future internet

MDPI

Article

Knowledge Distillation-Based GPS Spoofing Detection for Small UAV

Yingying Ren [1], Ryan D. Restivo [2], Wenkai Tan [3], Jian Wang [4,*], Yongxin Liu [5], Bin Jiang [6], Huihui Wang [2] and Houbing Song [3]

1 School of Computer, Electronic and Information, Guangxi University, Nanning 530004, China; yingyingren@gxu.edu.cn
2 Department of Cybersecurity, St. Bonaventure University, St. Bonaventure, NY 14778, USA; restivrd19@bonaventure.edu (R.D.R.)
3 Department of Information Systems, University of Maryland, Baltimore County, MD 21250, USA; wtan1@umbc.edu (W.T.); songh@umbc.edu (H.S.)
4 Department of Computer Science, The University of Tennessee at Martin, Martin, TN 38238, USA
5 Department of Mathematics, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA; liuy11@erau.edu
6 Department of Communication Engineering, College of Oceanography and Space Informatics, China University of Petroleum, Qingdao 266580, China
* Correspondence: jwang186@utm.edu

Abstract: As a core component of small unmanned aerial vehicles (UAVs), GPS is playing a critical role in providing localization for UAV navigation. UAVs are an important factor in the large-scale deployment of the Internet of Things (IoT) and cyber–physical systems (CPS). However, GPS is vulnerable to spoofing attacks that can mislead a UAV to fly into a sensitive area and threaten public safety and private security. The conventional spoofing detection methods need too much overhead, which stops efficient detection from working in a computation-constrained UAV and provides an efficient response to attacks. In this paper, we propose a novel approach to obtain a lightweight detection model in the UAV system so that GPS spoofing attacks can be detected from a long distance. With long-short term memory (LSTM), we propose a lightweight detection model on the ground control stations, and then we distill it into a compact size that is able to run in the control system of the UAV with knowledge distillation. The experimental results show that our lightweight detection algorithm runs in UAV systems reliably and can achieve good performance in GPS spoofing detection.

Keywords: knowledge distillation; GPS spoofing; small UAV; long-short term memory; LSTM

Citation: Ren, Y.; Restivo, R.D.; Tan, W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge Distillation-Based GPS Spoofing Detection for Small UAV. *Future Internet* **2023**, *15*, 389. https://doi.org/10.3390/fi15120389

Academic Editors: Wei Yu, Weixian Liao, Fan Liang and Gianluigi Ferrari

Received: 11 October 2023
Revised: 9 November 2023
Accepted: 28 November 2023
Published: 30 November 2023

1. Introduction

With the fast development of the Internet of Things (IoT) and cyber–physical systems (CPSs), many fields (like healthcare [1], agriculture [2], and transportation [3]) have had significant improvements. With the massive deployment of artificial intelligence (AI) and machine learning (ML), 5G New Radio (5G NR)-enabled IoT and CPSs have been implemented in every aspect of human life [4], providing much more accurate, reliable, and intelligent assistance to human activities than a few decades ago. The assistance also helps humans explore unknown areas with much greater assurance of security and safety. At the same time, the new transportation evolution connects IoT and CPS in ground, aerial, and space aspects. Unmanned aerial vehicles (UAVs), as a principal part of IoT and CPSs, connect ground devices with space systems via aerial platforms that are critical to space–aerial–ground communication (SAGC) [5].

Due to their flexibility, UAVs can provide instant services to disaster areas, help workers inspect power lines [6], and assist farmers in spraying pesticides on plants [7]. Accurate localization helps a UAV detect its positioning and control its precise positions,

so that we can ensure that the UAV finishes tasks with high accuracy. The Global Position System (GPS) module leverages satellites' signals to calculate the distance to each satellite so that GPS can output its positions. The GPS is dependent on the accuracy and strength of the satellite's signal, so the GPS utilizes the strong signal to calculate the distance and then outputs its position. Based on this mechanism, hackers can simulate fake GPS signals and amplify them to be over the satellite's signal [8] so the GPS receives the fake GPS signals. The fake GPS signals lead to incorrect localization generation for the GPS module. If the hackers attack the GPS installed in a UAV, they can use the wrong localization to control a UAV to fly into sensitive areas, which can threaten public safety and private security.

The conventional approaches leverage signal processing with equipment to detect abnormal signal sources so that fake GPS signals can be identified. The conventional approaches can identify fake GPS signals with high accuracy, which is good for ground devices [9]. However, the approaches need heavy equipment installed in a UAV, which is not feasible for deployment on a large scale. There are some novel approaches that leverage deep learning and machine learning [10] to detect abnormal GPS signals and identify GPS spoofing. However, the previous methods need a lot of power for computation, which is not suitable for compact UAVs [11]. The conventional approaches cannot provide a compact approach to help UAVs identify GPS spoofing during flight. Without correct identification of GPS spoofing, UAVs cannot prevent fake GPS signals, so the UAV may be compromised and used to conduct crimes by hackers.

In this paper, we propose a novel approach to implementing a lightweight detection algorithm in a small UAV system to detect GPS spoofing. GPS localization is time-sequential. To achieve a good prediction of GPS localization, the algorithm is supposed to have the capability of time sequence prediction. Different from the conventional window-based method, the novel approach detects point-by-point and saves a lot of time on spoofing detection. With long-short term memory (LSTM), we leverage knowledge distillation (KD) to have a lightweight LSTM-enabled detection algorithm that can be deployed in a UAV and assist UAVs in identifying GPS spoofing.

The organization of this paper is as follows: Section 1 introduces our motivations and contributions. Section 2 presents the related work of GPS spoofing and knowledge distillation. Section 3 introduces the system modeling for GPS spoofing. Section 4 states the problems we solved in the paper. Section 5 presents our methodology solving for the problems. Section 6 demonstrates the performance evaluation for our approaches. Section 7 concludes the paper and gives some insights into future work. All symbol definitions are summarized in Appendix A.

2. Related Work

2.1. GPS Spoofing in UAVs

To ensure navigation performance, many UAVs are equipped with GPS modules. The convenience of GPS also creates many vulnerabilities for UAVs. Attackers can interfere with GPS spoofing to mislead the localization of GPS modules [12]. GPS spoofing can cause the remote controller to lose control of the UAV, and then the attackers can control the UAV to conduct crimes and threaten public safety and private security.

The goal of GPS spoofing of UAVs is to leverage fake GPS signals to interfere with UAVs' navigation [13]. The navigation systems of the UAVs are said to be captured once control is secured over their position and velocity estimates [14]. To counteract GPS spoofing, the UAVs need to recognize the attacks.

UAVs can leverage hardware information derived from the autopilot to detect attacks. Ref. [15] analyzes the camera feed on UAVs, inertial measurement units (IMUs), and the velocity generated based on GPS signals. The difference in velocity derived from the GPS and IMUs can be used to detect GPS spoofing [16]. When GPS spoofing is detected, the UAV under attack can leverage IMUs to maintain a steady position [12]. IMUs are typically immune to interference from SDRs due to their use of physical sensors that operate at low frequencies, shielded enclosures, and a lack of dependence on radio frequency signals.

IMUs are designed to measure motion and rotation and do not rely on external signals susceptible to jamming.

Machine learning algorithms can also detect GPS spoofing of UAVs. In [17], the ensemble models of machine learning were used to detect GPS spoofing signals. A support vector machine (SVM) outperforms conventional detection methods [18]. Some research also proves that deep learning is effective at detecting GPS spoofing attacks [19,20].

The current methods can detect GPS spoofing of UAVs remotely and can recognize attacks effectively [21] and efficiently [22]. However, these methods need ground assistance to detect attacks, which cannot extend the range of UAV missions. The range is limited to the coverage of the ground assistance, which is not flexible, efficient, or compact. A compact method of GPS spoofing can reduce the cost of ground assistance and extend the range of UAV missions.

2.2. Knowledge Distillation

With the rapid development of the deep neural network (DNN), there are many advanced applications providing smart and intelligent assistance in many fields. With the compact deployment of AI and ML in computation-limited devices, IoT and CPSs are becoming indispensable to human activities. Advanced communication methods also accelerate cloud computing, fog computing, and edge computing [23] to be deployed ubiquitously to provide computational services. However, these computational services require many computational resources and lack the flexibility to provide instant support when communication quality is low. There are many reasons to deploy lightweight DNNs on computation-limited devices. Transfer learning (TL) is becoming a popular way to make lightweight DNNs feasible for computation-limited devices. Among the many technologies of TL, knowledge distillation has many compact and computation-limited applications.

KD has many explorations on knowledge categories, training schemes, training architectures, distillation algorithms, and performance comparisons [23]. The development speeds up the compact applications deployment in IoT and CPSs. In deployment, the most important part is distilling knowledge, which determines the quality of the networks after distillation. To explore this mechanism, a review mechanism in knowledge distillation uses an attention-based fusion module, a hierarchical context loss function, and a residual learning framework to improve the learning process of the review mechanism. The results show that the mechanism can improve the performance of transferred models on classification, object detection, and instance segmentation tasks [24]. Conventional approaches of KD focus on the transfer of instances and ignore the correlational congruence of KD. A generalized kernel-based Taylor series expansion to capture the correlation between instances in transfer learning was proposed in [25], which outperforms the conventional methods in the accuracy of the identification rate. However, accuracy improves with the sacrifice of storage.

Among the many methods of KD, the most popular model is the teacher–student (TS), which has two different networks: the teacher network and the student network. In KD processing, the student network imitates the input and output of teacher networks, so it does not need additional training materials and preserves private information in some special scenarios. Some research studies have investigated the research of knowledge distillation with the student–teacher framework on vision tasks. Their comprehensive survey explained the mechanisms of knowledge distillation [26]. Due to the different structures, there is a knowledge gap between student and teacher models in knowledge distillation. The gap causes the student models to underfit the teachers' models. A spherical knowledge distillation is proposed to eliminate the gap and significantly improve the students' performance [27]. There are also some applications of TS in different fields. To improve the observation accuracy and reduce the computation load, [28] focuses on human position predictions with transfer learning. With less input, the trained student models achieve similar abilities as the teacher models. Ref. [29] leverages TS to deploy lightweight deep neural networks to UAVs and provide good vision computation services

for UAV delivery. To deploy deep reinforcement learning in a large-scale UAV network, [30] transfers leader knowledge to local UAVs with TS to reduce the overhead for computation. To prevent direct contact with private information, TS transfers the complex neural network to lightweight networks with the consideration of preserving privacy. The new lightweight network is deployed in UAV networking to assist UAVs in recognizing targets [31].

The TS model of KD has the advantage of deploying complex neural networks to compact devices, which can obtain different sophisticated functions from the complex network and help computation-limited platforms achieve intelligent functions. UAVs have their own computation units to finish flights and different missions. TS can help the UAV achieve more smart and intelligent capabilities and adapt to dynamic environments.

3. System Modeling

GPS is critical to the navigation of UAVs. The UAV with a GPS module can receive the signal, Sa_i, from the satellite, which contains a timestamp and position information. The UAV GPS module leverages the information to calculate the localization, Pr_i. Here, $Pr_i = (x_i, y_i, z_i)$. With the collections of multiple satellites' signals, $\sum_{i=1}^{M} Sa_i$, the UAV can have a more accurate localization. However, hackers with software-defined radio (SDR) can simulate the signal generated from the satellite, denoted as Sa_i, to generate a forged signal, denoted as Sd_i, to mislead the UAV into calculating a wrong position, Pf_j. Here, $Pf_j = (x_j, y_j, z_j)$. With strong signals, the hackers can generate multiple forged signals, $\sum_{i=1}^{N} Sd_i$, to control and navigate the spoofed UAV into a sensitive area. In flight, the UAV connects to the ground control station (GCS) with a telemetry radio. The UAV acquires the acceleration, A_k, and the rotation, R_k, data from IMUs and obtains the received signal strength indicator (RSSI) in time l, RS_l. $A_k = (Ax_k, Ay_k, Az_k)$. $R_k = (Ry_k, Rp_k, Rr_k)$. Here, Ax_k, Ay_k, and Az_k represent the acceleration of time k in x, y, and z directions, respectively, and Ry_k, Rp_k, and Rr_k represent rotations of time k in yaw, pitch, and roll, respectively.

4. Problem Statement

With GPS, a UAV can localize its positions and adjust the output of its motors so that it can follow the trajectory designed by the GCS and finish missions. IMUs provide the motion information that enables the UAV to adjust its posture in flight to maintain safety. With the RSSI, the UAV can measure the distance between its localization and the GCS. In our scenarios, the hackers utilize SDR to generate forged GPS signals to send to the GPS module of the UAV. The signal generated from the SDR cannot impact the functionality of IMUs or the telecommunication radio. The telecommunication radio works at frequencies of 433 MHz or 915 MHz.

The attacker model is as follows. The attackers use compact SDR devices (like BladeRF 2.0 [32] and HackRF One [33]) to acquire satellite information. And then, the attacker uses a GPS simulator [34] to generate the forged signal. When the attacker broadcasts the forged signal, the UAV will calculate its localization with the forged signal. The strength of the forged signal surpasses the signal generated from the satellites, which enables the forged signal to be the only source of the GPS for the UAV. With forged signals, the UAV calculates the wrong localization. The wrong localization causes an inconsistency in the velocity and acceleration of the UAV. With this inconsistency, we can detect GPS spoofing attacks Figure 1. However, in practical scenarios, the noise derived from the motion and environment also has effects on the stability of GPS localization.

Conventional approaches have sensitive detection with good environmental noise acquisition, but it is hard to deploy this detection method on compact vehicles like UAVs. UAVs have limited capacities for power supply and loading. In this paper, we will deploy a compact neural network model on a compact device that can be installed on UAVs with less weight and a lower power supply. The compact device can acquire information from GPS, IMUs, and telecommunication radio and detect the status of the UAV to identify if the UAV is under a GPS spoofing attack. In this paper, we focus on GPS spoofing attack detection and lightweight deployment on devices that can be installed in UAVs.

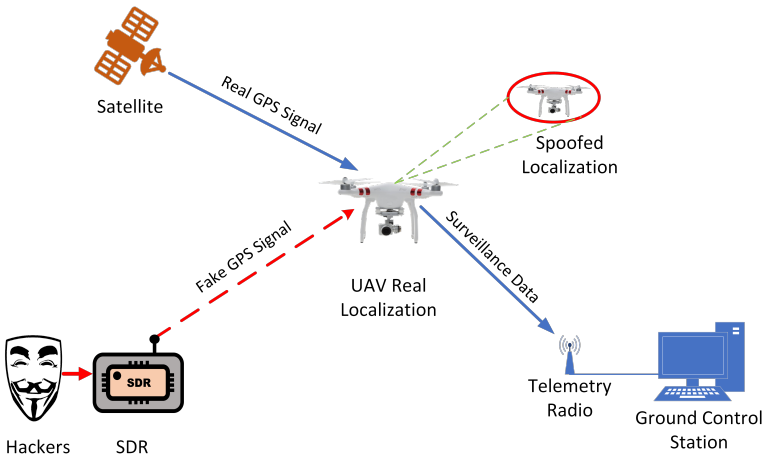

Figure 1. GPS spoofing attack.

5. Methodology

The conventional methods mainly focus on forged signal processing, which needs many computational sources to identify the hackers. Also, signal processing needs additional devices to receive signals, which reduces the loading capacity of UAVs and are hard to deploy on a large scale. Different from conventional methods, we identify the patterns of the movements of an UAV and predict the trajectory to classify the forged signals. LSTM has good performance in time-sequential data prediction [35]. Also, GPS localization has a strong relationship with time sequence. In this section, we first propose an LSTM-based detection model that can identify GPS attacks. And then, we leverage the knowledge distillation method to obtain a lightweight classifier that is able to be installed on computation-limited platforms like UAVs.

5.1. Long-Short Term Memory (LSTM)-Based Detection

With GPS localization, a UAV recognizes its positions effectively and adjusts its mobility to follow the designed trajectory and finish missions. With the correct navigation system, the UAV can avoid obstacles and reach destinations safely. Based on the laws of motion, force, and acceleration, we have

$$P_{t'} = P_t + v \times \Delta t \tag{1}$$

Here, $P_{t'}$ and P_t are two positions of the UAV in time t' and t, v is the speed of the UAV, and Δt is the duration of the measurement, $\Delta t = t' - t$. With IMUs, we can measure the acceleration A of the UAV. With A, we can convert equation 1 to

$$P_{t'} = P_t + \int_t^{t'} A \times \delta \tag{2}$$

Here, δ is the variance of time. Due to noise N existing in IMU, the real acceleration A is different from the measured acceleration $\hat{A}$.

$$\hat{A} = A + N \tag{3}$$

The noise includes thermal noise and zero drift, which are hard to eliminate and predict. The noise is not usually stable during measurement, which causes a loss of confidence in position prediction for the UAV with IMUs. GPS spoofing usually focuses on forged signal broadcasts, which cannot interfere with the functions of IMUs, so IMUs are also used to measure whether the UAV is under GPS spoofing. However, the noise causes many false alarms, which makes it hard to deploy IMU-based methods in real scenarios.

With regard to noise in IMUs, we leverage LSTM to optimize the processing of position prediction of UAVs. Due to its advantages in sequential data [36], LSTM can have good performance on time-sequential data, like position prediction. With the observation of GPS results and IMU measurements, we predict the position variance of the UAV and trigger alerts if the difference between the calculated positions and predicted positions is over the designed threshold, Th_p. Th_p is derived from the limitations of the UAV's mobility [37], which is usually set to 100 mph $\approx$ 44 m/s. We have a preliminary test of different values of Th_p on the false detection rate, which is shown in Figure 2. The triggered alerts indicate that the UAV is under GPS spoofing and needs countermeasures to get rid of the attacks.

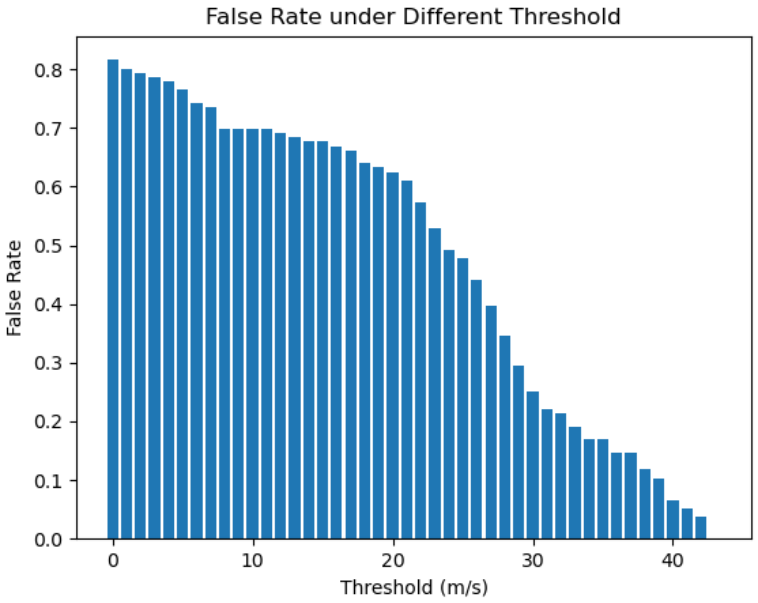

Figure 2. False rate under different Th_p.

With the GPS and IMUs, we have positions, $P_t = (x_t, y_t, z_t)$, and accelerations, $A_t = (Ax_t, Ay_t, Az_t)$, of the UAV. In the position prediction, we put P_t and A_t into LSTM and obtain the predicted position, $P_{\hat{t}}$. To make the two inputs compatible to LSTM [38], we concatenate P_t and A_t into a new array, $PA_t = \{P_t,\ A_t\}$. The integration of LSTM is shown as follows:

$$i_t = \sigma(W_{ii}PA_t + b_{ii} + W_{im}m_{t-1} + W_{ic}c_{t-1} + b_i) \tag{4}$$

In input layer, W_{ii}, W_{ic}, and W_{im} are weight matrices for the input gate to input, cell activation vector, c_{t-1}, and cell activation output vector, m_{t-1}, respectively. b_i is the bias for the input layer. σ is the logistic sigmoid function.

$$f_t = \sigma(W_{fi}PA_t + W_{fm}m_{t-1} + W_{fc}c_{t-1} + b_f) \tag{5}$$

In forget layer, W_{fi}, W_{cf}, and W_{mf} are weight matrices for the forget gate to input, c_{t-1}, and m_{t-1}, respectively. b_f is the bias for the forget layer. $\odot$ is the Hadamard product.

$$c_t = f_t \odot c_{t-1} + i_t \odot g(W_{cx}PA_t + W_{cm}m_{t-1} + b_c) \tag{6}$$

In cell state, g is the cell input activation function. W_{cx} and W_{cm} are weight matrices for the cell state to input and m_{t-1}, respectively. b_c is the bias for the cell state.

$$o_t = \sigma(W_{oi}PA_t + W_{om}m_{t-1} + W_{oc}c_t + b_o) \tag{7}$$

In output layer, W_{oi}, W_{oc}, and W_{om} are weight matrices for the output gates to input, c_t, and m_{t-1}, respectively. b_o is the bias for the forget layer. The output activation vector m_t is

$$m_t = o_t \odot h(c_t) \tag{8}$$

Here, $h()$ is cell output activation function, like *tanh*. The predicted position we have is

$$P_{\hat{t}} = W_{ym} m_t + b_y \tag{9}$$

Here, W_{ym} is the weight matrices for the final result to m_t. b_y is the bias for the final result. Based on the above, the pseudo Algorithm 1 for LSTM-based detection is shown as follows:

Algorithm 1: GPS spoofing detection

$P_{t_0} \leftarrow (x, y, z) \leftarrow GPS$;
$A_{t_0} \leftarrow (A_x, A_y, A_z) \leftarrow IMU$;
Initial $PA_{t_0} = \{P_{t_0}, A_{t_0}\}$;
Load-trained weights of LSTM;
while *Power is on* **do**
  $P_t \leftarrow GPS$;
  $A_t \leftarrow IMU$;
  $PA_t \leftarrow \{P_t,\ A_t\}$;
  $P_{\hat{t}} \leftarrow LSTM(PA_t)$;
  $P_{t+1} \leftarrow GPS$;
  if $\| P_{\hat{t}} - P_{t+1} \| \geq Th_p$ **then**
    Spoofing attack is determined;
  else
    continue;

If GPS spoofing is detected, alerts are sent to the UAV's operating system, which then utilizes its IMUs to navigate to the launch location while disregarding data from the GPS module. The algorithm's complexity and latency are constrained by those of the LSTM. To implement the algorithm on a UAV platform with limited resources, further steps are necessary to optimize its compactness and efficiency.

5.2. KD-Enabled Lightweight Detection

Due to the requirements of flexibility, UAVs usually have limited power and computation resources, which restricts them to being equipped with complex and computationally intensive algorithms. The LSTM trained for GPS spoofing detection is hard to deploy on a UAV platform. We need to tailor some features to make the LSTM compact so that the UAV can use LSTM-based detection onboard. The conventional approaches make adjustments to the architectures of the LSTM to reduce the consumption of computation and storage, which is a good method for deployment. However, the conventional approaches also lose accuracy control, which means that the performance of the algorithms will drop dramatically and cannot be controlled. This section uses knowledge distillation methods to obtain compact LSTM-based detection. We transfer performance from a teacher model (the trained LSTM), $T(PA_t)$, to a student model (a small NN model), $S(PA_t)$, with knowledge distillation.

For the teacher model, $T(PA_t)$ is a complex LSTM model, as described in Section 5.1. Trained with datasets, $T(PA_t)$ can achieve competitive performance on position predictions. However, $S(PA_t)$ is lightweight, which is different from $T(PA_t)$. $S(PA_t$ is combined with multiple 1D neural network (NN) layers, one fully connected layer, and one softmax layer. We leveraged the mean squared error (MSE) to calculate the loss of training $S(PA_t)$. The loss function is described as follows:

$$\mathbb{L} = \| T(PA_t) - S(PA_t) \| \tag{10}$$

With the configuration of the student model and teacher model, the loss paradigm of knowledge distillation can be

$$L = \mathbb{L}_1(S(PA_t), T(PA_t)) + \alpha \mathbb{L}_2(S(PA_t), P_{t'}) \quad (11)$$

Here, $L_1()$ and $L_2()$ are the loss functions of the student model vs. the teacher model and the student model vs. the real positions. $\mathbb{L}_1 = \| T(PA_t) - S(PA_t) \|$ and $\mathbb{L}_2 = \| P_{\hat{t}} - S(PA_t) \|$. α are the balance factors for the loss between $L_1()$ and $L_2()$.

The trained student model, $S'(PA_t)$, was deployed on a compact platform to test its performance and resource consumption; then, $S'(PA_t)$ was deployed in the UAV controller to detect GPS spoofing. As Algorithm 1 shows, we replaced the trained LSTM model with the student model, $S'(PA_t)$. At the initial phase, we loaded the original positions, PA_{t0}, and the trained weights of LSTM. When the power of the UAV was on, the algorithm ran without stopping. In the while loop, the algorithm acquired GPS data, P_t, and acceleration data, A_t, from the GPS module and IMU module, respectively. As the data went through the LSTM model, we could obtain $P_{\hat{t}}$. We compared the $P_{\hat{t}}$ with the updated data, P_{t+1}, from the GPS module. If the difference was over the threshold, the spoofing attack was detected. As the data go in as input, the storage size and time consumption do not change, so the complexity is O(1).

6. Evaluation

With compact and efficient GPS spoofing algorithms, UAVs can avoid attacks remotely, and the threats from the manipulated UAVs can be reduced. With KD and LSTM, our proposed approach enables UAVs to detect GPS spoofing attacks efficiently and automatically. In this section, we will evaluate the performance of LSTM-based GPS spoofing and the efficiency of KD-enabled lightweight detection. We utilize the open-source dataset derived from IEEE DataPort [39]. The dataset contains a comprehensive log of a benign flight and one where the UAV experiences GPS spoofing attacks. In the dataset, a Great Scott Gadgets SDR with GPS-SDR-SIM tools is utilized to enact GPS spoofing attacks. The evaluation is executed on Pycharm 2022.3.2 and the configuration of the workstation is as the following. CPU: Intel(R) Core(TM) i9-10900X CPU @ 3.70GHz; GPU: NVIDIA RTX A4000; OS: Ubuntu 18.04 LTS.

6.1. GPS Spoofing Detection

We compared our proposed method with a gated recurrent unit (GRU) [40] and a recurrent neural network (RNN) [41]. In Algorithm 1, we compared the GRU, RNN, and LSTM in terms of the performance of GPS detection. With the benign flight data, we trained the LSTM, GRU, and RNN to predict the GPS data with a time sequence. According to the training result, we set $Th_p = 1200$ as the detection baseline for a spoofing attack, which also considers reducing the false-positive situations. The configuration of the LSTM, GRU, and RNN is shown in Table 1. To prevent overfitting and underfitting, we set the epoch at 3000.

Table 1. Configuration of Networks.

Parameters	LSTM	GRU	RNN
Input Size	6	6	6
Hidden Size	12	12	12
Number of Layers	12	12	12
Number of Classes	1	1	1
Output Size	3	3	3
Learning Rate	0.001	0.001	0.001

We evaluated the performance of the LSTM, GRU, and RNN in the GPS spoofing dataset, as shown in Figures 3–5. In the dataset, a GPS spoofing attack at the time stamp

347844445 is marked in green in the figures. When the spoofing attack is detected, the start point is marked in yellow.

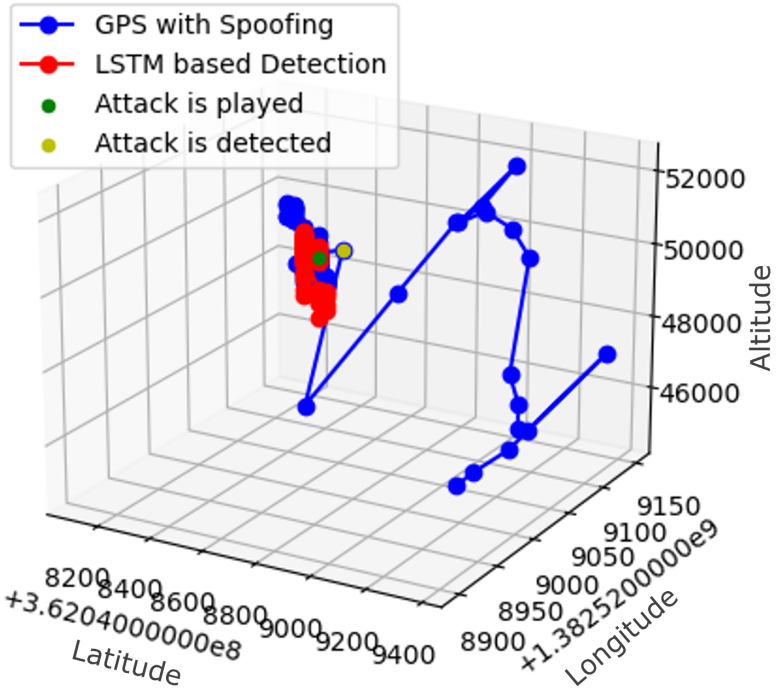

Figure 3. LSTM-based GPS spoofing detection.

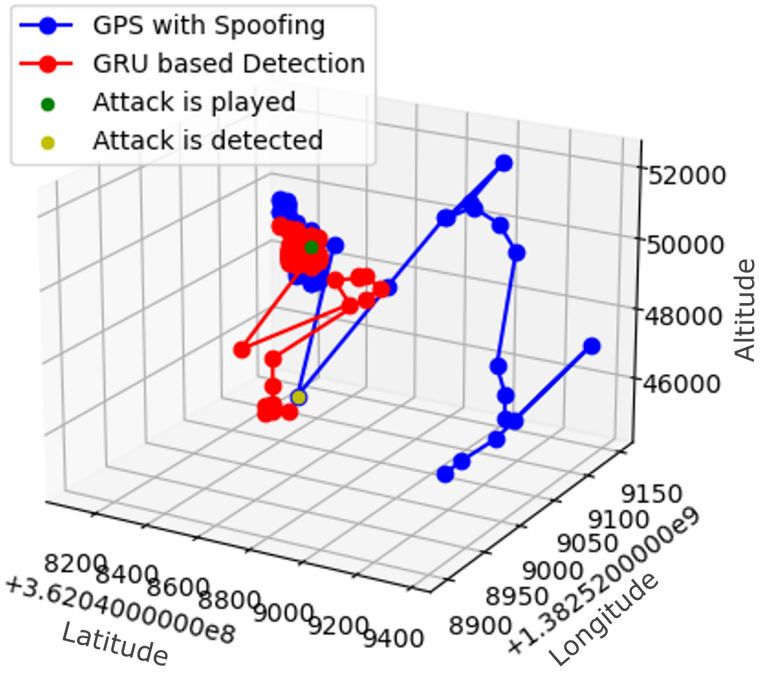

Figure 4. GRU-based GPSspoofing detection.

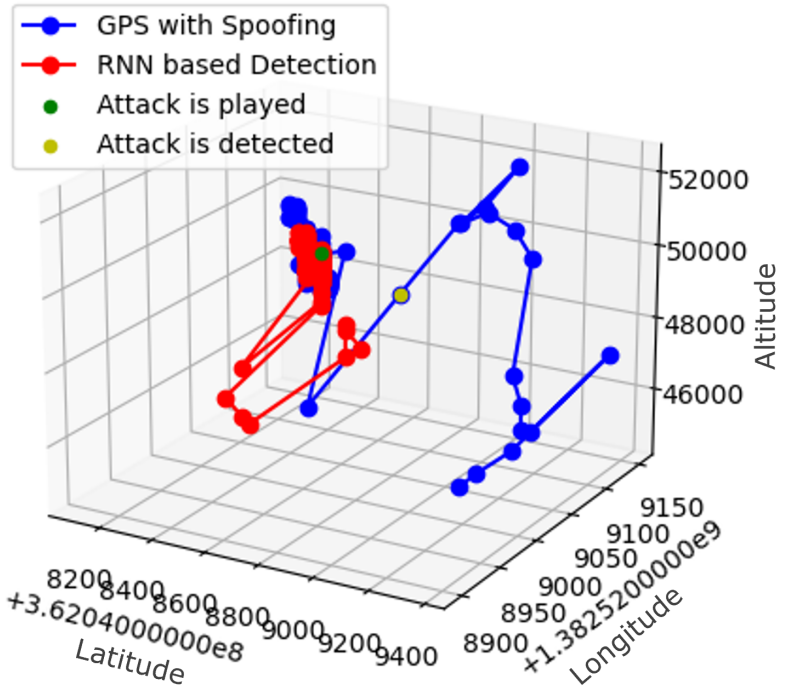

Figure 5. RNN-based GPSspoofing detection.

Figure 3 shows the LSTM-based GPS spoofing detection. Figure 3 shows that the LSTM-based approach has good stability for the GPS location prediction, which could help the small UAV to fly in a stable status. Also, we can see the detection point (timestamp: 348732228) is close to the spoofing attacking point, which is critical to rescuing the UAV and getting rid of the spoofing attack. Figure 3 shows that the LSTM-based approach can detect the spoofing attack successfully.

Figure 4 shows the GRU-based GPS spoofing detection. Figure 4 shows that the GRU-based approach has good stability for the GPS location prediction before the spoofing attack is triggered. Compared with the LSTM-based approach, we can see that the detection point (timestamp: 361729095) is a little bit later than in the LSTM-based approach. However, the GRU approach can also detect the spoofing attack successfully. When the spoofing attack is enacted, the GRU-based detection has fluctuations in the location prediction, which could cause the flight shake of the small UAV even though the small UAV is stable generally.

Figure 5 shows the RNN-based GPS spoofing detection. Figure 4 shows that the RNN-based approach has good stability for the GPS location prediction before the spoofing attack is triggered. We can see that the detection point (timestamp: 365732590) is a little bit later than in the LSTM-based and GRU-based approaches. However, the GRU approach can also detect the spoofing attack successfully. When the spoofing attack is enacted, the RNN-based detection has sharp fluctuations in location prediction, which could cause serious effects on the safe flight of the small UAV and increase the risk of a crash.

From the figures, we can see that LSTM-based detection can generate stable GPS prediction points for navigation. GRU-based GPS detection begins to generate fluctuating positions when the attacks are enacted.

6.2. Lightweight Detection

With the TS model, we obtained distilled modeling for lightweight detection. To transfer to another platform easily, we used a neural network (NN) as a student model to obtain a lightweight network. With the survey investigation [42], we set the balance factor, α, as 0.45. The parameter of the NN is shown in Table 2.

Table 2. Configuration of NN.

Input Size	Output Size	Hidden Layer
6	3	(16, 8)

With the benign flight data, we distilled the LSTM, GRU, and RNN models into NN models and predicted the GPS data with time sequences. The model parameters of the LSTM, GRU, and RNN are listed in Table 3. After distillation, we evaluated the distilled models with the previous experiments. Each of the distilled models is implemented to detect the spoofing point. The results are shown in Figure 6, which includes three subfigures (a), (b), and (c). Figure 6a–c are the results of the LSTM-distilled NN, GRU-distilled NN, and RNN-distilled NN, respectively.

Table 3. Parameters of the distilled models.

Models	LSTM	GRU	RNN
Model Size	72.7 kb	57.8 kb	27.7 kb
NN Model Size	3.0 kb	3.0 kb	3.0 kb
NN Model Overhead	266.88 Mb	266.88 Mb	266.88 Mb
Overhead	390.37 Mb	391.29 Mb	389.84 Mb
Learning Rate	0.001	0.001	0.001
Balance Factor	0.45	0.45	0.45
Model Reduced	95.74%	94.80%	89.17%
Overhead Reduced	31.63%	31.79%	31.54%

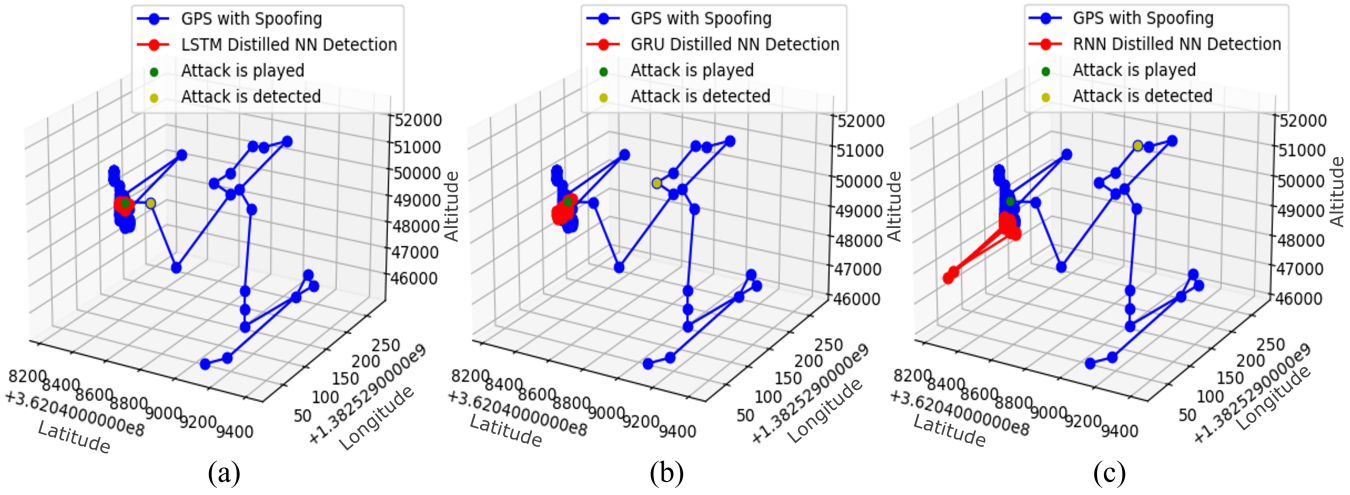

Figure 6. KD-based GPS spoofing detection.

Figure 6a is the result of the LSTM-distilled NN detection. The result shows that the LSTM-distilled NN has good stability for the GPS localization prediction, which can maintain a similar stability to the LSTM in a small UAV's flight control. The spoofing detection point is at the timestamp 374727138, which is later than in the LSTM-based detection. However, the detection of the LSTM-distilled NN can still help the small UAV find the spoofing attacks successfully. Due to its lightweight characteristics, the LSTM-distilled NN may be implemented on compact platforms that have constraints on computational resources.

Figure 6b is the result of the GRU-distilled NN detection. Generally, the GRU-distilled NN has similar capabilities for maintaining stable flight control of the small UAV. However, we found that the GPS spoofing detection point (timestamp: 375735466) is far later than in the LSTM-distilled NN model. From Figure 6b, we can see that the trajectory of the GPS

has already fluctuated sharply by this point, so it is weak in defending against the spoofing attack.

Figure 6c is the result of the RNN-distilled NN detection. Different from the LSTM-distilled NN and GRU-distilled NN, the RNN-distilled NN has weak performance in maintaining the stable flight control of the small UAV. We can see that the GPS location prediction of the RNN-distilled NN model still has sharp fluctuations. At the same time, the GPS spoofing detection point (timestamp: 377731032) is far later than the LSTM-distilled NN and GRU-distilled NN models. From Figure 6b, we can see that the trajectory of the GPS has already fluctuated sharply by this point, so it is not capable of defending against the spoofing attack.

In summary, compared with the GRU-distilled NN and RNN-distilled NN models, the LSTM-distilled NN has more potential to be implemented on compact platforms.

7. Conclusions

In this paper, we propose a novel approach to implementing a lightweight detection model for UAV systems so that GPS spoofing attacks can be detected from a long distance. With LSTM, we proposed a novel detection in ground control stations, and then we transferred it into the control system of a UAV with knowledge distillation in a compact size. The experimental results show that our lightweight detection model detects GPS spoofing attacks efficiently. Due to the resource restrictions of compact platforms, the platform has strict requirements for implementation, like communication efficiency. In addition, the detection results need to be delivered to the ground so that the ground response team can eliminate the attacks. In future research, we will implement the model onto compact platforms that can be integrated into a UAV system.

Author Contributions: Conceptualization, Y.R., J.W. and H.S.; Methodology, J.W. and B.J.; Software, Y.R., J.W. and Y.L.; Validation, W.T., J.W., Y.L. and B.J.; Formal analysis, Y.R., W.T., Y.L. and H.W.; Investigation, R.D.R. and H.W.; Resources, H.W. and H.S.; Supervision, H.S.. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: IEEE DataPort [39].

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Symbol Summary

Table A1. Symbol Summary

Symbols	Definition
Sa_i	The signal a GPS module received.
Pr_i	GPS location: $Pr_i = (x_i, y_i, z_i)$.
Sd_i	The forged GPS signal.
A_k	Acceleration of UAV at time k.
(Ax_k, Ay_k, Az_k)	Acceleration of UAV in x, y, and z axis at time k.
R_k	Rotation of UAV at time k.
(Ry_k, Rp_k, Rr_k)	Rotation of UAV in yaw, pitch, roll at time k.
RS_l	The received signal strength indicator (RSSI).
$P_{t'}, P_t$	Position at time t' and t.
v	The speed of UAV.
A	Acceleration of UAV.
N	Thermal noise and zero drift.
Th_p	Threshold of UAV movement.
PA_t	Combination of P_t and A_t.

Table A1. *Cont.*

Symbols	Definition
W_{ii}, W_{ic}, and W_{im}	Weight matrices for the input gate.
c_{t-1}	Cell activation vectors.
m_{t-1}	Cell activation output vector.
b_i	Bias for the input layer.
σ	Logistic sigmoid function.
W_{fi}, W_{cf}, and W_{mf}	Weight matrices for the forget gate.
b_f	Bias for forget layer.
$\odot$	The Hadamard product.
g	Cell input activation function.
W_{cx}	Weight matrices for the cell state.
b_c	Bias for cell state.
W_{oi}, W_{oc}, and W_{om}	Weight matrices for the output gates.
b_o	Bias for forget layer.
m_t	Output activation vector.
$h()$	Cell output activation function.
W_{ym}	Weight matrices for the final result.
$T(PA_t)$	The teacher model.
$S(PA_t)$	A student model.
$L_1()$	The loss functions of the student model vs. the teacher model.
$L_2()$	The loss functions of the student model vs. the real positions.

References

1. Qiu, H.; Qiu, M.; Liu, M.; Memmi, G. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2499–2505. [CrossRef] [PubMed]
2. Liu, R.; Zhang, Y.; Ge, Y.; Hu, W.; Sha, B. Precision Regulation Model of Water and Fertilizer for Alfalfa Based on Agriculture Cyber-Physical System. *IEEE Access* **2020**, *8*, 38501–38516. [CrossRef]
3. Wang, K.; Yuan, L.; Miyazaki, T.; Chen, Y.; Zhang, Y. Jamming and Eavesdropping Defense in Green Cyber—Physical Transportation Systems Using a Stackelberg Game. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4232–4242. [CrossRef]
4. Siozios, K.; Soudris, D.; Kosmatopoulos, E. An Overview of Emerging Systems-Related Concepts, Approaches and Technologies Unifying and Advancing S&T Achievements of the Past Decades (e.g., CPS, IoT, I2oT, SoS/E, 5G and Cross-Cutting Decision Making). In *Cyber-Physical Systems: Decision Making Mechanisms and Applications*; IEEE: Piscataway, NJ, USA, 2017; pp. 1–98.
5. Lu, H.; Duan, X. Collaborative Computing for Space-Air-Ground Integrated Vehicular Networks. In Proceedings of the 2021 International Conference on Space-Air-Ground Computing (SAGC), Huizhou, China, 23–25 October 2021; pp. 175–177. [CrossRef]
6. Zhou, Z.; Zhang, C.; Xu, C.; Xiong, F.; Zhang, Y.; Umer, T. Energy-Efficient Industrial Internet of UAVs for Power Line Inspection in Smart Grid. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2705–2714. [CrossRef]
7. Bacco, M.; Berton, A.; Gotta, A.; Caviglione, L. IEEE 802.15.4 Air-Ground UAV Communications in Smart Farming Scenarios. *IEEE Commun. Lett.* **2018**, *22*, 1910–1913. [CrossRef]
8. Eldosouky, A.; Ferdowsi, A.; Saad, W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet Things J.* **2020**, *7*, 2840–2854. [CrossRef]
9. Dang, Y.; Benzaïd, C.; Shen, Y.; Taleb, T. GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
10. Ahmad, M.; Farid, M.A.; Ahmed, S.; Saeed, K.; Asharf, M.; Akhtar, U. Impact and Detection of GPS Spoofing and Countermeasures against Spoofing. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019; pp. 1–8. [CrossRef]
11. Dang, Y.; Benzaïd, C.; Yang, B.; Taleb, T. Deep Learning for GPS Spoofing Detection in Cellular-Enabled UAV Systems. In Proceedings of the 2021 International Conference on Networking and Network Applications (NaNA), Lijiang, China, 29 October–1 November 2021; pp. 501–506. [CrossRef]
12. Dey, V.; Pudi, V.; Chattopadhyay, A.; Elovici, Y. Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. In Proceedings of the 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, India, 6–10 January 2018; pp. 398–403. [CrossRef]
13. Ranyal, E.; Jain, K. Unmanned Aerial Vehicle's Vulnerability to GPS Spoofing a Review. *J. Indian Soc. Remote Sens.* **2020**, *49*, 585–591. [CrossRef]

14. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned Aircraft Capture and Control Via GPS Spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
15. Qiao, Y.; Zhang, Y.; Du, X. A Vision-Based GPS-Spoofing Detection Method for Small UAVs. In Proceedings of the 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, 15–17 December 2017; pp. 312–316. [CrossRef]
16. Zou, Q.; Huang, S.; Lin, F.; Cong, M. Detection of GPS spoofing based on UAV model estimation. In Proceedings of the IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 24–27 October 2016; pp. 6097–6102. [CrossRef]
17. Gasimova, A.; Khoei, T.T.; Kaabouch, N. A Comparative Analysis of the Ensemble Models for Detecting GPS Spoofing attacks on UAVs. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Virtual Conference, 26–29 January 2022; pp. 0310–0315. [CrossRef]
18. Panice, G.; Luongo, S.; Gigante, G.; Pascarella, D.; Di Benedetto, C.; Vozella, A.; Pescapè, A. A SVM-based detection approach for GPS spoofing attacks to UAV. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–11. [CrossRef]
19. Agyapong, R.A. Efficient Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles Using Deep Learning. In Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 5–7 December 2021.
20. Chen, X.; Li, T.; Liu, H.; Huang, Q.; Gan, X. A GPS Spoofing Detection Algorithm for UAVs Based on Trust Evaluation. In Proceedings of the 2023 IEEE 13th International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Qinhuangdao, China, 11–14 July 2023; pp. 315–319. [CrossRef]
21. Dang, Y.; Karakoc, A.; Norshahida, S.; Jäntti, R. 3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs. *IEEE Trans. Mach. Learn. Commun. Netw.* **2023**, *1*, 313–327. [CrossRef]
22. Demir, M.Ö.; Kurt, G.K.; Pusane, A.E. A Pseudorange-Based GPS Spoofing Detection Using Hyperbola Equations. *IEEE Trans. Veh. Technol.* **2023**, *72*, 10770–10783. [CrossRef]
23. Gou, J.; Yu, B.; Maybank, S.J.; Tao, D. Knowledge Distillation: A Survey. *Int. J. Comput. Vis.* **2021**, *129*, 1789–1819. [CrossRef]
24. Chen, P.; Liu, S.; Zhao, H.; Jia, J. Distilling Knowledge via Knowledge Review. In Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Los Alamitos, CA, USA, 20–25 June 2021; pp. 5006–5015. [CrossRef]
25. Peng, B.; Jin, X.; Li, D.; Zhou, S.; Wu, Y.; Liu, J.; Zhang, Z.; Liu, Y. Correlation Congruence for Knowledge Distillation. In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Los Alamitos, CA, USA, 27 October–2 November 2019; pp. 5006–5015. [CrossRef]
26. Wang, L.; Yoon, K. Knowledge Distillation and Student-Teacher Learning for Visual Intelligence: A Review and New Outlooks. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *44*, 3048–3068. [CrossRef] [PubMed]
27. Guo, J.; Chen, M.; Hu, Y.; Zhu, C.; He, X.; Cai, D. Reducing the Teacher-Student Gap via Spherical Knowledge Disitllation. *arXiv* **2020**, arXiv:2010.07485.
28. Monti, A.; Porrello, A.; Calderara, S.; Coscia, P.; Ballan, L.; Cucchiara, R. How many Observations are Enough? Knowledge Distillation for Trajectory Forecasting. In Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Los Alamitos, CA, USA, 18–24 June 2022; pp. 6543–6552. [CrossRef]
29. Luo, H.; Chen, T.; Li, X.; Li, S.; Zhang, C.; Zhao, G.; Liu, X. KeepEdge: A Knowledge Distillation Empowered Edge Intelligence Framework for Visual Assisted Positioning in UAV Delivery. *IEEE Trans. Mob. Comput.* **2022**, 4729–4741. [CrossRef]
30. Wang, Z.; Wei, Y.; Wu, F. Knowledge Distillation based Cooperative Reinforcement Learning for Connectivity Preservation in UAV Networks. In Proceedings of the 2021 International Conference on UK-China Emerging Technologies (UCET), Chengdu, China, 4–6 November 2021; pp. 171–176. [CrossRef]
31. Yu, G. Data-Free Knowledge Distillation for Privacy-Preserving Efficient UAV Networks. In Proceedings of the 2022 6th International Conference on Robotics and Automation Sciences (ICRAS), Wuhan, China, 9–11 June 2022; pp. 52–56. [CrossRef]
32. Nuand. bladeRF 2.0, Available online: https://github.com/Nuand/bladeRF.git (accessed on 8 November 2023).
33. Martoyo, I.; Setiasabda, P.; Kanalebe, H.Y.; Uranus, H.P.; Pardede, M. Software Defined Radio for Education: Spectrum Analyzer, FM Receiver/Transmitter and GSM Sniffer with HackRF One. In Proceedings of the 2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME), Balikpapan, Indonesia, 10–11 December 2018; pp. 188–192. [CrossRef]
34. Ebinuma, T. Gps-sdr-sim. *Github*, 2018. Available online: https://github.com/osqzss/gps-sdr-sim (accessed on 23 May 2021).
35. Meng, X.; Fu, H.; Peng, L.; Liu, G.; Yu, Y.; Wang, Z.; Chen, E. D-LSTM: Short-Term Road Traffic Speed Prediction Model Based on GPS Positioning Data. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 2021–2030. [CrossRef]
36. Kim, J.; Lee, H.; Kim, S.; Park, J.H. Real-Time Power System Transient Stability Prediction Using Convolutional Layer and Long Short-Term Memory. *J. Electr. Eng. Technol.* **2023**, *18*, 2723–2735. [CrossRef]
37. Ludwig, N. 14 CFR Part 107 (UAS)–Drone Operators Are Not Pilots 14. Available online: https://www.suasnews.com/wp-content/uploads/2017/12/AS480-Research-Paper.pdf (accessed on 8 November 2023).
38. Sak, H.; Senior, A.; Beaufays, F. Long Short-Term Memory Based Recurrent Neural Network Architectures for Large Vocabulary Speech Recognition. *arXiv* **2014**, arXiv:1402.1128.
39. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. UAV Attack Dataset. *IEEE Dataport* **2020**. [CrossRef]
40. Liu, H.; Wu, H.; Sun, W.; Lee, I. Spatio-Temporal GRU for Trajectory Classification. In Proceedings of the 2019 IEEE International Conference on Data Mining (ICDM), Beijing, China, 8–11 November 2019; pp. 1228–1233. [CrossRef]

41. Mosavi, M.R.; Sorkhi, M. An efficient method for optimum selection of GPS satellites set using Recurrent Neural Network. In Proceedings of the 2009 IEEE/ASME International Conference on Advanced Intelligent Mechatronics, Singapore, 14–17 July 2009; pp. 245–249. [CrossRef]
42. Niu, S.; Liu, Y.; Wang, J.; Song, H. A Decade Survey of Transfer Learning (2010–2020). *IEEE Trans. Artif. Intell.* **2020**, *1*, 151–166. [CrossRef]