Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5517500, 16 pages
https://doi.org/10.1155/2021/5517500

Research Article

An Approach of Linear Regression-Based UAV GPS Spoofing Detection

Lianxiao Meng,[1,2] **Lin Yang**,[2] **Shuangyin Ren**,[2] **Gaigai Tang**,[2,3] **Long Zhang**,[2] **Feng Yang**,[2] **and Wu Yang**[1]

[1]*Information Security Research Center of Harbin Engineering University, Harbin, China*
[2]*National Key Laboratory of Science and Technology on Information System Security, Systems Engineering Institute, AMS, PLA, Beijing, China*
[3]*Harbin Engineering University, Harbin, China*

Correspondence should be addressed to Wu Yang; yangwu@hrbeu.edu.cn

Received 8 January 2021; Revised 23 February 2021; Accepted 1 April 2021; Published 7 May 2021

Academic Editor: Xiaojie Wang

A prominent security threat to unmanned aerial vehicle (UAV) is to capture it by GPS spoofing, in which the attacker manipulates the GPS signal of the UAV to capture it. This paper introduces an anti-spoofing model to mitigate the impact of GPS spoofing attack on UAV mission security. In this model, linear regression (LR) is used to predict and model the optimal route of UAV to its destination. On this basis, a countermeasure mechanism is proposed to reduce the impact of GPS spoofing attack. Confrontation is based on the progressive detection mechanism of the model. In order to better ensure the flight security of UAV, the model provides more than one detection scheme for spoofing signal to improve the sensitivity of UAV to deception signal detection. For better proving the proposed LR anti-spoofing model, a dynamic Stackelberg game is formulated to simulate the interaction between GPS spoofer and UAV. In particular, for GPS spoofer, it is worth mentioning that for the scenario that the UAV is cheated by GPS spoofing signal in the mission environment of the designated route is simulated in the experiment. In particular, UAV with the LR anti-spoofing model, as the leader in this game, dynamically adjusts its response strategy according to the deception's attack strategy when upon detection of GPS spoofer's attack. The simulation results show that the method can effectively enhance the ability of UAV to resist GPS spoofing without increasing the hardware cost of the UAV and is easy to implement. Furthermore, we also try to use long short-term memory (LSTM) network in the trajectory prediction module of the model. The experimental results show that the LR anti-spoofing model proposed is far better than that of LSTM in terms of prediction accuracy.

1. Introduction

With the progress of science and technology and the continuous reduction of manufacturing costs, UAV has entered the industrial production and people's daily life from the military field. Nowadays, UAV has been widely used in film and television shooting, agricultural monitoring, power inspection, personal aerial photography, meteorological monitoring, forest fire detection, traffic control, cargo transportation, and emergency rescue [1–3]. However, while UAV brings all kinds of convenience to our production and life, the security problems it faces are being gradually exposing.

At present, the common attacks on UAV mainly include the attacks on UAV sensors, UAV network, radio interference and hijacking, and GPS spoofing [4]. In these attacks, GPS spoofing is regarded as one of the most urgent threats, because it is practical and can be easily executed against UAV [5–7].

GPS spoofing refers to the following: in order to mislead the GPS navigation and positioning signal in the designated area, GPS attacker transmits pseudonavigation signal which cannot be effectively detected under the concealment condition because of its certain similarity with the real GPS signal, and user can get the false positioning, speed, and time

information from this type spoofing signal and finally be captured [8]. It should be pointed out that GPS spoofing is different from GPS jamming. GPS suppression jamming uses high-power jammer to transmit different types of suppression signals, which makes the target receiver unable to receive normal GPS signals, and users cannot obtain navigation, positioning, and timing results, which leads to the unavailability of GPS system [9]. GPS spoofing refers to the false signal to induce the GPS receiver to capture and track errors, so as to solve the wrong positioning, time, and speed information without being detected, achieving the purpose of cheating users. Because GPS spoofing often does not need strong transmitting power, it has good concealment and can guide related users to navigate in the wrong way to a certain extent, which also makes the deception have strong survivability. To some extent, the harm of spoofing jamming is more serious than that of suppressing jamming.

The vulnerability of GPS is the basis of GPS deception. The vulnerability of GPS mainly includes navigation signal format disclosure, navigation data format disclosure, and no protection for broadcast channel. In the current situation, GPS spoofing can be divided into three types [10, 11]: forwarding spoofing, generative spoofing, and track tracking spoofing. Detailed descriptions of the three spoofing are as follows, among them, the first two are the most commonly used and we choose the second type to solve in this paper.

(i) Forwarding spoofing: by recording the real GPS signal in the predeception positioning, forwarding spoofing uses the software to define radio and other signal transmitting equipment. Due to the fact that the structure of PN (pseudonoise) code cannot be changed and only the measurement value of pseudorange can be changed in the process of deception, the control flexibility is relatively poor, and the forwarding deception signal is easily detected. Therefore, the use of forwarding spoofing is often limited

(ii) Generative spoofing: it is to extract time, positioning, satellite ephemeris, and other necessary information from the real GPS signal, generate false GPS signal according to the predeception time and positioning information, and send it to the GPS receiver through the matrix antenna. This method does not require the current state of the receiver. It can cheat both the receiver in the acquisition state and the receiver in the steadytracking state [12]. Therefore, generative deception is often more practical

(iii) Track tracking spoofing: it mainly aims at the real-time flying air target [13]. Generally, the ground radar and other sensors detect the flight path of the aircraft in real time and send the detected air target positioning, speed, and other motion information to the deception equipment through the data link. Compared with the real signal, the deception signal produced by this method has higher fidelity and is not easy to be detected by other sensors such as inertial navigation system. Meanwhile, it has high requirements for the accuracy of the generated signal simulation, so it is difficult to be realized in practice

1.1. Problems to Be Solved. UAV is now in the critical period of transition from semi-intelligent to intelligent, and its main barrier is the degree of human intervention in flight tasks. Among them, fixed-point cruise only depends on preset information in flight, without any human operation, whether it can be completed safely is the first step to enter the era of UAV intelligence in the future. So in this paper, we choose the flight security of UAV in fixed-point cruise mission as the main research issue, that is, the UAV flies along the points selected in advance based on GPS positioning function. When the next selected flight location of the UAV is cheated by the fake GPS location, it is worth mentioning, the GPS spoofing here does not change the positioning of UAV, but rather changes its cognitive belief. By doing so, it is obvious that the UAV will betray its flight trajectory and fly in the direction of the connection between the deceiving location and the destination until it reaches the capture point [14], as showed in Figure 1. We expect to build an antispoof model, which can effectively prevent UAV from being trapped in such entrapment.

From the above analysis, it can be seen that the current GPS spoofing technology has a relatively clear technical implementation path. Therefore, it is necessary to put forward prevention strategies for the main deception technology in the current navigation system of UAV and other similar equipment.

1.2. Contributions. In view of the above problem, there are indeed many solutions, but they basically stop at detecting GPS spoofing, and there is no further action to ensure the mission going. Thus, the main contribution of this paper is to provide a general framework for UAV to reduce the impact of acquisition attack by detecting and defending GPS spoofing interference. Unlike previous work, our framework not only supports UAV detection of GPS spoofing attacks but also can guide UAV return to the previous flight path after detecting the attack and deviating from the route. This will enable the UAV to avoid being captured and complete its mission. In summary, our contributions are threefold:

(i) An LR anti-spoofing model for UAV is proposed in this paper. The flight trajectory prediction model of UAV is built by fitting the flight log of UAV with LR model, and the prediction accuracy is relatively high among all the methods. The model not only realizes the safety detection of UAV flight status in the process of mission but also realizes the deception mitigation when UAV is cheated, so as to ensure the smooth completion of flight mission

(ii) In order to meet the experimental needs, we built a GPS deception generator and realized the reappearance of deception scene when we analyzed the GPS deception problem faced by UAV

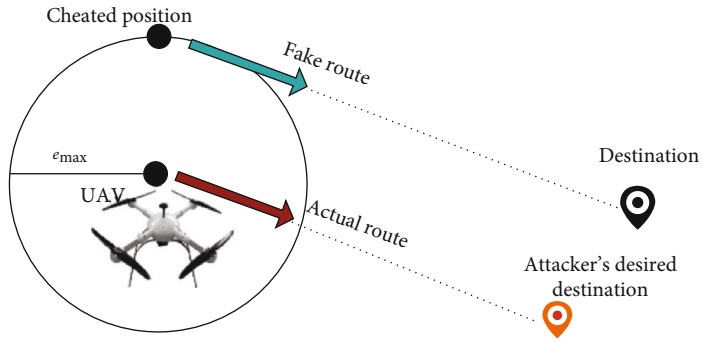

Figure 1: UAV actual and fake route.

(iii) In order to prove the effectiveness of the proposed LR anti-spoofing model, we design a Stackelberg attack and defense game consisting of GPS spoofer and UAV with LR anti-spoofing model. In this game, for the dynamic change of spoofing signal, it strongly proves that our algorithm can still achieve effective detection and resistance

The rest of this paper is organized as follows. Section 2 mainly introduces the current situation of GPS spoofing detection scheme. The UAV's LR anti-spoofing model is presented in Section 3. Section 4 describes the Stackelberg game scenarios in detail. In Section 5, we give details of our experimental setting, results, and corresponding analysis. The conclusions and future works are discussed in Section 6.

2. Related Work

In the world, there are frequent incidents of GPS positioning and navigation [15]. The most serious incident in the field of UAV security is Iran's capture of RQ-170 military UAV of the United States in 2011 [16]. In June 2012, Humphreys' research team of Texas State University successfully demonstrated in a track and field that the GPS spoofing device with hardware cost less than $1000 can change the flight path of a small UAV in real time by releasing deceptive jamming signals. Later, the team successfully demonstrated at the white sand missile range of the United States. In addition, in 2013, the team successfully used GPS deception technology to induce an $80 million white rose yacht to deviate 3° to the left, causing it to deviate 1 km from the scheduled route [17].

Nowadays, there are several protection methods for GPS spoofing at home and abroad, as follows:

(1) Signal physical layer characteristic detection method: GPS false signals are identified by comparing the characteristics of false signals and real signals in the signal physical layer. These differences mainly include automatic gain control [18], signal arrival direction, carrier phase value, and Doppler frequency shift [19]. Psiaki and others [20] [21] analyzed the principle of GPS deception detection based on the direction of arrival of signals. The angle of arrival of signals was determined by the change of signal carrier phase between different antennas, so as to judge whether the current target was attacked by GPS spoofing, and proposed a deception detection scheme based on the arrival direction of GPS signal. Ranganathan and others [22] proposed a deception detection method called auxiliary peak tracking, which can be used in combination with navigation message checker to track the strongest satellite signal and other weak environmental signals. Kang et al. [23] proposed a method to estimate the difference between the direction of arrival (DOA) and the measured DOA using GPS ephemeris and ephemeris data and used GPS directional antenna to detect deception

(2) Verification detection method based on cryptography: after receiving the signal, the receiver needs to decode the signal and authenticate the sender of the signal. Wesson et al. [24] proposed a probability model GPS signal authentication method based on statistical hypothesis test, which combines cryptographic source authentication with code timing authentication [25] and detects GPS spoofing attacks by using pseudorandom noise code of GPS signals

(3) Using other equipment to assist positioning detection method, through the use of inertial navigation, wireless network and cellular network, and other auxiliary means combined with GPS receiver to achieve the purpose of antideception, Panice et al. [6] proposed an anti-GPS spoofing detection mechanism based on state distribution combined with inertial navigation system and detected GPS spoofing attack by analyzing the error distribution between GPS and inertial navigation by using support vector machine. Magiera and Katulski [26] proposed a GPS deception detection and mitigation technology based on phase delay and spatial processing, which uses multiple receiving antennas to estimate the signal phase delay and spatial filter the signal to protect the GPS receiver from deception attack. Jansen et al. [27] proposed a group crowdsourcing method to detect the GPS spoofing attack of UAV. The method uses multiple aircraft to report the positioning difference and detects the GPS spoofing attack of UAV positioning through wireless air traffic control system. Kwon

and Shim [28] proposed a method to detect GPS spoofing attack by comparing the acceleration difference between GPS receiver and accelerometer

In the scenario of UAV flying along the designated route, such as power inspection and logistics distribution, the existing schemes still have the following problems:

(1) The method based on the physical layer detection of GPS signal can only detect simple GPS spoofing. When the attacker uses multidirectional GPS deception devices to transmit false GPS signals or dynamically adjust the frequency and power of GPS signals at the same time, the deception attack cannot be detected only by the physical layer characteristics of GPS signals. Therefore, this method cannot solve the problem of UAV trajectory deviation caused by the abovementioned GPS deception interference in power inspection

(2) The verification method based on cryptography cannot solve the replay attack of signal, and the encryption of signal is not suitable for civil GPS signal

(3) Using other equipment-aided positioning detection methods can improve the anti-spoofing ability of GPS receiver to a certain extent, but it will increase the cost of equipment positioning and the load of UAV in power inspection

Moreover, the focus of these schemes is mainly on the technology of detecting attack. A UAV is attacked in the process of moving towards a specific destination. The best it can do is to identify the attack and stop using the changed GPS signal. There is no other attack mitigation or defense mechanism to ensure the UAV to fly to the designated destination safely.

3. LR anti-spoofing Model

In LR (linear regression) anti-spoofing model proposed, UAV trajectory prediction is an important part, and LR is the final selected trajectory prediction method.

3.1. Linear Regression Analysis. Regression analysis is a statistical method that deals with the dependence between variables. It is one of the most widely used methods in mathematical statistics. Least squares regression analysis is the most typical linear regression algorithm [12, 29]. Regression analysis is based on the observation data to establish a quantitative relationship between two or more variables to analyze the inherent laws of the data. According to the number of independent variables, it can be divided into univariate regression analysis and multiple regression analysis; according to the relationship between independent variables and dependent variables, it can be divided into linear regression analysis and nonlinear regression analysis. Regression analysis is a predictive modeling technology, which is often used in predictive analysis. For example, the equipment frequency measurement method based on regression analysis is more accurate than other methods, and it is easier to realize; using regression analysis method to analyze the main factors affecting road traffic accidents can effectively prevent traffic accidents and improve road traffic efficiency.

In this paper, the univariate linear regression analysis method is used to establish a UAV positioning interval with the change of time stamp to predict the UAV trajectory in the mission. The method of univariate linear regression analysis is as follows.

According to the characteristics of the research object, the appropriate dependent variable and independent variable are selected. If the sample data shows that the two are in line with the linear relationship, then the univariate linear regression model is established:

$$y = a + bx + \varepsilon, \tag{1}$$

where y is the dependent variable, a is the constant term, b is the regression coefficient, x is the independent variable, and ε is the random error term, which reflects the influence of random factors on y except the linear relationship between x and y.

Assuming that the random error term ε in the regression model is a random variable with an expected value of 0 ($E(\varepsilon) = 0$) and it obeys normal distribution, then for a given x value, the expected value of y is

$$E(y) = a + bx. \tag{2}$$

The population regression parameters a and b are unknown and need to be estimated with sample data. For a selected sample, the regression parameters a and b in the model are replaced by sample statistics $\hat{a}$ and $\hat{b}$, and the estimated regression equation in linear regression is obtained, the sample regression equation

$$\hat{y} = \hat{a} + \hat{b}x \tag{3}$$

where $\hat{y}$ is the estimation of the mean value of dependent b variable y, $\hat{a}$ is the constant term of sample regression b equation, and $\hat{b}$ is the sample regression coefficient. For a dataset with sample size N, the values of $\hat{a}$ and $\hat{b}$ estimated by the least square method are

$$\hat{a} = \bar{y} - \hat{b}\bar{x}, \tag{4}$$

$$\hat{b} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^{N}(x_i - \bar{x})^2}, \tag{5}$$

where $\bar{x}$ and $\bar{y}$ are the average values of sample data x_i and y_i, respectively. After $\hat{a}$ and $\hat{b}$ are obtained, the linear regression equation of univariate can be obtained.

3.2. LR anti-spoofing Model Parameter. In our prediction model, the physical meaning of the parameters is as follows: x is the deviation of time stamp, and y is the deviation of longitude/latitude. To keep synchronization, the period of

deviation calculation is set to the same value of the frequency at which UAV receives GPS signals. Moreover, the data used in the deviation calculation is taken from the UAV under the condition of stable flight. Finally, the mapping relationship between x and y is established, and then, two linear regression models for latitude and longitude prediction are formed, respectively.

3.3. Workflow of LR anti-spoofing Model. Based on the LR model proposed in this paper, the flight trajectory prediction value of UAV and the positioning value of GPS receiver of UAV are fused at the decision level, which can quickly detect the GPS spoofing of UAV. The workflow chart of LR anti-spoofing model proposed is shown in Figure 2.

We will carry out single-step deception detection and multistep deception detection in the model. The difference lies in the discrepancy between the predicted value of single step or multistep with the current GPS positioning data to determine the status of UAV being cheated by GPS. If the deviation of longitude and latitude is less than the corresponding security threshold, it is determined that no GPS spoofing is detected; if the difference of either longitude or latitude is greater than the corresponding E (security threshold), it is determined that the target UAV has been spoofed. The predicted positioning data is used as the current positioning information to guide the UAV to fly. More details of single- and multistep predictions are as follows.

(i) Single-step detection: for each time interval, we first input the correction value, time stamp, and current GPS time stamp of the previous time to the linear regression trajectory prediction model, which outputs the positioning information of the predicted current time

(ii) Multistep detection: for each time interval, we first input the correction value, time stamp, and current GPS time stamp of the last m times to the linear regression trajectory prediction model, which outputs the positioning information of the predicted current time

The reason why we introduce multistep detection is that the deception signal is set in a reasonable error range in order to improve its credibility. In particular, we set up a sliding window to store the correction data of m histories for multistep prediction. For each multistep prediction, the corrected data at the previous m times is compared with the predicted data to detect deception. After that, this data is eliminated and the data in the window is pushed forward one step. Finally, the correction data of this time is saved in the $m-1$ positioning. The physical meanings of parameters in Figure 2 are shown in Table 1.

3.4. E (Noise Threshold) Setting. Given a group of UAV's continuous historical trajectory of normal fixed-point cruise, $T = \{(t_1, \mathrm{lat}_1, \mathrm{lon}_1), \cdots, (t_i, \mathrm{lat}_i, \mathrm{lon}_i)\}$, $i = 1, 2, \cdots, N$. Each track point is represented by a tuple, which contains three elements: time stamp, latitude, and longitude. Then, we can extract the deviation of longitude and latitude in the range of two adjacent time stamps:

$$\begin{aligned} \delta_{\mathrm{lat}} &= \mathrm{lat}_i - \mathrm{lat}_{i-1}, \\ \delta_{\mathrm{lon}} &= \mathrm{lon}_i - \mathrm{lon}_{i-1}. \end{aligned} \tag{6}$$

The 1.5 times of the maximum value of δ_{lon} is taken as the deviation threshold E of longitude, and the latitude takes the same setting. This setting is due to the consideration of physical environment interference in actual flight.

4. Attack Defense Game

For approaching the real scene as much as possible, we take quadrotor UAV as the research object and design an attack defense game based on Stackelberg leader-follower game theory [14, 30, 31] between the simulated GPS dynamic deception signal generator and the UAV with our LR anti-spoofing model.

4.1. Stackelberg Leader-Follower Game. The concept of leader-follower game was first proposed by Heinrich von Stackelberg, a German economist, in 1934. In the Stackelberg leader-follower game, after the leader makes the decision, the follower makes the optimal response to the leader's decision, and finally, the leader makes the most favorable decision according to the follower's decision. Principal subordinate game belongs to the category of asymmetric game, the positioning of participants in the game is unequal, and the strategy choice of followers depends on the strategy choice of leaders. This idea is consistent with our LR defense model and GPS dynamic deception signal generator positioning in UAV mission.

4.2. Stackelberg Game Scenario. In the attack defense game, UAV with our LR anti-spoofing model is the leader, named LR defender, and the simulated GPS dynamic deception signal generator is the follower, named GPS spoofer. In the planning game, each player will choose a strategy and take actions to control the positioning of UAV in each time step. In this way, both players can observe the initial positioning of the drones and their subsequent positions to the current time step. In addition, the game is based on the assumption of complete information, that is, both players have the complete information of their opponents. Our work includes three game rounds, seven steps.

(1) LR defender: receive a two-point fixed voyage mission

(2) GPS spoofer: according to the current positioning and the expected deception positioning of UAV, a deception trajectory (a group of GPS trajectory data) is calculated, and a deception signal is sent every 200 ms

(3) LR defender: the deviation between the current predicted trajectory point and GPS real-time positioning data is calculated every 200 ms. If the deviation is greater than the safety threshold of the prediction

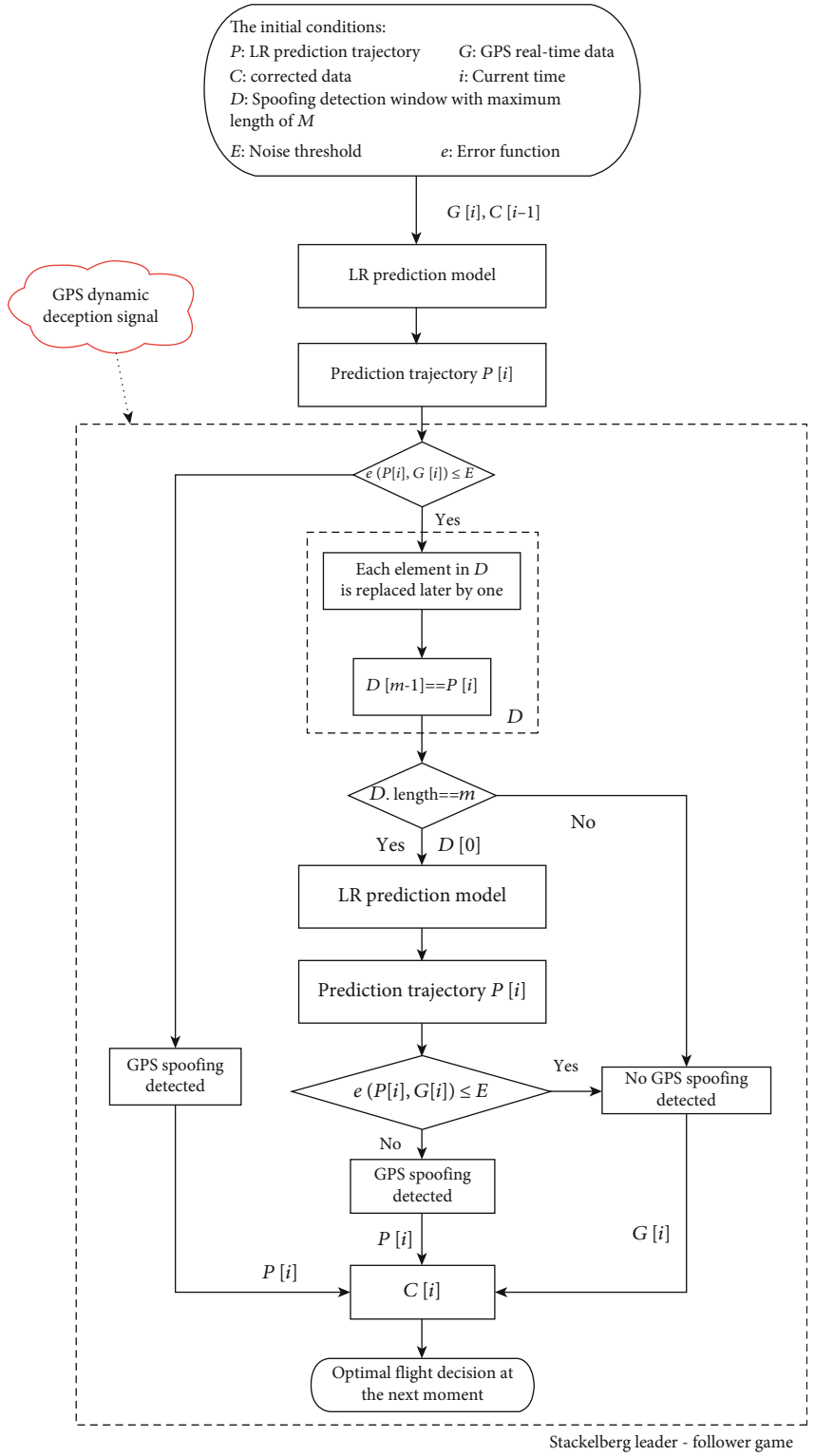

Figure 2: Workflow chart of LR anti-spoofing model.

module, the GPS real-time data will be removed at the next time, and the LR predicted trajectory points will be used to guide the UAV to complete the flight mission; if the deviation is less than the safety threshold, the GPS real-time data will continue to be received for trajectory positioning

(4) GPS spoofer: if the flight trajectory of UAV is not in accordance with the expected deception trajectory, the trajectory point information of GPS deception trajectory is adjusted until the data deviation between each two trajectory points is less than the safety threshold of UAV prediction module

Table 1: Physical meaning of parameters in workflow chart of LR anti-spoofing model.

Parameters	Physical meaning
P: LR predicts trajectory points	The continuous mission track points of UAV predicted by LR prediction model through historical track.
G: GPS real-time data	At present, the UAV airborne sensors receive the real signal from the mission environment.
C: corrected data	The value ($P[i]/G[i]$) transmitted to the UAV navigation system is selected according to the judgment of whether the current UAV mission environment is safe (whether there is GPS deception signal).
E: noise threshold	From the analysis of flight experience, the reasonable path error of UAV in a safe and normal mission environment due to its own attitude control and physical environment is obtained.
D: spoofing detection window with maximum length of M	The model provides two detection means. The window is set for further detection of deception, recording the trajectory values of the UAV at five adjacent moments (M is set to 5 in the invention).
e: error function	The variables involved in the calculation are LR predicted value and GPS real-time data at the current time. Compared with E, the results are used to judge whether the current UAV mission environment is safe or not.

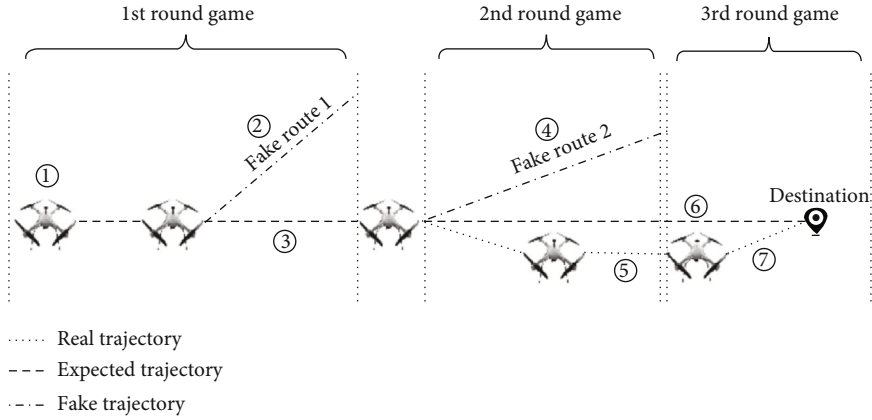

Figure 3: The expected motion state of UAV in Stackelberg game.

(5) LR defender: the deviation between the current predicted track point and GPS real-time positioning data is calculated at each time. If the deviation at five consecutive times is less than the safety threshold of the prediction module, the deviation between the track point data at the fifth time predicted by LR and the current GPS real-time data is calculated. If it is still less than the safety threshold, the flight will continue according to the GPS real-time data. If it is greater than the safety threshold, the GPS spoofer will be removed at the next time. The real-time data is used to guide the UAV flight with LR predicted trajectory points

(6) GPS spoofer: observe the flight trajectory of UAV at several times, and give up the deception if it does not follow the expected deception trajectory

(7) LR defender: after receiving the predicted trajectory values, we synchronously calculate the longitude/latitude variation, Δ, of GPS signals received at adjacent times (e.g., n time and $n+1$ time). Because the generation of deception signal is based on constant deviation, the longitude/latitude variation of adjacent time is also fixed. When

$$\Delta_{(n+1)-n} \neq \Delta_{n-(n-1)}, \tag{7}$$

it can be determined that there is no GPS spoofing at present. Then, the UAV stops using the predicted value and starts to use the GPS signal currently received to locate and continue to complete the task.

In this game, the expected motion state of UAV is shown in Figure 3.

5. Simulation and Evaluation

Our aim is to evaluate the performances of LR anti-spoofing model. To be specific, the experiment is mainly carried out from the following aspects.

5.1. Experiment Setting. The experiment is based on the UAV Simulation Platform consisted of jMAVSim and QGroundControl. jMAVSim is a simple and lightweight multirotor simulator. It connects directly to the hardware-in-the-loop (HITL, via serial) or software-in-the-loop (SITL, via UDP) instance of the autopilot. QGroundControl is simulation ground control station. It provides full flight control and mission planning for any MAVLink-enabled UAV and collects flight logs. The flight log contains the data collected by various sensors and some system output data during the flight. We extract GPS-related data (time stamp, longitude, and latitude) from flight log to consist the training dataset. In the experiments, the training dataset of LR anti-spoofing model is generated by a preset fixed-point cruise flight mission in the UAV simulation environment. The relevant parameters of the dataset are as follows in Table 2.

5.2. Deception Scenario Validation. Before verifying our proposed LR anti-spoofing model, we first verify the effectiveness of our deception scenario.

5.2.1. Deception Scenario Construction. In order to better simulate the real situation, we build a simulation deception scene which depends on a simulated GPS dynamic deception signal generator designed by us. We expect to realize the decoy capture of UAV in this scene. In this scenario, the deception means is to dynamically generate a group of trajectory point signals to deceive the UAV by observing the track changes of the target aircraft after entering the stable flight state. The deception trajectory setting is based on the noise range of UAV GPS itself. The specific implementation details are as follows.

In the beginning, we can calculate the noise threshold of GPS data of UAV in normal flight through the intermediate interpolation method. Based on this background, a group of deceptive trajectories is generated randomly. In order to capture the target more quickly, the GPS change value of two adjacent moments is greater than the upper limit of noise threshold. When the UAV does not fly according to the expected deception trajectory, it is speculated that the UAV may have certain detection and filtering ability for the signals with large changes. Based on the purpose of acquisition, a new deception trajectory is generated according to the error threshold so that the GPS change value of the two adjacent moments is within the noise threshold range, and the credibility of the deception signal is improved. The simplest way is to add a fixed increment to the GPS deception data at the next time.

5.2.2. Validity Verification. Figure 4 shows the trajectory diagram of UAV completing a given flight mission in the environment without any interference and deception is based on the ground coordinate system, and the abscissa and ordinate represent the latitude information and longitude information, respectively. Figure 5 is the visual expression of mission route in QGC. As you can see, H represents the home point of the UAV, and 1 represents the destination.

Table 2: Collected dataset parameters.

Parameters	Value
Signal frequency	20 Hz
Total number of tracks	40000
Total length of mission	1243.31 m
Threshold-latitude	$63 * 10e\text{-}6$
Threshold-longitude	$133.8 * 10e\text{-}6$

Figure 6 shows the experimental results of the target that is affected by the GPS deception signal we send in the UAV mission environment.

At the beginning, GPS spoofer did not send deception signals. From the ground control station, we can observe that the target aircraft was flying normally along the established route during this period. Therefore, we can also see from the chart that the trend of the blue line is a smooth and regular straight line. After flying for a period of time, we started the GPS simulation deception signal generator designed by us, GPS spoofer, to send GPS deception signal to the target's mission environment. Point A in Figure 6 represents the beginning time of deception. According to the principle of GPS deception signal mentioned in Section 1, the route of target plane after being spoofed by GPS spoofer is determined by deception signal and target point. We can see from Figure 6 that the trend of the blue line changes with the change of the red line after point A, which indicates that the target has indeed accepted the GPS deception signal, changed its belief in its positioning, and thus changed its movement state.

It is a fact that the target aircraft periodically returns to adjust the trajectory: in the fixed-point cruise mission, the UAV does not always take the current positioning and destination positioning as the optimal trajectory planning, but sets a local prediction point within a certain distance based on the given route so that the UAV will fly to the destination first after a certain distance from the route. The next point is predicted near this prediction point and the flight path is planned. Finally, Figure 6 shows that the target plane flies almost perpendicularly to the established route. What is worse, with the accumulation of time there is no tendency that the target UAV fly to the mission destination, and it is in a state of complete and serious yaw. This phenomenon can also be intuitively seen on the ground control station of the simulation platform, as shown in Figure 7. This proves that our GPS simulation deception signal generator and deception scene can effectively realize the deception acquisition of UAV.

5.3. Validation of LR anti-spoofing Model. In the constructed simulated deception scenario, we put on a Stackelberg game to verify the effectiveness of LR anti-spoofing model. According to Section 4, the GPS spoofer dynamically adjusts the deception signal according to the flight state of the target plane and plays a game with the UAV with LR anti-spoofing model.

Figure 8 shows the experimental results of our LR anti-spoofing model deployed on UAV.

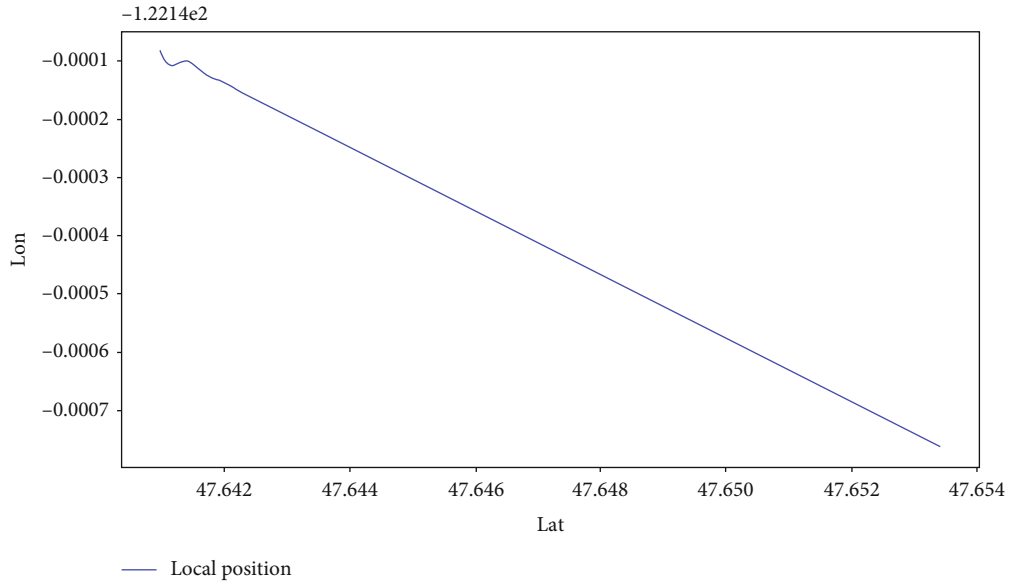

Figure 4: The trajectory diagram of a given flight mission is based on the ground coordinate system, and the abscissa and ordinate represent the latitude information and longitude information, respectively.

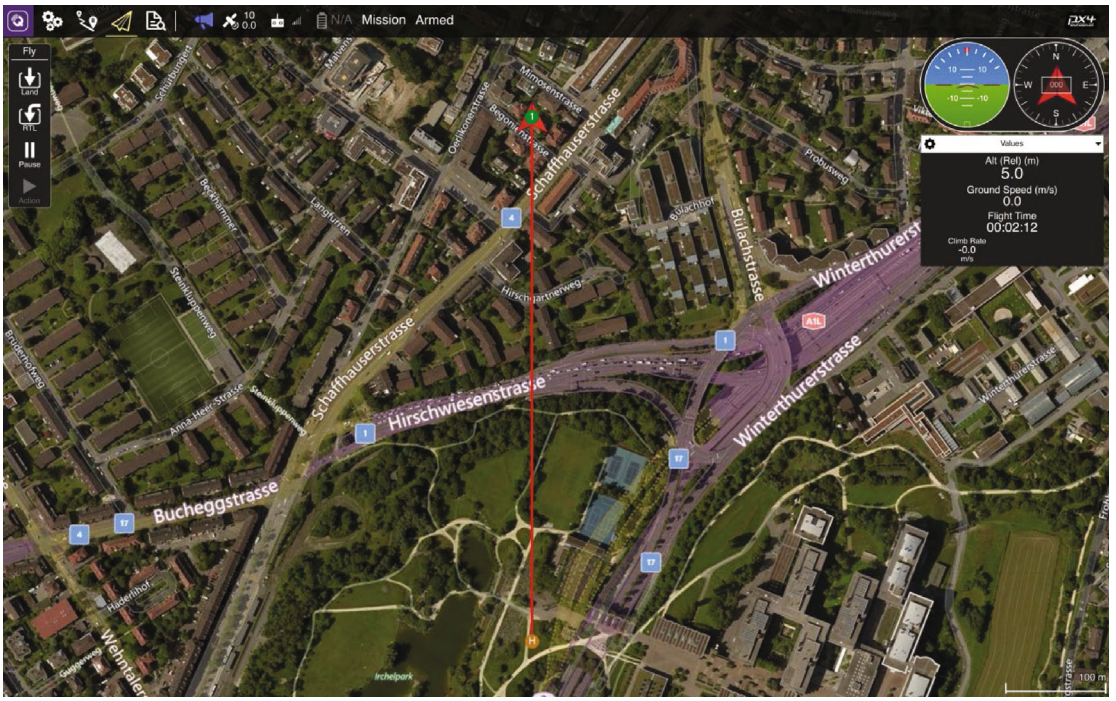

Figure 5: The visual expression of mission route in QGC.

We can see from Figure 8 the following:

(1) LR defender: the UAV enters a stable flight state after taking off for a period of time

(2) GPS spoofer: after observing the UAV in a stable flight state, GPS spoofer starts to send deception signals in the mission environment. In order to capture the target UAV as soon as possible, the deception signal is set outside the current positioning of the target which is greater than E in the AB segment

(3) LR defender: due to the deployment of our LR anti-spoofing model, the target plane will directly detect the step source and abandon it and follow the prediction module in LR anti-spoofing model to continue to move. As can be seen from the AB segment, the target UAV is in normal flight state

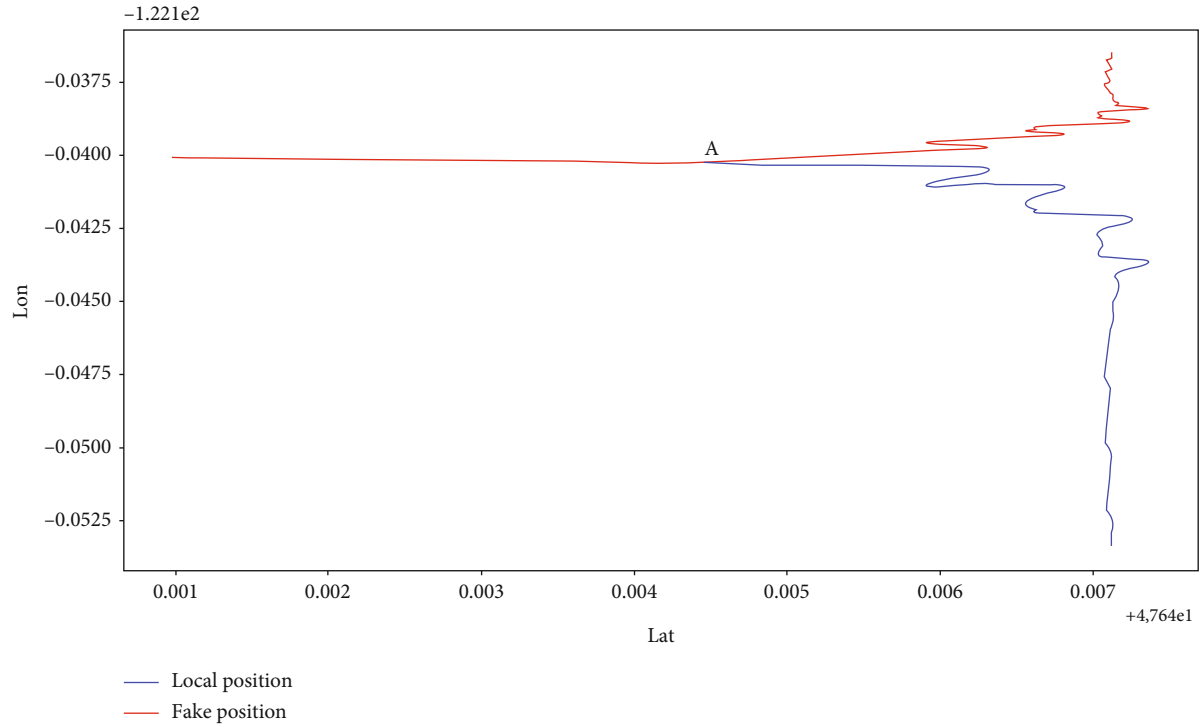

Figure 6: The red line indicates the dynamic change track of GPS deception signal in the process of trapping. The blue line indicates the real positioning of the target aircraft during the mission, that is, the real flight path.

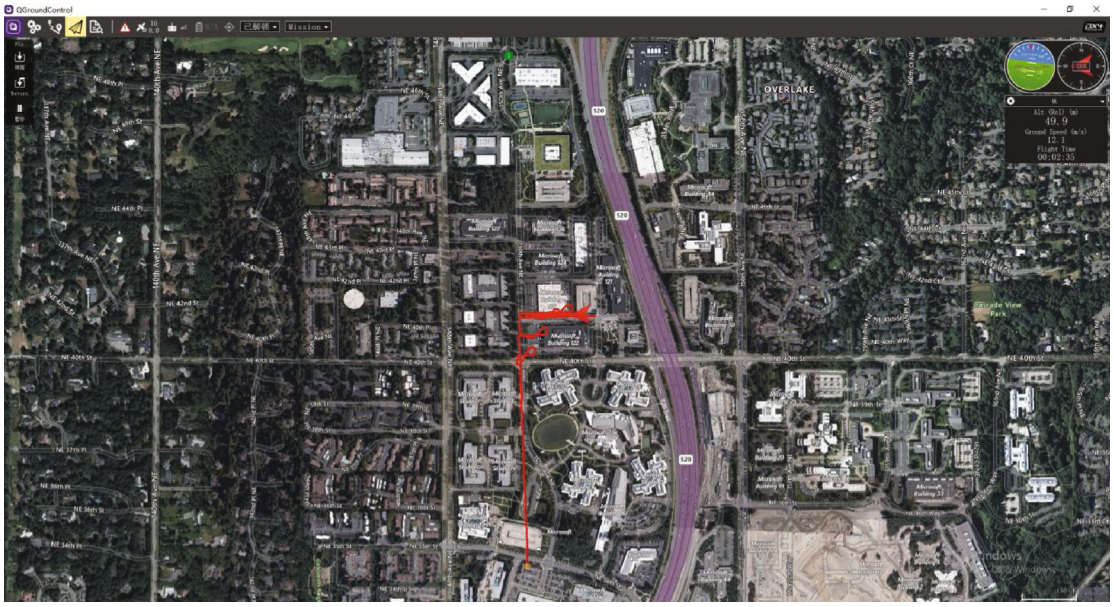

Figure 7: The complete yaw trajectory of UAV can be seen directly in QGC.

(4) GPS spoofer: after observing that the target UAV is not affected by the deception signal, GPS spoofer adjusts the deception signal to make it change within the range of E. At this time, we can see that in the BC segment, the target UAV has received the deception signal and has replanned its flight route. The spoofing is successful and effective in this period of time

(5) LR defender: it is worth mentioning that, in order to better ensure the safe flight of UAV, our detection mechanism, LR anti-spoofing model, is a two-step reinforcement type. At moment C, the target UAV detects the adjusted deception signal through the multistep detection mechanism in LR anti-spoofing model, starts to output the predicted value in time

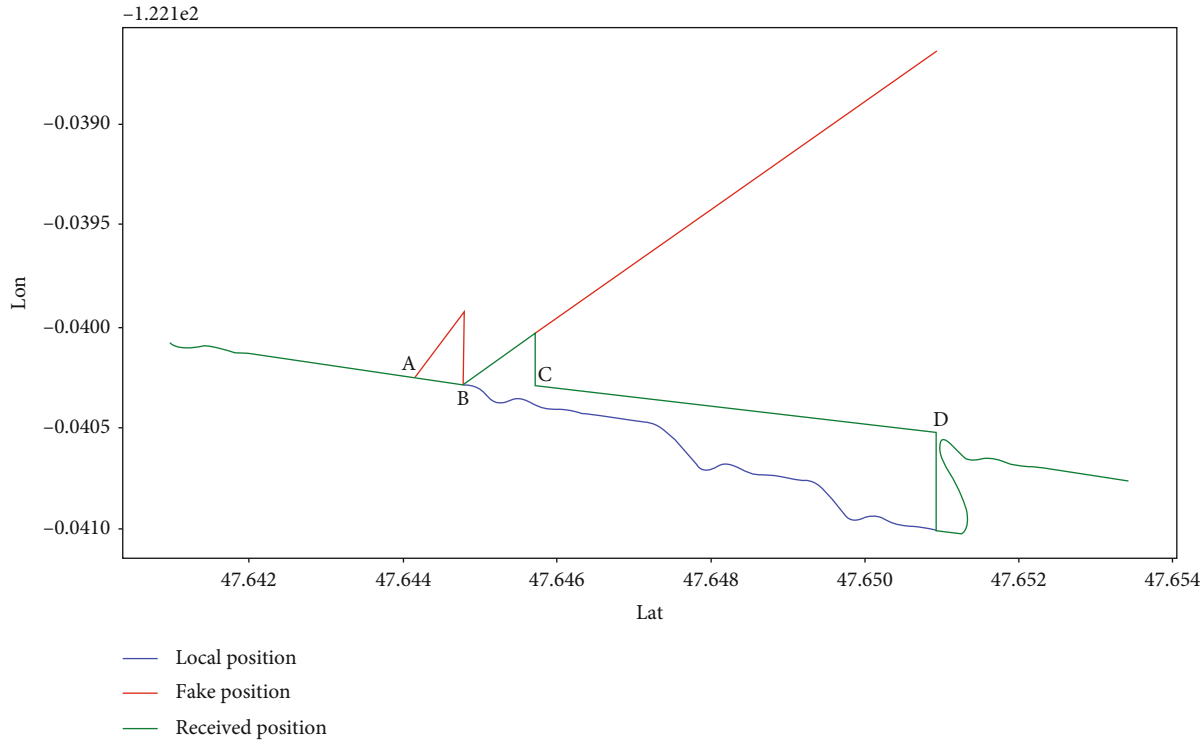

Figure 8: The red line indicates the dynamic change track of GPS deception signal in the process of trapping. The green line represents where the UAV thinks it is. The blue line indicates the real positioning of the target aircraft during the mission, that is, the real flight path.

Figure 9: Trajectory correction of UAV deployment LR anti-spoofing model (1).

window D to the UAV, and makes a self-adjustment according to the fact mentioned above. In the CD segment, the target receives the predicted trajectory value, which is equivalent to a self-deception for the UAV that has deviated from the course. From the first half of CD, we can see that the motion state of the target UAV is consistent with the deception principle mentioned in Section 1. The drift of the second half is due to the small cumulative deviation between the predicted route and the established route; the deviation has been verified by engineering and is within a reasonable range

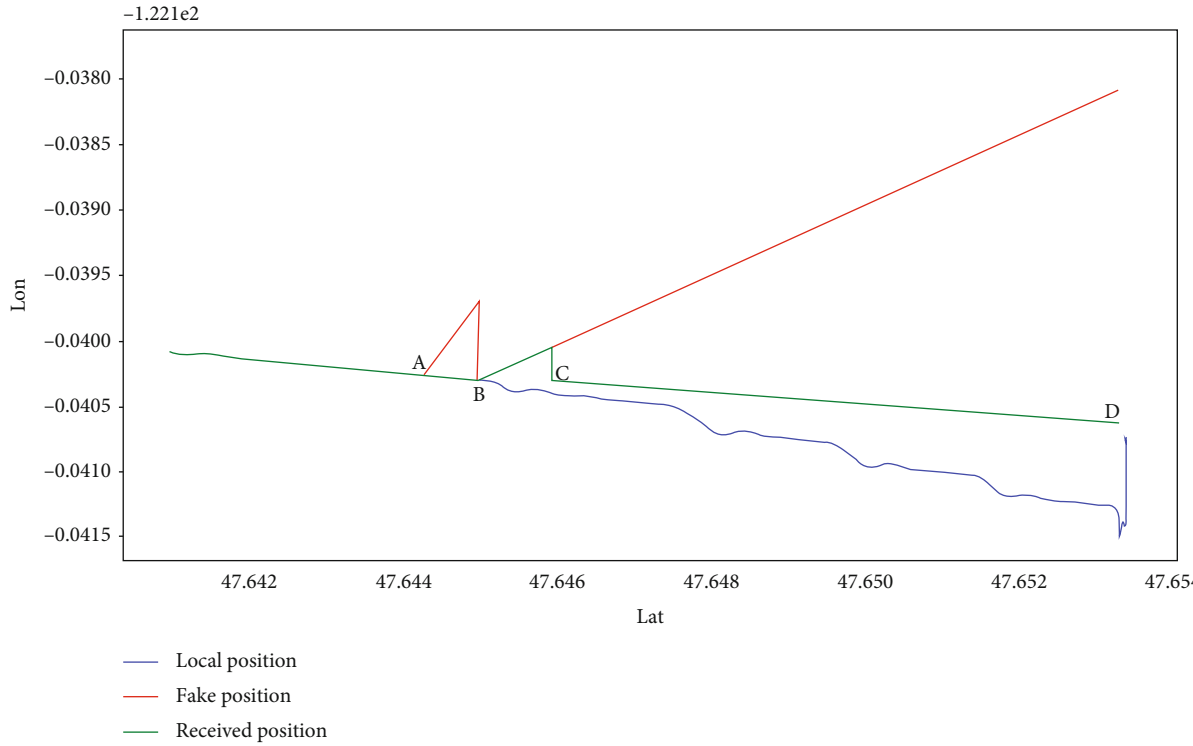

Figure 10: The red line indicates the dynamic change track of GPS deception signal in the process of trapping. The green line represents where the UAV thinks it is. The blue line indicates the real positioning of the target aircraft during the mission, that is, the real flight path.

Figure 11: Trajectory correction of UAV deployment LR anti-spoofing model (2).

(6) GPS spoofer: gave up spoofing at D moment

(7) LR defender: after moment D, target UAV to receive the real GPS signal when it detects that there is no deception interference in the mission environment and then finds that it has a certain degree of yaw; it will automatically adjust to the route and then continue to complete the task along the established route

Figure 9 is a QGC visual chart of the UAV that successfully resisted deception, completed the flight mission, and arrived at the established destination safely. Due to the scale

problem, the performance of flight status in the chart is not obvious, but some track fluctuations can still be seen.

In order to further verify the effect of our LR anti-spoofing model, we also designed an experiment while the GPS spoofer did not give up cheating in the whole process. The result is shown in Figure 10.

From Figure 10, we can see that under the guidance of our predicted value, although the UAV has a fixed deviation from the established routes, resulting in the UAV having a small stage yaw, the target UAV has still finally completed the flight mission. When the UAV receives the predicted value and thinks that it will arrive at the destination, the deviation from the real destination is only 72.35 m, which is within the visual range of the real destination. The total length of the mission route is 1243.31 m. This experiment also proves that the LR anti-spoofing model proposed is effective.

It can also be seen from QGC (Figure 11) that there is no uncontrollable yaw phenomenon in the whole course of UAV.

5.4. Comparison of Different Methods' Performance for UAV Trajectory Prediction Performance. The trajectory prediction module in our anti-spoofing model plays the role of navigation after the target UAV is affected by deception signal, so we expect the prediction accuracy to be as high as possible. On the same dataset, in addition to linear regression, we also try to use neural network, LSTM, in the selection of trajectory prediction module [32]. The result is inferior to the current linear regression.

5.4.1. Description and Processing of Experimental Data. The relevant parameters of the dataset are as follows in Table 3.

5.4.2. Evaluation Metrics. In order to determine the performance of the LSTM-KF defense model, the root mean square error is used to evaluate the fitting performance of the model.

Root mean square error (RMSE) is the relationship between the data sequence and the real value, which is the square root of the average of the sum of squares of the distances that each data deviates from its true value.

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=2}^{n}\left(X_{\mathrm{obs},i} - X_{\mathrm{model},i}\right)^2}. \tag{8}$$

5.4.3. Trajectory Prediction of UAV Based on LSTM. The LSTM [33, 34] model has strong ability to predict time series data, which is the main reason why we choose it for trajectory prediction [35]. The LSTM model is trained. The historical trajectory characteristic data of UAV is taken as input, and the future UAV trajectory characteristic data is taken as the corresponding label. By training LSTM recurrent neural network, the mapping relationship between UAV historical flight trajectory and UAV future flight trajectory is established to realize the prediction of UAV future flight trajectory.

Let $x(t)$ be the triple data of UAV at each time, where t represents the time of UAV flight, and the information represented by triple data is $[\mathrm{lon}_t, \mathrm{lat}_t, v_t]$, where lon, lat, and v are longitude, dimension, and velocity of UAV at time t, respectively. Then, the trajectory characteristic $x(t)$ of UAV at time t can be expressed as

$$x(t) = \{\mathrm{lon}_t, \mathrm{lat}_t, v_t\}. \tag{9}$$

Table 3: Collected dataset parameters.

Parameters	Value
Signal frequency	5 Hz
Pseudocode type	C/A
Total number of tracks	30000
Training set : test set	4 : 1

After training, the flight trajectory of UAV can be predicted by using the trained LSTM model. The UAV flight trajectory data $[x_{t-n+1}, \cdots, x_t]$ of n consecutive moments are taken as the input data of LSTM model, and the prediction n steps backward, that is, the UAV trajectory data $[x_{t+1}, \cdots, x_{t+n}]$ at the future n moments is taken as the output, where n is the step size of input layer in the LSTM model. Therefore, the expression of UAV flight trajectory prediction model is

$$\{x_{t+1}, \cdots, x_{t+n}\} = f(\{x_{t-n+1}, \cdots, x_t\}). \tag{10}$$

For LSTM, the main parameters that affect its performance are the input step size and the number of neuron nodes. Through experiments, we choose the optimal parameters for LSTM.

From Table 4, we can see that when the number of neurons is 8, the prediction accuracy is relatively low. With the increase of the number of neurons, the prediction error decreases significantly. When the number of neurons is 16, the overall prediction error is the smallest, showing the best prediction accuracy, so we set the number of neurons as 16. From Table 5, we can clearly see from the results that with the increase of input step size from 5 to 10, the prediction error of the model gradually decreases. When the input step size is 12, the prediction error of the model increases greatly, which shows poor prediction performance. This may be because the input step size is too large, which leads to the overfitting phenomenon and the degradation of generalization performance. Therefore, we set the input step size of the LSTM prediction model to 10.

5.5. Comparison and Evaluation. It has been mentioned many times in this paper that trajectory prediction module is an important part of LR anti-spoofing model. Figure 12 mainly shows the performance of LR and LSTM in trajectory prediction, respectively, blue represents the established waypoint, and green and red represent the predicted waypoint of LR and LSTM separately. It is obvious in this figure that the fitting ability of LR-based prediction model is better than that of LSTM-based prediction model, taking the given route as the criterion. This is because, for the trajectory prediction problem of UAV two-point cruise mission, there is a linear relationship between the longitude and latitude change and the time change of UAV positioning. The target value

Table 4: Comparison of RMSE corresponding to neuron node.

Step_in	Step_out	Neurons	$e * 10^{-3}$	e_lat $* 10^{-5}$	e_lon $* 10^{-5}$	vel $* 10^{-3}$
10	5	8	68.114	5.600	25.750	5.943
10	5	16	1.923	0.035	0.160	0.755
10	5	32	5.135	0.449	2.060	0.321
10	5	48	4.555	0.368	1.696	0.426
10	5	64	9.472	0.847	3.890	0.499

e is the RMSE of all predicted data and real data, e_lat is the RMSE of latitude, e_lon is the RMSE of longitude, and vel is the RMSE of speed.

Table 5: Comparison of RMSE corresponding to input timing steps.

Step_in	Step_out	Neurons	$e * 10^{-3}$	e_lat $* 10^{-5}$	e_lon $* 10^{-5}$	vel $* 10^{-3}$
5	5	16	2.636	0.076	0.360	0.896
8	5	16	2.063	0.076	0.360	0.594
10	5	16	1.923	0.035	0.160	0.755
12	5	16	61.393	5.092	23.410	5.142

e is the RMSE of all predicted data and real data, e_lat is the RMSE of latitude, e_lon is the RMSE of longitude, and vel is the RMSE of speed.

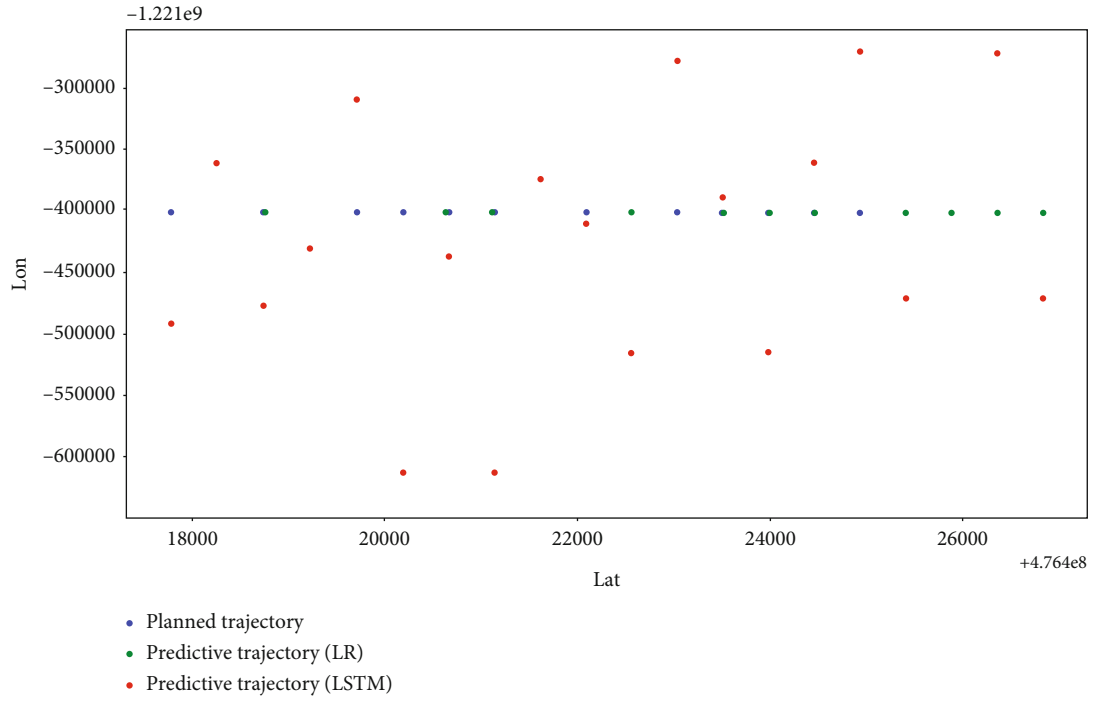

Figure 12: Performance comparison of trajectory prediction based on LSTM and LR in secure mission environment.

expectation of the LR model is a linear combination of input variables, and the model is simple and easy to model, so it is very suitable to solve this problem. Thus, the LSTM neural network is suitable for solving nonlinear problems; it has a big disadvantage in solving linear problems which is its own uncertainty, for the same input will produce different output, so the single use of LSTM is not suitable for the problem we want to solve.

6. Conclusion

Spoofing is one of the most important threats to GPS receivers. This paper discusses the detection model of UAV anti-GPS spoofing and proposes the LR anti-spoofing model. The flight trajectory prediction model of UAV is obtained by fitting the flight log of UAV with LR model, and the prediction accuracy is relatively high among all the methods. The

model not only realizes the safety detection of UAV flight status in the process of mission but also uses the decision fusion of sensor information to accurately detect the deception signal, so as to achieve the purpose of anti-spoofing interference. At the same time, when the UAV is cheated, it can also achieve deception mitigation, so as to ensure the smooth completion of the flight mission. Compared with the traditional anti-spoofing detection method or that based on neural network, this method not only has the characteristics of high accuracy and no need to increase the hardware cost of auxiliary equipment but also has fast linear regression modeling speed and does not require high computing ability of small computing board carried by UAV. In short, the LR anti-spoofing model can effectively achieve the effect of anti-GPS spoofing in the scene of UAV flying along the specified route.

Last but not least, although the LR anti-spoofing model successfully resists GPS spoofing and ensures the maximum completion of UAV tasks, strictly speaking, it is only a spoofing mitigation method. In the future work, we will further optimize our method from the perspective of UAV sensor integrated navigation and UAV attitude control, hoping to achieve the solution of GPS spoofing.

Data Availability

The raw/processed data required to reproduce these findings cannot be shared at this time as the data also forms part of an ongoing study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is supported by the National Natural Science Foundation of China (Grant No. 61771153, No. 61831007, and No. 61971154).

References

[1] J. I. Maza, F. Caballero, J. Capitán, J. R. M. de Dios, and A. Ollero, "Experimental results in multi-uav coordination for disaster management and civil security applications," *Journal of Intelligent & Robotic Systems*, vol. 61, no. 1-4, pp. 563–585, 2011.

[2] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: performance and tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949–3963, 2016.

[3] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (uavs) for energy-efficient Internet of things communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574–7589, 2017.

[4] L. Kai, N. Ahmed, S. S. Kanhere, and S. Jha, "Reliable communications in aerial sensor networks by using a hybrid antenna," in *IEEE Conference on Local Computer Networks*, Clearwater Beach, FL, USA, 2012.

[5] D. P. Shepard, J. Bhatti, T. E. Humphreys, and A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, Tennessee,USA, 2012.

[6] G. Panice, S. Luongo, G. Gigante et al., "A svmbased detection approach for GPS spoofing attacks to UAV," in *23rd International Conference on Automation and Computing, ICAC 2017*, pp. 1–11, Huddersfield, United Kingdom, September 2017.

[7] Y. Qiao, Y. Zhang, and X. Du, "A vision-based gpsspoofing detection method for small uavs," in *13th International Conference on Computational Intelligence and Security, CIS 2017*, pp. 312–316, Hong Kong, China, December 2017.

[8] W. U. Bin and L. I. U. Hanwen, "A behavior-based covert channel based on GPS deception for smart mobile devices," in *2019 IEEE International Conference on Communications, ICC 2019*, pp. 1–6, Shanghai, China, May 2019.

[9] B. Van den Bergh and S. Pollin, "Keeping uavs under control during GPS jamming," *IEEE Systems Journal*, vol. 13, no. 2, pp. 2010–2021, 2019.

[10] J. Noh, Y. Kwon, Y. Son et al., "Tractor beam," *ACM Transactions on Privacy and Security*, vol. 22, no. 2, pp. 1–26, 2019.

[11] F. A. Milaat and H. Liu, "Decentralized detection of GPS spoofing in vehicular ad hoc networks," *IEEE Communications Letters*, vol. 22, no. 6, pp. 1256–1259, 2018.

[12] L. Zhang, W. Hu, W. Qu, Y. Guo, and S. Li, "A formal approach to verify parameterized protocols in mobile cyber-physical systems," *Mobile Information Systems*, vol. 2017, Article ID 5731678, 10 pages, 2017.

[13] E. G. Manfredini and F. Dovis, "On the use of a feedback tracking architecture for satellite navigation spoofing detection," *Sensors*, vol. 16, no. 12, article 2051, 2016.

[14] A. R. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: a game-theoretic countermeasure for protecting uavs against GPS spoofing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2840–2854, 2020.

[15] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of uav: a survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95–101, 2020.

[16] W. M. Y. W. Bejuri, W. M. N. W. M. Saidin, M. M. B. Mohamad, M. Sapri, and K. S. Lim, "Ubiquitous positioning: integrated gps/wireless LAN positioning for wheelchair navigation system," in *Volume 7802 of Lecture Notes in Computer Science*, A. Selamat, N. T. Nguyen, and H. Haron, Eds., pp. 394–403, Springer, 2013.

[17] P. Moosbrugger, K. Y. Rozier, and J. Schumann, "R2U2: monitoring and diagnosis of security threats for unmanned aerial systems," *Formal Methods in System Design*, vol. 51, no. 1, pp. 31–61, 2017.

[18] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for gnss structural interference detection and mitigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1–12, 2016.

[19] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[20] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[21] X. Hu, J. Cheng, M. Zhou et al., "Emotion-aware cognitive system in multichannel cognitive radio ad hoc networks," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 180–187, 2018.

[22] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "SPREE: a spoofing resistant GPS receiver," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, MobiCom 2016*, pp. 348–360, New York City, NY, USA, October 2016.

[23] C. H. Kang, S. Y. Kim, and C. G. Park, "Adaptive complex-ekf-based doa estimation for gps spoofing detection," *IET Signal Processing*, vol. 12, no. 2, pp. 174–181, 2018.

[24] K. D. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil gps signal authentication," *Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[25] H. Rao, S. Wang, X. Hu et al., "Self-supervised gait encoding with locality-aware attention for person re-identification," in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI 2020*, pp. 898–905, Yokohama, Japan, 2020, http://ijcai.org.

[26] J. Magiera and R. Katulski, "Detection and mitigation of gps spoofing based on antenna array processing," *Journal of Applied Research and Technology*, vol. 13, no. 1, pp. 45–57, 2015.

[27] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, "Crowd-gps-sec: leveraging crowdsourcing to detect and localize gps spoofing attacks," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 1018–1031, San Francisco, CA, USA, 2018.

[28] K. C. Kwon and D. S. Shim, "Performance analysis of direct gps spoofing detection method with ahrs/accelerometer," *Sensors (Basel, Switzerland)*, vol. 20, no. 4, p. 954, 2020.

[29] Y. Tang, X. Zhang, X. Hu, S. Wang, and H. Wang, "Facial expression recognition using frequency neural network," *IEEE Transactions on Image Processing*, vol. 30, pp. 444–457, 2021.

[30] A. Sinha, P. Malo, A. Frantsev, and K. Deb, "Finding optimal strategies in a multi-period multi-leader-follower stackelberg game using an evolutionary algorithm," *Computers & Operations Research*, vol. 41, pp. 374–385, 2014.

[31] N. Groot, B. De Schutter, and H. Hellendoorn, "Optimal affine leader functions in reverse Stackelberg games," *Journal of Optimization Theory and Applications*, vol. 168, no. 1, pp. 348–374, 2016.

[32] L. Zhang, Q. WanXia, Y. Huo, G. Yang, and S. Li, "An sat-based method to multithreaded program verification for mobile crowdsourcing networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 3193974, 8 pages, 2018.

[33] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[34] H. Cheng, Z. Xie, L. Wu, Z. Yu, and R. Li, "Data prediction model in wireless sensor networks based on bidirectional LSTM," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[35] S. Xu, H. Rao, H. Peng, X. Jiang, and B. Hu, "Attention based multi-level co-occurrence graph convolutional lstm for 3d action recognition," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.