

基于 LSTM-KF 模型的无人机抗 GPS 欺骗方法

孙旸^{1,2,3}, 曹春杰^{1,2,3}, 赖俊晓^{1,2}, 于天娇^{1,2}

(1. 海南省 Internet 信息检索重点实验室, 海南 海口 570228;

2. 海南大学计算机与网络空间安全学院, 海南 海口 570228;

3. 南海海洋资源利用国家重点实验室, 海南 海口 570228)

摘要: 针对无人机 GPS 信号易受干扰、易欺骗的问题, 提出一种结合深度学习和卡尔曼滤波的无人机抗 GPS 欺骗的检测方法, 该方法通过使用长短期记忆网络从无人机飞行状态中预测得到无人机飞行的动力学模型, 并利用卡尔曼滤波结合动力学模型进行动态调整来识别 GPS 欺骗, 从而达到抵御 GPS 欺骗信号干扰的目的, 同时该方法无须增加接收器的硬件开销, 且易于实现。实验结果证明, 相比同类方法, 该方法对于识别 GPS 信号具有更高的准确率和更低的误报率, 可有效增强无人机抗 GPS 欺骗干扰的能力。

关键词: 无人机; GPS; 抗欺骗; 长短期记忆网络; 卡尔曼滤波

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020069

AntiGPS spoofing method for UAV based on LSTM-KF model

SUN Yang^{1,2,3}, CAO Chunjie^{1,2,3}, LAI Junxiao^{1,2}, YU Tianjiao^{1,2}

1. Key Laboratory of Internet Information Retrieval of Hainan Province, Haikou 570228, China

2. College of Computer and cyberspace security, Hainan University, Haikou 570228, China

3. China State Key Laboratory of Marine Resource Utilization in South China Sea, Haikou 570228, China

Abstract: A detection method of anti GPS deception of UAV was proposed for the problem that GPS signal of UAV was easy to be interfered and deceived, which combined deep learning and Kalman filter. The dynamic model of UAV flight was predicted from the flight state of UAV by using long short-term memory network, and the dynamic adjustment of Kalman filter and dynamic model was used to identify GPS deception. In order to resist the interference of GPS deception signal, this method did not need to increase the hardware overhead of the receiver, and was easy to realize. The experimental results show that the method has higher accuracy and lower false alarm rate for the

收稿日期: 2020-02-09; 修回日期: 2020-03-31

通信作者: 曹春杰, chunjie.cao@126.com

基金项目: 国家自然科学基金(61661019); 国家自然科学基金联合基金重点项目(U19B2044); 海南省高等学校教育教学改革研究重点资助项目(Hnjg2017ZD-1)

Foundation Items: The National Natural Science Foundation of China(61661019), The State Key Program of National Natural Science Foundation of China(U19B2044), Key Project of Education Teaching Reform Research in Higher Education Institutions in Hainan Province(Hnjg2017ZD-1)

论文引用格式: 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[J]. 网络与信息安全学报, 2020, 6(5): 80-88.

SUN Y, CAO C J, LAI J X, et al. AntiGPS spoofing method for UAV based on LSTM-KF model[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 80-88.

recognition of GPS signals, and can effectively enhance the UAV's ability to resist GPS deception interference.

Key words: UAV, GPS, anti spoofing, long short-term memory network, Kalman filter

1 引言

GPS 欺骗是当前 GPS 面临的主要威胁^[1], 其手段是通过伪造或重放虚假的 GPS 信号, 使被攻击的 GPS 接收器捕获并跟踪虚假的 GPS 信号, 从而解算出错误的时间和位置信息。GPS 欺骗分为转发式欺骗和生成式欺骗两种类型。① 转发式欺骗通过记录预欺骗位置真实的 GPS 信号, 使用软件定义无线电等信号发射设备, 将记录的真实 GPS 信号经过一定的延迟发射到处于另一位置的目标接收器, 达到欺骗目标接收器的目的。② 生成式欺骗是从真实的 GPS 信号中提取时间、位置、卫星星历等必要信息, 根据预欺骗的时间、位置信息生成虚假的 GPS 信号, 将虚假 GPS 信号的载波与真实 GPS 信号对齐, 通过矩阵天线发送给 GPS 接收器, 从而使 GPS 接收器解算出错误的时间、位置信息, 达到欺骗的目的。

国际上针对 GPS 定位导航的事件频发^[2]。2013 年, Humphreys 研究团队使用 GPS 欺骗技术成功诱导一艘价值 8 000 万美元的白玫瑰号游艇向左偏离航道 3°, 造成其偏出预定航线 1 km。因此, 针对 GPS 安全问题, 必须找到有效的解决方案来检测 GPS 攻击。

目前国内外针对 GPS 欺骗的防护方法主要有如下几种。

(1) 信号物理层特性检测方法

通过对比虚假信号与真实信号在信号物理层特性的差异来识别 GPS 虚假信号, 这些差异主要包括自动增益控制^[3]、信号到达方向、载波相位值、多普勒频移^[4]等。Psiaki^[5]等分析了基于信号到达方向检测 GPS 欺骗的原理, 通过不同天线间信号载波相位的变化来判断信号的到达角, 从而判断当前目标是否受到 GPS 欺骗攻击, 并提出了根据 GPS 信号到达方向的欺骗检测方案。Ranganathan^[6]等提出了辅助峰值跟踪的欺骗检测方法, 该方法与导航消息检查器结合使用, 可以通过跟踪最强的卫星信号以及其他较弱的环境信号实现欺骗检测。Kang^[7]提出了利用 GPS 历书和

星历数据估计到达方向 (DOA) 和实测 DOA 的差异, 利用 GPS 定向天线进行欺骗检测的方法。

(2) 基于密码学验证检测方法

使用密码学手段加密为随机噪声码, 接收机接收到信号后需要对信号进行解码, 对信号的发送者进行身份认证。Wesson 等^[8]提出了基于统计假设检验的密码源认证和码定时认证相结合的概率模型 GPS 信号认证方法, 通过利用 GPS 信号的伪随机噪声码检测 GPS 欺骗攻击。

(3) 使用其他设备辅助定位检测方法

通过使用惯性导航、无线网络和蜂窝网络等辅助手段结合 GPS 接收器进行定位, 达到抗欺骗的目的。Panice 等^[9]结合惯性导航系统提出了基于状态分布的抗 GPS 欺骗检测机制, 通过使用支持向量机分析 GPS 与惯性导航之间的误差分布来检测 GPS 欺骗攻击。Magiera 等^[10]提出了基于相位延迟和空间处理的 GPS 欺骗检测和缓解技术, 通过使用多个接收天线对信号相位进行延迟估计和对信号进行空间滤波, 以保护 GPS 接收器免受欺骗攻击。Jansen^[11]提出了群体众包的方法来检测无人机的 GPS 欺骗攻击, 该方法使用多架飞机报告位置的差异, 通过无线空中交通管制系统来检测无人机位置的 GPS 欺骗攻击。Kwon 等^[12]提出通过对比 GPS 接收器和加速度计之间的加速度差来检测 GPS 欺骗攻击的方法。

在诸如电力巡检、物流配送等无人机沿指定路线飞行的场景中, 现有方案仍存在如下问题: 基于 GPS 信号物理层检测的方法只能检测到简单的 GPS 欺骗, 当攻击者使用多个方向的 GPS 欺骗装置发射虚假 GPS 信号或在欺骗的同时动态调整 GPS 发射信号的频率和功率时, 仅通过 GPS 信号物理层特性无法检测出欺骗攻击, 因此该方法无法解决无人机在电力巡检中因上述 GPS 欺骗干扰引起的轨迹偏移问题; 基于密码学验证方法不能解决信号的重放攻击, 且对信号进行加密不适用于民用 GPS 信号; 使用其他设备辅助定位检测方法, 可以在一定程度上提高 GPS 接收器的抗欺骗能力, 然而会因此增加设备定位的成本

和无人机在电力巡检中的负载。针对现有方案的局限性, 本文将长短期记忆 (LSTM, long short-term memory) 网络和卡尔曼滤波 (KF, Kalman filter) 相结合, 提出了 LSTM-KF 模型。该模型提高了无人机在沿指定路线飞行时的抗 GPS 欺骗干扰的能力; 一方面, 利用 LSTM 循环神经网络学习当前环境无人机飞行轨迹规律, 对无人机飞行轨迹进行有效的预测, 避免了物理层检测方法对 GPS 信号过度依赖的问题; 另一方面, 使用 Kalman 滤波有效地解决了 LSTM 模型预测轨迹的误差, 提高了无人机轨迹预测精度, 从而有效增强了无人机抗 GPS 欺骗干扰的能力。同时, 此方法不需要对 GPS 接收器增加额外的硬件开销, 也无须对 GPS 信号进行任何修改, 且易于实现。

2 LSTM-KF 模型设计

2.1 设计思想

本文基于 LSTM-KF 模型的无人机抗 GPS 欺骗方法, 通过比较无人机飞行轨迹预测值与无人机 GPS 接收机定位值之间的差异, 可以快速检测出无人机 GPS 欺骗干扰。该方法使用 LSTM 与 Kalman 滤波相结合来预测无人机飞行轨迹。LSTM 模型具有很强的时间序列数据预测能力, 能够被应用于无人机飞行轨迹的预测, 同时 Kalman 滤波能很好地解决 LSTM 预测的飞行轨迹因噪声等外部因素干扰带来的误差缺陷。基于 LSTM-KF 模型的无人机抗 GPS 欺骗方法流程如图 1 所示。

图 1 所示的系统流程实现是基于 LSTM 模型的无人机飞行轨迹静态预测和基于 Kalman 滤波的轨迹动态调整相结合, 得出轨迹预测值的, 并与 GPS 实时定位数据对比, 检测无人机 GPS 定位安全性。其中, LSTM 模型为预测的基础, 利用训练好的 LSTM 模型从无人机的历史轨迹中计

算出需要预测的无人机飞行轨迹。但 LSTM 模型不能对无人机所处的复杂环境 (如噪声干扰等) 进行调整, 所以将卡尔曼滤波算法加入模型中。将 LSTM 模型预测的无人机轨迹作为初始的预测轨迹, 再将该初始的预测轨迹输入卡尔曼滤波器中对结果进行动态地调整。卡尔曼滤波模型利用更新方程将最新的更新值加入预测向量中, 从而有效地提高预测的精度。通过与 GPS 实时定位的数据作对比, 发现该方法可有效地提高无人机抗欺骗干扰能力。

2.2 基于 LSTM 的无人机轨迹静态预测

2.2.1 无人机飞行轨迹预测模型

无人机飞行轨迹的预测是运用 LSTM 循环神经网络解决回归问题。对 LSTM 模型进行训练, 将无人机的历史轨迹特征数据作为输入, 将未来的无人机轨迹特征数据作为对应的标签, 通过训练 LSTM 循环神经网络, 建立无人机历史飞行轨迹与无人机未来飞行轨迹的映射关系, 实现模型对无人机未来飞行轨迹的预测。

设 $x(t)$ 为无人机在各时刻的四元组数据, 其中 t 表示无人机飞行中的时刻, 四元组数据代表的信息为 $[\text{lng}_t, \text{lat}_t, \text{hig}_t, v_t]$, 其中 lng 、 lat 、 hig 、 v 分别表示无人机在 t 时刻的经度、纬度、高度和速度。则无人机在 t 时刻的轨迹特征 $x(t)$ 可表示为

$$x(t) = \{\text{lng}, \text{lat}, \text{hig}, v\} \quad (1)$$

通过训练后的 LSTM 模型可对无人机飞行轨迹进行预测, 将连续 n 个时刻的无人机飞行轨迹数据 $[x(t-n+1), \dots, x(t)]$ 作为 LSTM 模型的输入数据, 向后预测 n 步, 即将预测未来 n 个时刻的无人机轨迹数据 $[x(t+1), \dots, x(t+n)]$ 作为输出。其中 n 为 LSTM 模型中输入层的 step 大小。因此, 无人机飞行轨迹预测模型表达式为

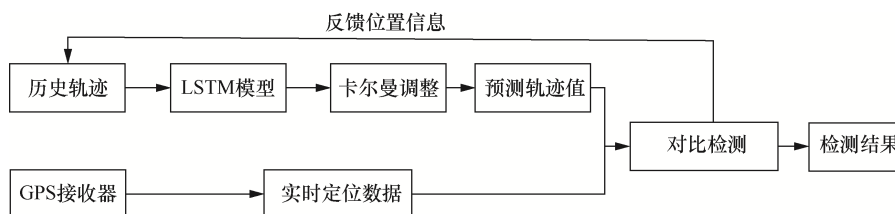


图 1 基于 LSTM-KF 模型的无人机抗 GPS 欺骗方法流程
Figure 1 Flow chart of anti-GPS spoofing method for drone based on LSTM-KF model

$$\{x(t+1), \dots, x(t+n)\} = f(\{x(t-n+1), \dots, x(t)\}) \quad (2)$$

2.2.2 数据归一化处理

为了消除无人机飞行轨迹数据间不同量纲对 LSTM 模型训练引起的误差,对无人机飞行轨迹数据进行归一化处理。本文采用离差标准化(min-max normalization)方法,经处理后的无人机飞行轨迹数据取值范围映射到[0, 1]。转换函数为

$$X^* = \frac{X - \min}{\max - \min} \quad (3)$$

其中, $\max$ 为无人机轨迹样本数据的最大值, $\min$ 为无人机轨迹样本数据的最小值。 X 为无人机飞行轨迹原始数据, X^* 为归一化处理后的无人机飞行轨迹数据。经过归一化处理,可以消除数据间取值范围和数量级的影响,但仍会保留数据间的关系。使用 LSTM 模型对无人机飞行轨迹进行预测后,对预测结果进行反归一化处理,使预测的无人机轨迹符合真实意义,以便后期与 GPS 接收器定位值作对比检测。

2.2.3 无人机轨迹预测 LSTM 模型输入层步数的选择

LSTM 模型中引入了时序的概念,使模型的处理数据增加了一阶步数的选择。该步数即无人机飞行轨迹输入时刻的长短。根据步数的选择, LSTM 模型的记忆神经元会选择记忆和遗忘所累积的信息,从而更加准确地由所选时刻的长短预测对应的无人机未来飞行的轨迹。在本文实验中,选择 3~7 个连续时刻的无人机飞行轨迹,即选择输入层的步数大小为 3~13,并将无人机抗 GPS 欺骗评估指标作为评判标准,选取最佳的步数大小。

2.2.4 无人机轨迹预测 LSTM 模型隐藏层神经元节点个数选择

LSTM 模型隐藏层神经元节点个数对无人机轨迹预测精度有直接的影响。如果节点数目太小,无人机轨迹预测不能很好地拟合,导致预测精度低,影响无人机抗 GPS 欺骗的性能;如果节点数目过大,会增加算法的复杂性与训练的时间。因此,本文实验中对隐藏层节点数目的选取进行分析,并将无人机抗 GPS 欺骗评估指标作为评判标准,选取最佳的隐藏层神经元节点个数。

2.3 基于 Kalman 滤波的轨迹动态调整

通过 LSTM 模型对无人机飞行轨迹预测,实现对无人机未来飞行状态和趋势较为合理的预测,然而由于复杂环境中不可避免的噪声干扰等问题,经过 LSTM 预测后的轨迹会出现偏移,需要对 LSTM 预测后的无人机飞行轨迹进行优化和调整,以提高预测精度,从而提高无人机的抗欺骗干扰能力。

卡尔曼滤波通过状态预测方程和更新方程对 LSTM 模型预测的无人机飞行轨迹结果进行更新,使无人机飞行轨迹预测结果更加精准,基于 Kalman 滤波的轨迹动态调整流程如图 2 所示。

图 2 中, LSTM 模型预测后的无人机飞行轨迹是卡尔曼滤波的观测值, Kalman 滤波通过状态方程的预测阶段和测量更新阶段两个部分对 LSTM 模型预测的无人机轨迹进行动态调整,提高无人机轨迹预测的精确度。模型中卡尔曼滤波的状态方程和观测方程分别如式(4)、式(5)所示。

$$X(k+1) = F(k+1)X(k) + B(k)W(k) \quad (4)$$

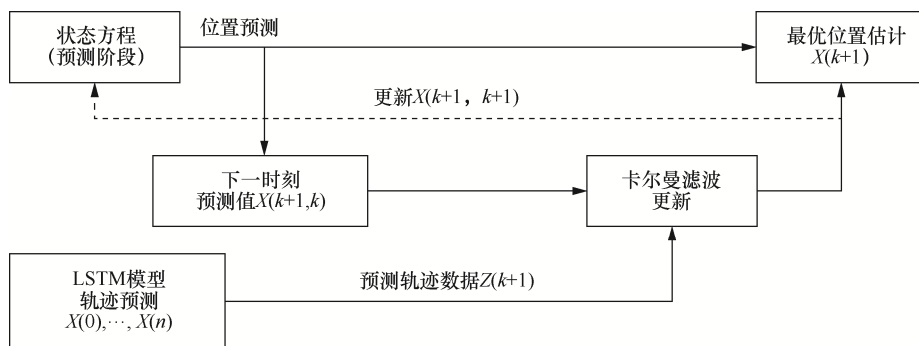


图2 基于 Kalman 滤波的轨迹动态调整流程
Figure 2 Dynamic adjustment of trajectories based on Kalman filtering

$$\mathbf{Z}(k+1) = \mathbf{H}(k+1)\mathbf{X}(k+1) + \mathbf{V}(k) \quad (5)$$

其中, $\mathbf{X}(k)$ 为系统状态向量, 表示无人机在 k 时刻的状态矢量, $\mathbf{F}(k+1)$ 为状态转移矩阵, 表示无人机飞行轨迹中由前一时刻的运动状态到下一时刻的运动状态的转移方式, $\mathbf{W}(k)$ 为无人机运动模型的系统状态噪声, 其统计特性相当于高斯白噪声; $\mathbf{Z}(k+1)$ 为观测向量, 表示无人机在 $k+1$ 时刻 LSTM 模型预测的无人机轨迹值, $\mathbf{H}(k+1)$ 为观测矩阵, $\mathbf{V}(k)$ 为无人机轨迹估计过程中产生的观测噪声。

卡尔曼滤波状态方程预测根据无人机轨迹前一时刻值最优状态估计预测出无人机轨迹下一时刻值的状态, 同时更新当前预测状态的协方差, 状态预测方程如下所示。

$$\mathbf{X}(k+1, k) = \mathbf{F}(k+1)\mathbf{x}(k, k) \quad (6)$$

$$\mathbf{Z}(k+1, k) = \mathbf{H}(k+1)\mathbf{X}(k+1, k) \quad (7)$$

得到下一时刻预测值之后, 利用 LSTM 模型预测的无人机轨迹提供观测值 $\mathbf{Z}(k+1, k)$, 利用卡尔曼更新方程来推测出最优无人机轨迹估计值, 同时通过状态噪声协方差和观测噪声协方差得出卡尔曼增益矩阵 $\mathbf{K}$ 。观测更新方程如式(8)所示。

$$\begin{aligned} \mathbf{X}(k+1, k+1) &= \mathbf{X}(k+1, k) + \\ &\mathbf{K}[\mathbf{Z}(k+1) - \mathbf{H}\mathbf{X}(k+1)] \end{aligned} \quad (8)$$

经过卡尔曼滤波更新过程, 得到无人机轨迹下一时刻的最优位置估计值, 通过不断迭代, 可完成对 LSTM 模型预测无人机轨迹的动态调整。

3 GPS 抗欺骗系统设计与实现

本文方法首先加载无人机飞行记录数据集并对其进行规范化, 将数据集分成训练数据集和测试数据集。接下来, 创建并初始化 LSTM 模型。设定 LSTM 的每个输入数据与以前的数据输入之间的递归关系。在 LSTM 中, 激活函数为 sigmoid, 在编译模型时指定损失函数为 mean_squared_error, 优化器为 adam。然后对训练数据进行批量迭代训练, 并进行 LSTM 预测。最后, 利用 Kalman Filter.em()学习参数, 建立并拟合 Kalman 滤波器, 利用 KalmanFilter.smooth()预测隐藏状态序列。最

终得出预测值, 与 GPS 接收器的数据进行实时对比, 得出检测结果, 判断无人机是否受到 GPS 欺骗干扰。

基于 LSTM-KF 模型的 GPS 欺骗检测算法如算法 1 所示。

算法 1 基于 LSTM-KF 模型的 GPS 欺骗检测算法

输入 无人机 GPS 轨迹集 T

输出 无人机 GPS 欺骗检测结果

1) 加载数据集

2) 规范化数据集

scaler = MinMaxScaler(feature_range = (0, 1))

dataset = scaler.fit_transform(dataset)

3) 创建训练数据和测试数据集

4) 初始化 LSTM 训练模型

model = Sequential()

model.fit(trainX, trainY, epochs = 100, batch_size = 5)

5) 对数据进行训练, 并进行 LSTM 预测

6) 初始化 Kalman 滤波模型

kf = KalmanFilter(initial_state_mean = observations[0])

7) EM 算法学习 Kalman 参数

kf = kf.em(observations, n_iter = 5, em_vars = 'all')

8) 利用 Kalman 模型预测隐藏状态序列

measurements_predicted = (kf.smooth (measurements) [0])[:, 0]

9) 对比预测值与定位值, 判断欺骗结果

if compare(D_PRE, D_RES) > ε

output true;

else

T = T + D_RES

output false

无人机 GPS 抗欺骗接收器软件实现: 运用 GPS 定位模块和 LSTM-KF 算法模块组合实现 GPS 抗欺骗功能, GPS 接收器模块实时接收定位数据, 对数据进行处理, 解算无人机定位数据。定位软件开启后可检测硬件设备和驱动是否安装正确, 并开始采集数据, 将实时数据通过与 LSTM-KF 算法预测轨迹数据进行对比分析, 得出

无人机抗欺骗结果，并在地图上将定位点实时显示出来。飞行完成后的定位数据可保存在本地中，以供后续处理分析和使用。

4 实验结果与分析

4.1 实验数据描述与处理

数据的采集来自无人机携带的 GPS 接收器实际接收的 GPS 信号产生的定位记录，无人机的飞行轨迹区间为海南大学第一田径运动场至海南大学图书馆，无人机携带的 GPS 接收器能够记录无人机飞行轨迹的经度、维度、高度和速度。无人机 GPS 欺骗场景通过软件定义无线电实现，攻击者可以通过生成式欺骗产生虚假信号，通过定向天线对无人机进行 GPS 欺骗干扰。采集数据集参数如表 1 所示。

4.2 评估指标

为了确定研究的 LSTM-KF 模型的性能，采用 4 种评价指标对该模型的抗 GPS 欺骗性能进行评估。

表 1 采集数据集参数

参数	值
信号频率	1575.42 MHz
伪码类型	C/A
无人机训练轨迹总数	2 000
测试轨迹数量	500, 800, 1 200, 1 500, 2 000
判断阈值	15 m
激活函数	sigmoid

检测率 (DR, detection rate)、漏检率 (MR, missing report rate)、误报率 (FR, false alarm rate)、准确率 (Accuracy) 的计算式如下。

$$P_d = P(x=1|y=1) \quad (9)$$

$$P_m = P(x=0|y=1) \quad (10)$$

$$P_f = P(x=1|y=0) \quad (11)$$

$$P_a = P(x=1|y=1)P(y=1) + P(x=0|y=0)P(y=0) \quad (12)$$

其中， P_d 为检测率，代表无人机正确识别 GPS

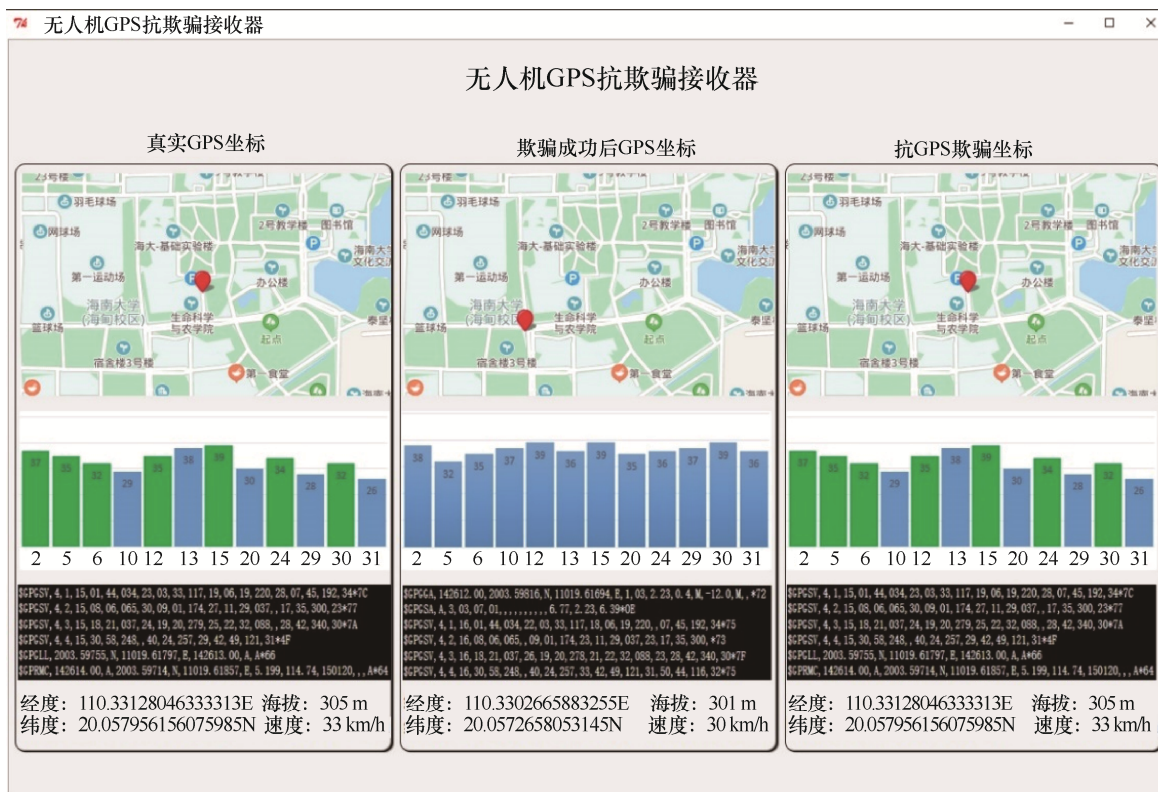


图3 无人机抗GPS欺骗系统实现
Figure 3 Implementation of UAV anti-GPS deception system

欺骗信号的概率； P_m 为漏检率，代表无人机将 GPS 欺骗信号识别为正常的信号的概率； P_f 为误报率，代表无人机将正常的 GPS 信号识别为欺骗信号的概率； P_a 为准确率，代表无人机将 GPS 正常信号和欺骗信号均正确识别的概率。

4.3 结果分析

本节实验结果分析主要分成两部分：① 针对本文提出的 LSTM-KF 模型，研究不同的参数对无人机抗 GPS 欺骗的性能的影响；② 分析对比不同的方法对无人机抗 GPS 欺骗的效果。

4.3.1 无人机抗 GPS 模型参数分析

对无人机飞行轨迹数据作归一化处理后，设定不同的隐藏层神经元节点个数，将连续 6 个时刻的无人机飞行轨迹数据作为模型的输入，将未来 6 个时刻的无人机飞行轨迹数据作为输出来训练模型。在实验中设置不同的 LSTM 预测模型的隐藏层神经元节点个数。通过比较实验结果的准确率和误报率，确定该模型中最佳的参数，实验过程中不同隐藏层节点数对应的准确率和误报率对比如图 4 所示。

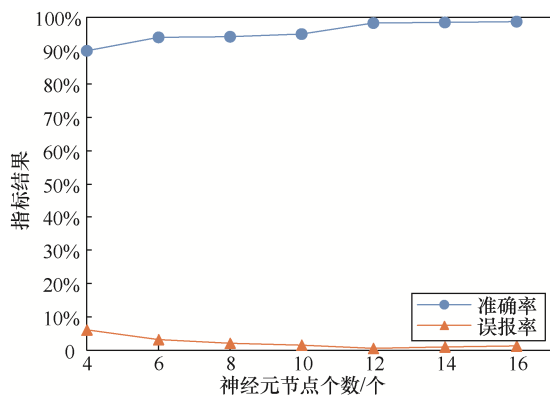


图 4 神经元节点对应的准确率和误报率对比
Figure 4 Comparison of accuracy and false alarm rates corresponding to neuron nodes

由图 4 可知，随着隐藏层神经元节点个数不断增加，无人机识别 GPS 信号真伪的性能随之提高。隐藏层神经元个数从 4 增加到 12，准确率提高了 8.3%。而神经元个数从 12 增加到 16 时，准确率的提升比较缓慢。当神经元个数增加到 12 之后，随着神经元个数的增加，误报率出现上升的趋势。从实验结果可以看出，当隐藏层神经元节点数为 12 时，训练效果最佳，无人机识别 GPS

欺骗准确率高、误报率低、无人机抗 GPS 欺骗性能最佳。综上所述，该模型设置的最佳隐藏层神经元节点数为 12。

无人机飞行轨迹输入时刻的长短直接影响着该模型对无人机飞行轨迹预测的精度，实验中设置输入层不同的步数，即设置不同连续时刻的无人机飞行轨迹作为模型的输入，对比实验结果中不同步数的准确率和误报率，确定该模型最佳的步数。实验过程中输入层步数对应的准确率和误报率图 5 所示。

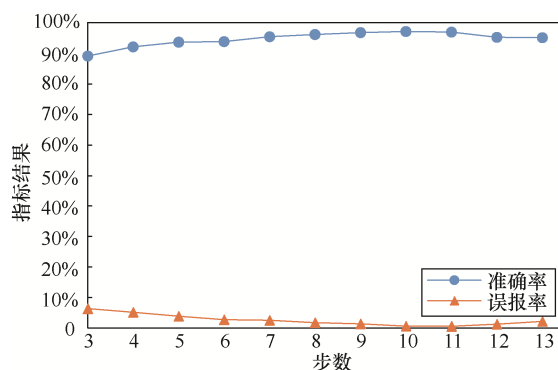


图 5 输入时序步长对应的准确率和误报率对比
Figure 5 Comparison of accuracy and false alarm rates corresponding to input timing steps

由图 5 可知，随着输入层步数逐渐增大，无人机识别 GPS 信号真伪的性能在步数为 10 时达到最高值。当步数从 3 增加到 10，准确率逐步提升，在 10 时准确率达到 97.1%。同时误报率明显下降，无人机识别 GPS 信号性能不断提升。当步数增加到 10 以后，随着步数不断增加，准确率开始逐步下降，同时当步数达到 11 之后，误报率开始出现上升趋势。输入的步数越大，模型计算越复杂，模型出现过拟合现象，导致无人机识别 GPS 信号的准确率开始下降，误报率出现上升趋势。从图 5 可以看出，当输入层步数为 10 时，训练效果最佳，无人机识别 GPS 欺骗准确率高、误报率低、无人机抗 GPS 欺骗性能最佳。综上所述，该模型设置的最佳步数为 10。

4.3.2 不同方法对于无人机抗 GPS 欺骗性能对比

为了验证该模型的无人机抗 GPS 欺骗的性能和效果，在相同的数据集的基础上，采用循环神经网络 (RNN, recurrent neural network) 模型、LSTM 模型、支持向量机 (SVM, support vector

表 2 各模型抗 GPS 欺骗性能对比结果
Table 2 Comparison results of anti-GPS deception performance of each model

分类模型	准确率	检测率	误报率	漏检率
LSTM-KF	98.3%	99.2%	0.56%	0.8%
LSTM	88.5%	92.7%	10.7%	7.3%
SVM	84.7%	87.3%	16.8%	12.7%
RNN	72.6%	83.1%	21.6%	16.9%

machine) 模型测试本次实验中无人机抗 GPS 欺骗的效果。利用本文提出的评估指标对以上模型进行抗 GPS 欺骗性能的比较, 实验结果如表 2 所示。

由表 2 可知, 本文提出的 LSTM-KF 模型的无人机抗 GPS 欺骗性能优于 LSTM 模型、SVM 模型和 RNN 模型。LSTM-KF 模型的准确率达到 98.3%, 误报率仅为 0.56%, 漏检率为 0.8%。一方面, 该模型使用的 LSTM 预测方法本身可以提供较好的时序预测能力; 另一方面, 结合 Kalman 滤波可有效地改善 LSTM 预测模型因外部环境等因素产生的预测误差。本文提出的 LSTM-KF 模型的抗 GPS 欺骗准确率分别比 LSTM 模型、SVM 模型、RNN 模型提高了 9.8%、13.6%和 25.7%, LSTM-KF 模型的准确率得到了极大地提升。对于虚假信号的检测率, 该模型相对其他 3 种模型分别提高了 6.5%、11.9%和 16.1%。同时 LSTM-KF 模型对于实验结果的误报率有明显的优势, 分别比其他 3 种模型误报率降低了 10.14%、16.24%和 21.04%。

5 结束语

欺骗是 GPS 接收器上最重要的威胁之一。本文讨论了无人机抗 GPS 欺骗干扰的检测模型, 提出了基于 LSTM-KF 模型抗 GPS 欺骗检测方法, 通过长短期记忆网络预测出无人机飞行轨迹并结合卡尔曼滤波对其进行调整, 之后通过与 GPS 接收器定位结果的对比达到对无人机 GPS 欺骗干扰做出有效判断的目的。模型采用长短期记忆网络模型实现静态预测, 同时采用卡尔曼滤波模型结合实时定位数据对静态预测的预测值进行动态调整。通过两个模块的静态预测和动态调整的结果,

实现最优估计, 从而对欺骗信号进行准确的判断, 达到抗欺骗干扰的目的。该方法相对于传统的抗 GPS 欺骗检测方法无须增加辅助设备等硬件成本, 且具有准确率高、误报率和漏报率低的特点, 能在无人机沿指定路线飞行的场景下有效地实现抗 GPS 欺骗干扰的效果。

参考文献:

- [1] 刘炜, 冯丙文, 翁健. 小型无人机安全研究综述[J]. 网络与信息安全学报, 2016, 2(3): 39-45.
- [2] LIU W, FENG B W, WENG J. Survey on research of mini-drones security[J]. Chinese Journal of Network and Information Security, 2016, 2(3): 39-45.
- [3] ZHI Y, FU Z, SUN X, et al. Security and privacy issues of UAV: a survey[J]. Mobile Networks and Applications, 2019: 1-7.
- [4] BROUMANDAN A, JAFARNIA-JAHROMI A, DANESHMAND S. Overview of spatial processing approaches for GNSS structural interference detection and mitigation[J]. Proceedings of the IEEE, 2016, 104(6): 1246-1257.
- [5] PSIAKI M L, O'HANLON B W, BHATTI J A, et al. GPS spoofing detection via dual-receiver correlation of military signals[J]. IEEE Transactions on Aerospace & Electronic Systems, 2013, 49(4): 2250-2267.
- [6] PSIAKI M L, HUMPHREYS T E, STAUFFER B. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies[J]. IEEE Spectrum, 2016, 53(8): 26-53.
- [7] RANGANATHAN A, ÓLAFSDÓTTIR H, CAPKUN S. SPREE: a spoofing resistant GPS receiver[C]//22nd Annual International Conference on Mobile Computing and Networking, 2016: 348-360.
- [8] KANG C H, KIM S Y, PARK C G. An adaptive complex-EKF-based DOA estimation for GPS spoofing detection[J]. IET Signal Processing, 2017, 12(2): 174-181.
- [9] WESSON K, ROTH LISBERGER M, HUMPHREYS T. Practical cryptographic civil GPS signal authentication[J]. Navigation: Journal of The Institute of Navigation, 2012, 59(3): 177-193.

- [9] PANICE G, LUONGO S, GIGANTE G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV[C]//2017 23rd International Conference on Automation and Computing (ICAC). 2017: 1-11.
- [10] MAGIERA J, KATULSKI R. Detection and mitigation of GPS spoofing based on antenna array processing[J]. Journal of applied research and technology, 2015, 13(1): 45-57.
- [11] JANSEN K, SCHÄFER M, MOSER D, et al. Crowd-GPS-Sec: leveraging crowd sourcing to detect and localize GPS spoofing attacks[C]//IEEE Symposium on Security and Privacy (SP). 2018: 1018-1031.
- [12] KWON K C, SHIM D S. Performance analysis of direct GPS spoofing detection method with AHRS / accelerometer[J]. Sensors, 2020, 20(4): 954.



曹春杰（1977—），男，河北衡水人，海南大学教授、博士生导师，主要研究方向为无线网络安全、无人机安全、信息对抗、区块链安全。



赖俊晓（1994—），男，福建漳州人，海南大学硕士生，主要研究方向为人工智能、大数据和物联网安全。

[作者简介]



孙旻（1994—），男，山西大同人，海南大学硕士生，主要研究方向为无人机安全、物联网安全。



于天娇（1995—），女，河南安阳人，海南大学硕士生，主要研究方向为物联网安全、无人机安全和区块链安全。