位以及混合定位[16]. 传统的 3G/4G 网络下, 实际定位精度在 100 m 以上, 很多时候无法满足用户定位需求. 而传统的 GPS 静态单点定位精度一般在 10 m 以下[17], 所以 3G/4G 基站定位在精度方面还是略显不足. 随着 5G 技术迅速发展, 5G 引入的毫米波技术和高带宽带来了更高精度的到达角和到达时间, 同时 5G 布设的密集基站也为高精度、高鲁棒性的基站定位提供了硬件基础. 根据 3GPP 的标准, 5G 定位服务 1 级应能达到水平精度 10 m, 垂直精度 3 m[18]. 此外, 在安全方面, 目前的 5G 标准中引入了用户隐藏标识符 (subscription concealed identifier, SUCI) 防止用户真实身份信息的泄露, 5G 中终端的真实身份称为 SUPI (subscription permanent identifier), 利用存放在用户终端的公钥, 将 SUPI 加密成用户隐藏标识符 SUCI, 并经由基站上传至 5G 核心网. 在核心网内由统一数据管理 (unified data management, UDM) 解密 SUCI 得到用户正式身份 SUPI, 然后再根据用户选择的认证方式提取对应的鉴权密钥与鉴权结果, 校验鉴权结果真伪[19]. 由此可知, 5G 网络具有较高的安全性.

基于以上内容, 本文提出了一种基于基站辅助对 GPS 系统进行欺骗检测的技术, 由于基站信号具备运营商的加密认证机制, 其本身可信程度较高, 因此基站定位为 GPS 抗欺骗提供了可信基础. 此外, 本文提出了一致性因数用于描述 GPS 定位结果和基站定位的一致性程度. 本文对该算法进行了全面的理论分析和实验. 实验表明, 在使用本论文模型情况下, 本算法的准确率为 99.98%, 且在其他分类方法引入一致性因数的情况下, 准确率均有不同程度的提升.

1 系统模型与数据度量

1.1 系统模型

为便于后续对基于基站辅助的 GPS 抗欺骗技术的研究, 本节将对相关参数建立数学模型. 本文系统模型建立在 WGS84 (world geodetic system) 大地测量系统标准中的标准经纬坐标系中. 由于本文提出的抗欺骗方法仅与 GPS 定位和基站定位的位置有关, 与其他因素无关, 因此不考虑信号生成、传播、捕获的过程,

直接对解算出的定位结果进行分析. 假设 GPS 定位采用静态单点定位方式, 基站定位采用 1 级 5G 定位标准, 二者定位精度均为 10 m[18]. 假设地球上的某随机真实位置为(R_x,R_y), 正常工作下的 GPS 解算出的定位结果为(G_x,G_y), 基站定位解算出的定位结果为(B_x,B_y), 遭受攻击的 GPS 解算出的定位结果为(S_x,S_y).

由于真实位置可为地球上任意位置, 则有R_x服从$[-180,180]$上的均匀分布, 记为$R_x \sim U[-180,180]$, R_y服从 $[-90, 90]$ 上的均匀分布, 记为$R_y \sim U[-90,90]$.

假设攻击者意图是完全随机的, 同理有S_x服从$[-180,180]$上的均匀分布, 记为$S_x \sim U[-180,180]$服从$[-90, 90]$ 上的均匀分布, 记为$S_y \sim U[-180,180]$.

GPS 和基站定位误差均用高斯分布表示. 则有:

$$G_x = R_x + D_x \tag{1}$$

$$G_y = R_y + D_y \tag{2}$$

其中, D_x和D_y为相互独立且均服从$N(0,10^{-8})$的高斯分布. 根据高斯分布特点, 可知G_x在 95% 的情况下处于区间$(R_x-2\times10^{-4},R_x+2\times10^{-4})$. 如果将地球看为一个标准球体, 使用半正矢公式计算可得到水平方向上最大误差为 22.26 m, 可见误差符合满足 GPS 单点定位精度.

同理有:

$$B_x = R_x + D'_x \tag{3}$$

$$B_y = R_x + D'_y \tag{4}$$

其中, D'_x和D'_y为相互独立且均服从$N(0,10^{-8})$的高斯分布. 且误差符合 1 级 5G 定位标准精度.

1.2 数据集

目前, 通用的 GPS 欺骗数据集较少, 仅有 TEXBAT (Texas spoofing test battery). 然而该数据集缺乏基站定位信息, 不适用于本文. 因此, 本文在实验采集的数据基础上, 根据上述建立的模型进行扩充, 生成了包含基站定位的 GPS 欺骗数据集, 数据集示例如表 1 所示, 其中, “标签”列为 0 代表 GPS 遭受欺骗, 1 代表 GPS 工作正常.

表 1 数据集示例

GPS经度	GPS纬度	基站经度	基站纬度	标签
155.110 8	−48.410 4	142.077 3	−51.082 9	0
−130.195	−9.157	99.380 08	12.290 8	0
−67.983 4	63.784 43	−67.991 7	63.775 41	1
−139.222	54.566 04	−139.23	54.562	1

1.3 一致性因数

为了描述 GPS 定位和基站定位结果的一致性程度, 本文提出了一种新的度量: 一致性因数 (consistency factor, CF), 该度量的计算方法如式 (5):

$$CF(G_x,G_y,B_x,B_y) = |G_x - B_x| + |G_y - B_y| \tag{5}$$

其中, G_x为 GPS 定位经度, G_y为 GPS 定位纬度, B_x为基站定位经度, B_y基站定位纬度. 使用本公式, 可将上述数据集中具有 4 维的输入特征组合为单维度特征. 根据经纬度范围可推导出CF的取值区间为$[0,540]$, 且该一致性因数CF越大, 则代表二者一致性程度越低, 反之, 一致性因数CF越小, 则二者一致性程度越高.

2 基于基站辅助的抗欺骗方法

2.1 系统总体结构

本文提出基于基站辅助的 GPS 欺骗检测方法, 利用可信的基站定位信号来校验可能被欺骗的 GPS 信号. 系统的总体结构包括 GPS 信号接收单元、基站信号接收单元、信号处理单元和导航接收机. 其中各单元的功能为: GPS 信号接收单元负责接收 GPS 信号, 并将 GPS 信号发送至信号处理单元处理. 基站信号接收单元负责接收基站信号, 并将基站信号发送至信号处理单元. 信号处理单元将二者信号处理完毕后, 解算出定位结果, 计算一致性因数, 根据阈值判断是否遭受欺骗式攻击, 最后发送至导航接收机. 总体结构如图 1.

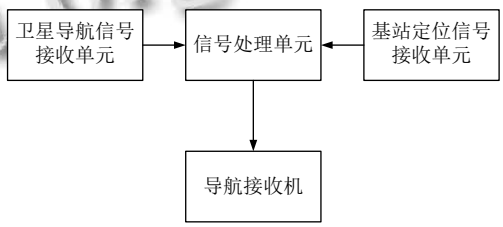

图 1 基于基站辅助的 GPS 欺骗检测系统总体结构图

下面分别分析正常工作情况和受到攻击情况的一致性因数.

2.2 不存在攻击情况下的一致性因数分析

当欺骗攻击不存在时, 系统的工作状况如图 2 所示. 首先, GPS 信号接收单元接收 GPS 信号, 计算得定位位置为经度G_x, 纬度G_y, 并将以上结果发送至信号处理单元. 接着, 基站定位信号接收单元接收基站定位信号, 计算得定位位置为经度B_x, 纬度B_y, 并将以上结果

发送至信号处理单元. 信号处理单元根据式 (6) 计算出一致性程度CF.

$$CF(G_x,G_y,B_x,B_y)=|G_x-B_x|+|G_y-B_y| \tag{6}$$

根据第 1.1 节中的模型定义, 在正常工作情况下, 一致性程度 CF 的最大值推导如式 (7) 所示.

$$\begin{aligned}\max(CF)&=\max\left(\left|G_x-B_x\right|\right)+\max\left(\left|G_y-B_y\right|\right)\\&=\max\left(\left|R_x+D_x-R_x-D_x'\right|\right)\\&\quad+\max\left(\left|R_y+D_y-R_y-D_y'\right|\right)\\&=\max\left(\left|D_x-D_x'\right|\right)+\max\left(\left|D_y-D_y'\right|\right)\end{aligned} \tag{7}$$

由于D_x, D_x', D_y, D_y'均为互相独立且服从$N(0,10^{-8})$, 则在 95% 的情况下, 他们的值域为$(-2\times10^{-4},2\times10^{-4})$, 因此有:

$$\max(CF)=8\times10^{-4} \tag{8}$$

根据上述推导过程可以得出结论, 攻击不存在时, 即在正常工作情况下, 一致性程度最大值为8×10^{-4}.

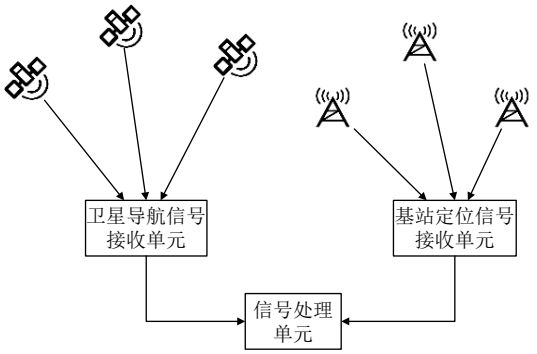

图 2 攻击不存在时的工作状况示意图

2.3 受到攻击的一致性因数分析

当存在欺骗攻击源信号时, 其工作状况如图 3 所示. 首先, GPS 信号接收单元接收 GPS 信号和攻击源信号, 计算得攻击者设定位置为经度S_x, 纬度S_y, 并将以上结果发送至信号处理单元. 接着, 基站定位信号接收单元接收基站定位信号, 计算得定位位置为经度B_x, 纬度B_y, 并将以上结果发送至信号处理单元. 信号处理单元根据式 (9) 计算出一致性因数CF.

$$CF(S_x,S_y,B_x,B_y)=|S_x-B_x|+|S_y-B_y| \tag{9}$$

下面计算 CF 小于正常情况下一致性因数最大值的概率, 由于 CF 的分布较为复杂, 采取放缩法来估计此概率值.

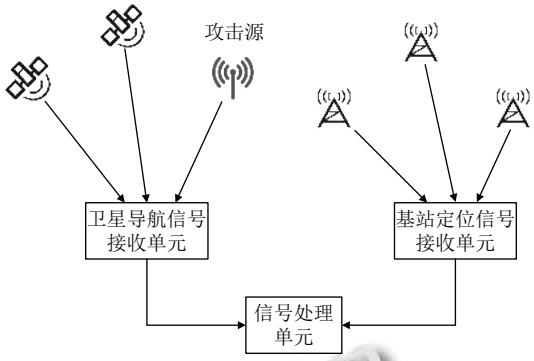

图 3 受到攻击时的系统工作状况示意图

$$\begin{aligned}CF(S_x,S_y,B_x,B_y)&=|S_x-B_x|+|S_y-B_y|\\&=|S_x-R_x-D_x'|+|S_y-R_y-D_y'|\\&\approx|S_x-R_x|+|S_y-R_y|\\&\geqslant|S_x-R_x|\end{aligned} \tag{10}$$

根据第 1.1 节中的模型定义, $S_x,R_x\sim U[-180,180]$, 且S_x,R_x互相独立, 则有$|S_x-R_x|$服从低限为 0, 众数为 0, 上限为 360 的三角分布. 计算可得该三角分布$|S_x-R_x|<8\times10^{-4}$的概率为2.22×10^{-6}. 则有:

$$P(CF<8\times10^{-4})=2.22\times10^{-6} \tag{11}$$

因此, 在使用本文所定义的模型时, 当 GPS 遭受攻击后, 可将正常情况下一致性程度的最大值作为阈值进行判决, 从而检测出欺骗攻击的存在.

2.4 算法具体流程

基于第 2.2 节和第 2.3 节的讨论, 得到算法的具体流程如算法 1 所示. 下面对本算法的时间复杂度和空间复杂度进行分析, 首先算法获取 4 个输入参数G_x, G_y,B_x,B_y, 然后使用式 (5) 计算一致性因数CF, 该公式涉及到 3 次加减法运算以及两次绝对值运算. 最后将 CF 与阈值d比较一次即得出判断结果. 对于不同的输入, 算法的执行语句数和额外存储空间均为常数, 因此本算法的时间复杂度和空间复杂度均为 O(1), 故本算法具有较高的计算效率.

算法 1. GPS 欺骗检测算法

1) GPS 接收单元接收 GPS 信号并发送至信号处理单元, 记为G_x,G_y.
2) 基站定位信号接收基站信号并发送至信号处理单元, 记为B_x,B_y.
3) 信号处理单元将步骤 1) 和 2) 中接收到的定位结果, 根据式 (5) 计算出一致性因数CF.
4) 如果CF大于等于设定的阈值d则判定为遭受攻击. 反之, 则判定为正常工作.
5) 基于步骤 4) 中的判断结果, 如果 GPS 信号被欺骗, 则发送基站定位坐标至导航接收机, 并返回遭受攻击; 如果 GPS 信号工作正常, 则发送 GPS 定位坐标至导航接收机, 返回正常工作.

3 实验处理和分析

3.1 实验环境

为验证本文算法的实际效果, 本文使用第 1 节所提出的数据集, 共 10 万条数据, 其中 5 万条为攻击数据, 5 万条为正常数据. 经过式 (5) 转化为单维的一致性因数, 并使用阈值分割法进行判决.

实验硬件为 Intel(R) Core i5-9400F CPU @2.90 GHz, 内存 16.0 GB 的台式电脑, 软件配置为 Windows 10 Professional, 工具语言采用 Python 3.9.5.

3.2 评价指标

一般来说, 判断 GPS 接收机是否遭受欺骗攻击可以视为一个二元分类问题, 因此本文使用准确率 (*Accuracy*) 和精度 (*Precision*) 作为指标来评价本算法, 其中准确率作为主要评价指标. 计算方式如式 (12)–式 (13) 所示. 英文缩写含义如表 2 所示.

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} \tag{12}$$

$$Precision = \frac{TP}{TP+FP} \tag{13}$$

表 2 英文缩写含义表

英文缩写	英文全称	含义
TP	True positive	正常工作, 被检测为正常工作
FN	False negative	正常工作, 被错分为遭受攻击
TN	True negative	遭受攻击, 被检测为遭受攻击
FP	False positive	遭受攻击, 被检测为正常工作

3.3 实验结果

为了充分研究设定不同阈值对结果的影响, 本文采用遍历阈值法来观察各阈值的分割效果. 第 1.3 节已给出一致性因数 *CF* 的区间, 故遍历区间设为[0,540]. 考虑到服从$N(0,10^{-8})$的分布数量级多为10^{-4}, 故步长设置为10^{-4}. 得到准确率、精确率的曲线分别如图 4 所示, 部分具体结果如表 3 所示. 图 5 表明准确率在 (0, 2×10^{-4}) 区间内为单调递增, 再结合图 4 可知准确率在$(2\times10^{-4},540)$区间单调递减. 由此可见, 设定合适的阈值可以有效检测 GPS 欺骗的发生. 第 1 节中推导出的阈值为8×10^{-4}接近极大值点, 可见理论和实际符合的很好. 另外, 在准确率相近的情况下, 应选取较小的阈值, 以检测距离基站定位结果较近的攻击点.

本文还使用了经典的机器学习分类算法进行对比实验. 实验按 7:3 的比例划分训练集和测试集, 以同样的指标来评估各模型, 得到实验结果如表 4 所示. 可以看到, 本文使用的“阈值分割+一致性因数”进行分类后, 在准确率上和精确率上均优于其他 6 种机器学习分类算法. 此外, 由于本算法实现简单, 因此在运行时间上也有极大优势, 相较于传统机器学习分类算法, 运行效率有较大提升.

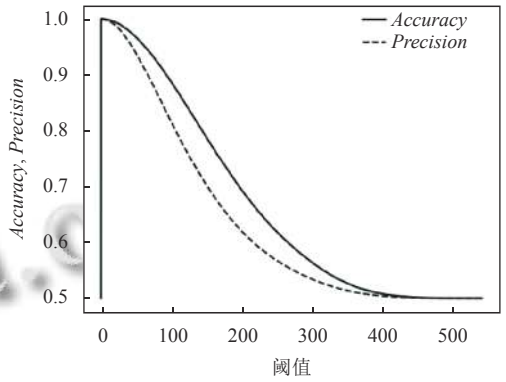

图 4 精确率、准确率随阈值变化曲线

表 3 部分实验结果

阈值	准确率 (%)	精确率 (%)
0	50.00	—
10^{-4}	75.26	100
2×10^{-4}	99.98	99.97
4×10^{-4}	99.98	99.97
8×10^{-4}	99.98	99.97
1	99.98	99.97
10	99.87	99.74
100	88.64	81.48
200	69.26	61.93
400	50.76	50.38
540	50.00	50.00

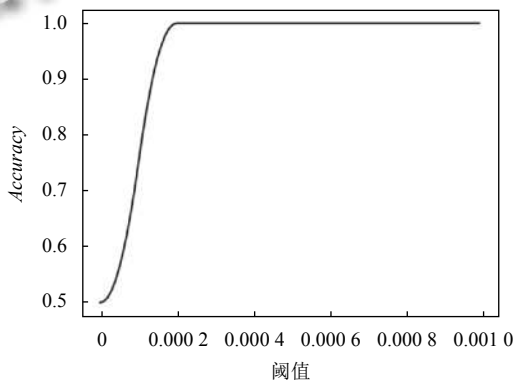

图 5 原点附近的准确率随阈值变化曲线

4 结论

本文提出了一种基于基站辅助的 GPS 抗欺骗技

术, 通过安全性高的基站定位校验 GPS 定位结果, 且引入了一致性因数用于描述 GPS 定位结果和基站结果的一致性程度. 然后采用阈值分割法对一致性因数进行判决, 取得了较高分类准确率和精确率. 此外, 本文通过实验证明了引入一致性因数可有效提高分类算法的准确率. 与现有欺骗检测技术相比, 本文方法实现简单, 由于电力 5G 终端兼具 GPS 信号接收模块和 5G 基站信号接收模块, 因此本算法可有效应用在电力 5G 场景.

表 4 本文方法与其他方法效果对比

分类方法	准确率 (%)	精确率 (%)	运行时间 (ms)
逻辑回归	47.72	47.53	47.32
K近邻	98.95	97.95	91.90
决策树	99.05	98.69	56.52
随机森林	87.18	79.77	71.48
朴素贝叶斯	51.64	52.38	50.73
多层感知机	99.76	99.53	107.99
本文方法	99.98	99.97	31.94

参考文献

1 赵威, 王强, 商可易, 等. 基于北斗导航的电力行业精准时空服务网. 电力信息与通信技术, 2021, 19(7): 75–82.

2 吕雅婧, 滕玲, 邢亚, 等. 北斗卫星导航系统在电力行业的应用现状. 电力信息与通信技术, 2019, 17(8): 70–74.

3 赵金磊. GPS 定位及欺骗干扰技术 [硕士学位论文]. 西安: 西安电子科技大学, 2014.

4 孙旸, 曹春杰, 赖俊晓, 等. 基于 LSTM-KF 模型的无人机抗 GPS 欺骗方法. 网络与信息安全学报, 2020, 6(5): 80–88.

5 闫占杰, 吴德伟, 刘海波. GPS 转发欺骗式干扰时延分析. 空军工程大学学报 (自然科学版), 2013, 14(4): 67–70.

6 马克, 孙迅, 聂裕平. GPS 生成式欺骗干扰关键技术. 航天电子对抗, 2014, 30(6): 24–26, 34. [doi: 10.3969/j.issn.1673-2421.2014.06.007]

7 边少锋, 胡彦逢, 纪兵. GNSS 欺骗防护技术国内外研究现状及展望. 中国科学: 信息科学, 2017, 47(3): 275–287.

8 Wesson K, Rothlisberger M, Humphreys T. Practical cryptographic civil GPS signal authentication. Navigation, 2012, 59(3): 177–193. [doi: 10.1002/navi.14]

9 Kerns AJ, Shepard DP, Bhatti JA, *et al*. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 2014, 31(4): 617–636. [doi: 10.1002/rob.21513]

10 Liang H, Work DB, Gao GX. GPS signal authentication from cooperative peers. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(4): 1794–1805. [doi: 10.1109/TITS.2014.2372000]

11 史鹏亮, 靳文鑫, 吴舜晓. 实施转发式 GNSS 欺骗干扰的选星方法研究. 北京理工大学学报, 2019, 39(5): 524–531.

12 何婷. GNSS 转发式欺骗干扰方法的改进. 测绘通报, 2019, (4): 71–74, 83.

13 梁高波, 高义, 陈杨. 欺骗式干扰信号对 GPS 民用接收机的影响分析. 第四届中国卫星导航学术年会论文集-S1 北斗/GNSS 导航应用. 武汉: 中国卫星导航学术年会组委会, 2013. 174–180.

14 高扬骏, 吕志伟, 周朋进, 等. 便携式 GPS 生成式欺骗干扰设备的设计与实现. 第十届中国卫星导航年会论文集——S11 抗干扰与反欺骗技术. 北京: 中科北斗汇 (北京) 科技有限公司, 2019. 49–55.

15 郭金梅. 卫星导航抗欺骗干扰技术综述. 第十一届中国卫星导航年会论文集——S11 抗干扰与反欺骗技术. 北京: 中科北斗汇 (北京) 科技有限公司, 2020. 37–42.

16 刘琪, 冯毅, 邱佳慧. 无线定位原理与技术. 北京: 人民邮电出版社, 2017.

17 贾小林, 陶清瑞, 王利军, 等. GNSS 基本服务性能评估. 测绘科学, 2021, 46(1): 62–75.

18 张建国, 徐恩, 周鹏云, 等. 基于 OTDOA 的 5G 定位性能综合分析. 邮电设计技术, 2021, (5): 38–42.

19 刘长波, 张敏, 常力元, 等. 5G 伪基站威胁分析及安全防护建议. 移动通信, 2019, 43(10): 58–61. [doi: 10.3969/j.issn.1006-1010.2019.10.011]