Journal of Cyber Security
DOI:10.32604/jcs.2021.019105
Article

Tech Science Press

Multi-UAV Cooperative GPS Spoofing Based on YOLO Nano

Yongjie Ding[1] and Zhangjie Fu[1,2,*]

[1]Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing, 210044, China

[2]College of Information Science and Technology, College of Cyber Security, Jinan University, Guangzhou, 510632, China

[*]Corresponding Author: Zhangjie Fu. Email: fzj@nuist.edu.cn

Received: 02 April 2021; Accepted: 06 April 2021

Abstract: In recent years, with the rapid development of the drone industry, drones have been widely used in many fields such as aerial photography, plant protection, performance, and monitoring. To effectively control the unauthorized flight of drones, using GPS spoofing attacks to interfere with the flight of drones is a relatively simple and highly feasible attack method. However, the current method uses ground equipment to carry out spoofing attacks. The attack range is limited and the flexibility is not high. Based on the existing methods, this paper proposes a multi-UAV coordinated GPS spoofing scheme based on YOLO Nano, which can launch effective attacks against target drones with autonomous movement: First, a single-attack drone based on YOLO Nano is proposed. The target tracking scheme achieves accurate tracking of the target direction on a single-attack drone; then, based on the single-UAV target tracking, a multi-attack drone coordinated target tracking scheme based on the weighted least squares method is proposed to realize the target drone Finally, a new calculation method for false GPS signals is proposed, which adaptively adjusts the flight trajectory of the attacking drone and the content of the false GPS signal according to the autonomous movement of the target drone.

Keywords: UAV safety; GPS spoofing; multi-UAV; target detection

1 Introduction

Unmanned aerial vehicle [1] stands for unmanned aircraft, which is an unmanned aerial vehicle controlled by radio remote control equipment and its control program. In recent years, with the gradual maturity of the global satellite positioning system, the lightweight of composite materials, and the integration of electronic modules, the UAV industry has entered a stage of leapfrog development. Aside from military drones that have long achieved outstanding military exploits in the military field, civilian drones have also played an extremely powerful role in many industries and professional fields, such as aerial photography, pesticide spraying, cargo transportation, emergency rescue disaster relief, and many other occasions. You can see the figure of the drone [2]. Also, the emergence and rapid development of civilian drone manufacturers have allowed ordinary people interested in drones to purchase and own their civilian drones, to experience the joy of manipulating drones and use drones to realize themselves. Corresponding needs.

However, fast-developing things will inevitably have certain hidden dangers while bringing innovation, and drones are no exception. The current UAV control methods are immature [3], and the laws and regulations related to UAVs have not reached a sound level. Everyone can operate UAVs simply by reading the operation manual. This kind of UAV “black flight” (operating the UAV to fly without professional training) will cause interference to the normal flight taking off and landing, and it may also cause out-of-control collision accidents [4]. Therefore, the control of drones has become an urgent task for relevant departments. Among the existing control methods, GPS spoofing interference is a method with higher feasibility and larger operating space [5].

UAVs can fly and hover freely in the air according to people's wishes and need to rely on the flight control system of the UAV, and one of the cores of the UAV flight control system is the GPS navigation module. The Global Positioning System (GPS) is a navigation and positioning timing system based on 24 artificial satellites developed by the US military. It can provide accurate geographic location information under all climatic conditions throughout the entire period [6]. In June 2011, the US Air Force successfully expanded the GPS satellite constellation, adjusted the positions of 6 satellites, and added 3 more satellites. This increases the number of working satellites to 27, expands the coverage of the GPS, and improves accuracy. As of January 09, 2021, there are a total of 31 operational satellites in the GPS constellation, excluding the standby satellites in orbit. Since the development of GPS, its signal can cover 98% of the world, and it has been applied to almost every aspect of our lives [7]. In today's society, the navigation and positioning functions provided by GPS are inseparable from the map positioning and route guidance of each of our smartphones, and the safe travel of each car, to the equipment navigation and weapon guidance in the military field.

Because the GPS signal transmitted by the satellite has to travel tens of thousands of meters, through the multi-layer atmosphere such as ionization and convection, it can be transmitted to the receiver after being interfered with by various uncertain factors. The GPS signal that the receiver can successfully receive is very weak [8]. Also, the signal composition of GPS signals in the civil frequency band is completely public, which allows us to interfere with GPS signals by artificial means, including suppressive interference and deceptive interference [9]. Suppressive interference uses high-power artificial signals to prevent the receiving device from successfully receiving satellite signals [10], while deceptive interference uses false signals similar to real GPS signals to deceive the receiving device, making it mistaken for the received location. The information and time information comes from the correct GPS satellites, thus affecting the equipment to make corresponding judgments [11]. As early as December 2011, a U.S.-produced RQ-170 "Sentinel" UAV was discovered and successfully captured by the Iranian side. According to Iranian engineers, they used GPS deception jamming technology. The GPS signal induces the UAV of the U.S. military to land at a designated location [12].

This article is based on the existing GPS deception jamming technology, according to the working characteristics of the UAV, A YOLO Nano-based multi-UAV coordinated GPS spoofing scheme is proposed. Based on the existing scheme, combined with the multi-machine coordinated target detection and positioning method based on YOLO Nano and the weighted least squares method, it can realize the unmanned movement of autonomously moving targets. The target point spoofing attack and the track spoofing attack of the machine Finally, in a real environment, relying on the multi-UAV cooperative attack platform to conduct no-fly zone deception and trajectory deception experiments on the target drones in two states, and successfully achieved the drive away and control of the target drone. The effectiveness of the program.

The main contributions of our research work can be summarized as follows:

(1) A multi-aircraft cooperative target detection and positioning method is proposed, which uses YOLO Nano and the weighted least square method to achieve high-precision positioning of the target UAV under multi-aircraft cooperation.

(2) Optimize the generation method of GPS spoofing signal and the calculation method of the trajectory of attacking drones, and propose a GPS spoofing scheme for drones in motion.

(3) A real UAV GPS spoofing attack experiment was carried out on the above scheme to verify the effectiveness of the scheme.

The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 introduces our proposed methods and framework in detail. In Section 4 we present our findings and discussion of results. Lastly, we conclude the paper and also give highlights of future work in Section 5.

2 Related Works

UAV GPS spoofing technology and detection technology are just like spears and shields. They constitute the opposite of UAV GPS security research. The continuous improvement of the two has promoted the rapid development of UAV GPS security research. This chapter will analyze the status quo of GPS spoofing research from two aspects: GPS spoofing technology and GPS spoofing detection technology.

With the gradual promotion and wide application of GPS technology, GPS spoofing technology is also constantly developing. Nowadays, GPS spoofing methods have become diverse. According to the different sources of false GPS signals, GPS spoofing can be divided into two categories: forward spoofing and generative spoofing [13].

2.1 Research Status of Forwarding GPS Spoofing Attacks

Forwarding spoofing refers to the use of GPS signal receiving equipment to record real GPS signals in specific locations (such as no-fly zones), and the use of GPS signal transmitting equipment to transmit the recorded GPS signals at a higher power during an attack. Such an attack The GPS signal content is consistent with the GPS signal content at the time of recording [14]. After receiving the attacking GPS signal, the target device will parse out the geographic location of the GPS signal recording location, thereby making a wrong judgment on its location. Such deception methods require that GPS signals of characteristic locations be recorded in advance, and cannot be temporarily adapted to actual needs.

In 2005, Yang et al. gave the relationship between the actual location and deception location based on GPS positioning principles [15]. In 2011, Zhang et al. pointed out that the timing error of the GPS receiver is far greater than its timing requirements, so GPS positioning deception can be completed without affecting GPS timing [16]. Then, Zhang et al. realized the mapping of the positioning area through the method of time delay control, analyzed the distribution and movement scheme of the integrated platform [17], and pointed out that the effective range of the attack under the coordination of multiple forwarding stations is much larger. Achieve attack area coverage [18]. In 2013, Yan et al. proposed a delay algorithm suitable for GPS forwarding spoofing and obtained the clock error conditions for the success of GPS forwarding spoofing [19]. In 2015, Yan et al. gave a four-station forwarding mapping model [20]. In 2016, Liang et al. pointed out the influence of receiver clock change on GPS forwarding spoofing and proposed a spoofing method to modify navigation messages, which implements a spoofing scheme that does not affect the clock error [21].

Forwarding spoofing is simpler in processing GPS signals and can record GPS signals according to different needs. For large-scale spoofing attacks, multi-site forwarding can also be conveniently carried out to achieve the best deception effect. At the same time, since forward spoofing does not involve the processing of GPS signals, it also has an attack effect on encrypted military GPS signals, which cannot be achieved by generative spoofing.

However, forwarding spoofing relies heavily on pre-recorded GPS signals and cannot be flexibly adjusted according to the scene and target of the attack. The scene adaptability is not high and the effect is limited.

2.2 Research Status of Generative GPS Spoofing Attacks

Different from the forward spoofing scheme, the signal used by generative spoofing is not from the recorded real GPS signal but is calculated based on the composition of the GPS signal. Generative deception can generate different false GPS signals according to different deception needs and has higher flexibility [22].

In 2002, Warner et al. used a simple GPS signal simulator to successfully deceive the GPS receiver of a freight truck, which means that the spoofing attack on civilian GPS receivers is easy to achieve [23]. In 2008, Humphreys et al. designed and manufactured the first true GPS generative deception jammer based on Software Defined Radio (SDR) [24]. By adjusting various parameters of the spoofing signal, the spoofing signal can be closer to the real GPS signal, and the spoofing attack can be made more concealed. In 2012, the team used GPS deception equipment to make an error in the unmanned helicopter's autopilot system and control the helicopter to continue to descend [25]. In 2012, Huang et al. pointed out that as long as the power of the spoofing signal is 4 dB higher than the real signal, the receiver can block the lock of the real signal for a long time and make it track the spoofing signal [26].

In 2014, Mark et al. proposed that at least 5 dB interference signal ratio is required to ensure that the receiver can capture GPS spoofing signals [27]. In the same year, Shepard et al. used the Monte Carlo method to prove how many carrier frequency differences will cause the receiver to lose lock [28]. In 2015, Hu et al. adjusted the deception power in real-time to achieve continuous and effective deception by limiting the noise floor to 3 dB and the maximum deceptive signal-to-noise ratio to 22 dB while realizing the capture loop pull of the receiver [29].

The difficulty of generative spoofing is to make the generated false GPS signal and the real GPS signal maintain a high similarity to avoid signal distortion detection [30]. In 2016, the spoofing signal synchronization scheme designed by Liang et al. realized the problem of signal synchronization [31], but the scheme was only tested in simulation [21]. In 2018, Ying et al. gave a calculation method for Doppler frequency offset and phase delay, which can be used to calculate the Doppler frequency offset and phase delay of the signal during the generation of GPS signals [32]. In 2018, Zeng et al. designed a search algorithm to determine the cheapness and route of the GPS receiver, while using a portable deception device to deceive it, so that 95% of the victims went to wrong location without a deception attack [33].

In summary, the domestic research on generative GPS spoofing is still at the stage of program design and simulation, lacking corresponding hardware support and experimental verification. The current Ducati solution relies on a relatively fixed launch platform, which has low flexibility and limited coverage, and it has a poor effect on UAV attacks.

3 Methodology

This chapter mainly introduces the multi-UAV coordinated GPS deception scheme based on YOLO Nano. The details are as follows: Study the multi-UAV coordinated target detection and positioning scheme based on YOLO Nano and weighted least squares method to accurately determine the real-time position of the target drone; Research on the calculation scheme of false GPS signals for the moving target UAV, and realize the deception and trajectory deception of the target UAV.

3.1 Multi-UAV Cooperative Target Detection and Location Scheme

The prerequisite for successfully launching a GPS spoofing attack on a moving UAV is to determine its real-time and accurate location. To achieve fast and accurate tracking of the target UAV, multi-aircraft coordinated target detection and positioning scheme is proposed, which specifically includes the YOLO Nano-based target detection method implemented on a single F-UAV (Follower UAV) and the coordinated target tracking implemented by multiple F-UAVs.

3.1.1 Single F-UAV Target Detection Method Based on YOLO Nano

This method uses the drone's airborne gimbal as the video stream acquisition device and uses the YOLO Nano-based target detection method to locate the target drone in the video stream.

YOLO Nano is an optimized version for edge and mobile devices. Compared with other YOLO networks, it has a smaller size and simpler calculations. YOLO Nano can achieve good results on the edge and mobile devices where power is limited and computing power is generally insufficient. For attacking drones, the use of the YOLO Nano algorithm can greatly increase the speed of target detection and positioning to increase the attack success rate and save energy to extend the attack time.

On the drone's onboard computer, the recognition speed of YOLO Nano can reach 45 fps. When the on-board camera uses the 30 fps mode, it can achieve real-time detection and quickly lock the target position.

Using the YOLO Nano model on a single F-UAV to perform target detection and positioning on the video stream, the relative position of the target drone in the video screen can be obtained in real-time. According to the coordinates of the center point of the target drone screen in the video screen, the angle between the target and the optical axis of the airborne camera can be calculated. Then, the pitch angle, rotation angle, UAV fuselage inclination, and other relevant data obtained by the onboard computer can be used to calculate the accurate azimuth of the target relative to the F-UAV.

3.1.2 Multi-F-UAV Cooperative Tracking Strategy Based on Weighted Least Squares

Since a single F-UAV can only obtain the angular relationship with the target UAV, it cannot accurately obtain the exact distance to the target UAV, so multiple F-UAVs are required to collaborate and share their position. On this basis, the position of target UAV is calculated cooperatively.

According to the principle of triangulation, the intersection of the straight lines determined by the two F-UAVs based on their position, and the target's azimuth is the position of the target UAV. However, due to the sensor error and the accumulation of errors caused by multiple angle calculations, there will be a certain deviation between the target UAV position calculated by the two F-UAVs and the actual position of the target UAV, and even the target cannot be adjusted. Location solution.

To improve the accuracy of positioning, multiple F-UAV co-locations are adopted, and the target orientation data collected by multiple F-UAVs are comprehensively considered. Each F-UAV can obtain the parameter equation set of the straight line where the target UAV is located based on obtaining its position and the azimuth of the target UAV:

$$\begin{cases} x = t + x_i \\ y = \tan(\delta_1)t + y_i, \text{when}\,\delta_1 \neq \pi / 2 \\ y = a + y_i (a \in R), \text{when}\,\delta_1 = \pi / 2 \\ z = \cot(\delta_2)t + z_i, \text{when}\,\delta_2 \neq 0 \\ \mathrm{z} = b + z_i (b \in R), \text{when}\,\delta_2 = 0 \end{cases} \tag{1}$$

Among them, (x_i, y_i, z_i) represents the location of the n-th F-UAV. With n F-UAVs, n linear equations of the target UAV as shown in expression (1) can be obtained. Without considering the error, these straight-line equations should intersect at one point, which is the location of the target drone.

According to these equations, multiple different target UAV azimuth information can be obtained. The estimated position information of the target UAV can be obtained by solving the intersection of this azimuth information. To obtain the optimally estimated coordinates of the target UAV, it is necessary to minimize the error in the solution of this equation system.

Considering that the errors of F-UAV acquisition of target angles under different angles are not the same, only using the least square method to calculate the target position will make the F-UAV data with larger errors affect the prediction of the final target position, so the weighting method is used Improve the optimization objective of the least square method.

Due to the three-dimensional structure of the target UAV, its center position will be offset from the center point of its geometric boundary under different viewing angles. The larger the viewing angle deviation, the greater the deviation of the center position. Therefore, this solution proposes to use the reciprocal of the square root of the sum of the angle between the target drone and the optical axis of the camera and the angle between the target drone and the central axis as the corresponding equations listed in F-UAV.

At the same time, considering the impact of the distance between the F-UAV and the target and the resolution of the F-UAV airborne camera on the target detection error, the target UAV area and the complete image area are used as one of the weighting factors, and the target The ratio of the number of pixels contained in the drone marquee to the number of pixels in the complete image obtained by the F-UAV gimbal camera is used as the weighting coefficient.

The weighting method can effectively suppress the influence caused by the accumulation of camera imaging, PTZ reading, F-UAV attitude reading, and other errors, and improve the accuracy of target positioning. The specific optimization function is shown in the following expression (2):

$$\arg\min \sum_{i=1}^{C_n^2} (1+(\tan(\delta_1)+\cot(\delta_2))^{-1/2} + S_{iUAV} / S_i + P_i / P_{\max})D_i \tag{2}$$

among this,

$$D_i = \left|\left(x-x_i, y-y_i, z-z_i\right)\times\left(1,\tan(\delta_1),\cot(\delta_2)\right)\right| / \sqrt{\left(1^2+\tan(\delta_1)^2+\cot(\delta_2)^2\right)} \tag{3}$$

represents the distance between the position of the target drone and the azimuth line obtained by the i-th F-UAV target detection and positioning, S_{iUAV} / S_i represents the ratio between the area of the target drone in the image taken by the i-th F-UAV and the complete image area, $P_i / P_{\max}$ represents the ratio between the resolution of the i-th F-UAV airborne camera and the highest resolution of the airborne camera in the F-UAV, and (x, y, z) represents the optimal position of the desired target.

3.2 GPS Spoofing Attack Signal Calculation Scheme

With the help of multiple F-UAV coordinated tracking, C-UAV (Controller UAV) obtains the position of the target UAV in real-time and predicts its motion trajectory. According to the predicted motion trajectory of the target UAV, combined with the final position of the expected UAV to be attacked, false location information can be generated in real-time. When the target UAV obtains the false position information, it will adjust the direction of movement to move to the expected position of the attack. The specific position relationship is shown in Fig. 1.

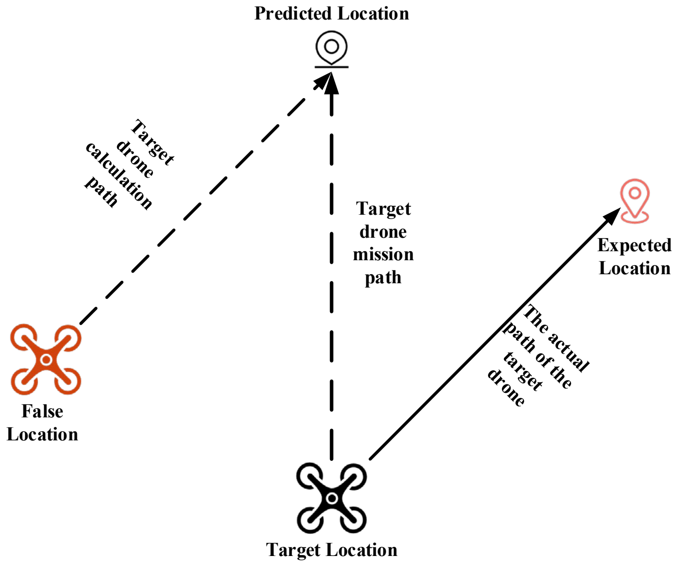
Predicted Location
Target drone calculation path
Target drone mission path
Expected Location
The actual path of the target drone
False Location
Target Location

Figure 1 Diagram of the relationship between positions during the attack

Due to the inaccuracy of the predicted position, it is necessary to continuously update the target position, predicted position, and false position information during the movement of the target drone, so that the target drone can fly strictly by the expected flight trajectory. When F-UAV detects that the flight trajectory of the target UAV has deviated from the expected trajectory, it needs to re-predict the destination of the target UAV according to the target position to adjust the content of the false position information. The specific adjustment method is shown in Fig. 2. The F-UAV detects the movement direction of the target UAV and obtains its displacement direction relative to the false position. This direction is the direction of the predicted position relative to the original false position, that is, the false position is at the intersection of the original predicted direction and the new predicted position. From this, the revised predicted position can be obtained.

Based on obtaining the corrected predicted position, use the false position generating method described above to generate corrected false position information, so that the target drone can adjust the flight direction and fly toward the expected position. The correction method is shown in Fig. 3. To prevent the revised false location information from being too different from the original false location information, it is necessary to increase the refresh rate of the false location information as much as possible to make the changes of the false location information continuous and smooth. With the aid of YOLO Nano's rapid target recognition ability, the refresh rate of target position information can be reached 30 times per second, and on this basis, the smooth and continuous change of false position can be guaranteed.

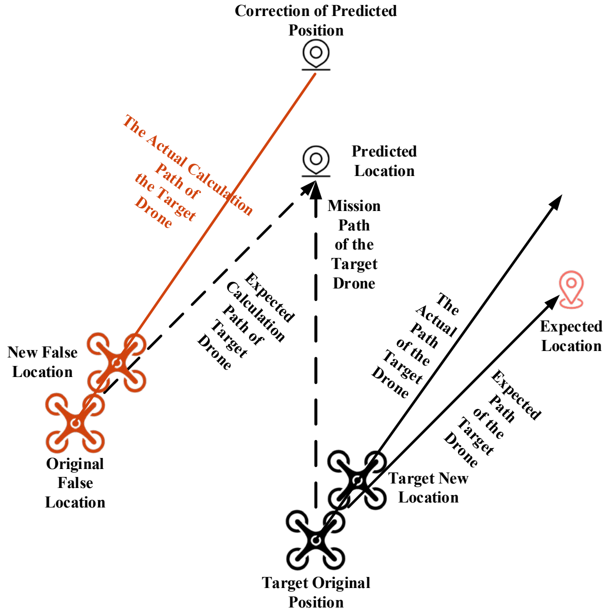
Correction of Predicted Position
The Actual Calculation Path of the Target Drone
Predicted Location
Mission Path of the Target Drone
Expected Calculation Path of Target Drone
New False Location
Original False Location
The Actual Path of the Target Drone
Expected Location
Expected Path of the Target Drone
Target New Location
Target Original Position

Figure 2: Architecture 1 of the proposed scheme

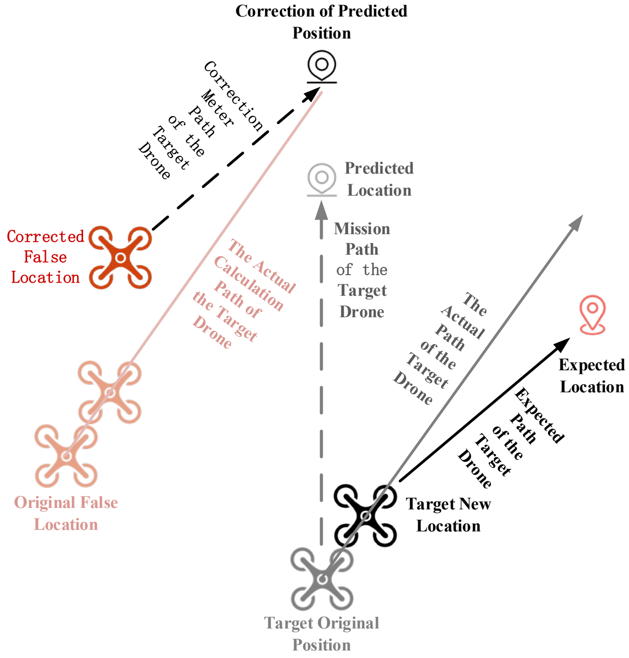
Correction of Predicted Position
Correction Meter Path of the Target Drone
Predicted Location
Corrected False Location
The Actual Calculation Path of the Target Drone
Mission Path of the Target Drone
The Actual Path of the Target Drone
Expected Location
Expected Path of the Target Drone
Original False Location
Target New Location
Target Original Position

Figure 3: Architecture 2 of the proposed scheme

T-UAV (Transmitter UAV) adjusts the flight trajectory based on the calculated false position information so that its position is always maintained on the connection between the target UAV and the false GPS satellite. At the same time, T-UAV will adjust the GPS signal content so that the position information calculated by the target drone is consistent with the false position.

4 Results and Discussion

4.1 Experimental Environment

The YOLO Nano-based multi-UAV coordinated GPS spoofing attack solution also selected Mavic Mini as the target drone. The target drone uses the official DJI GO app to set the flight trajectory. During the attack, the target drone flies autonomously according to the set trajectory.

In the setting of the attack drone, improvements have been made based on the NSGA-II-based multi-UAV coordinated GPS spoofing solution, and the DJI M600 drone serving as the C-UAV has added high-precision vision sensors and A high-performance pan/tilt, adding a visual sensor to the selected part of the DJI M100 serving as T-UAV at random. The vision sensor uses Zenmuse P1, the video size is set to 1920 × 1080, and the frame rate is set to 30 fps, which means that the target position information is collected 30 times per second. At the same time, the PTZ angle and the inclination angle information of the fuselage are synchronously acquired at a frequency of 30 times per second, so that the acquired angle information corresponds to the target position information in real-time.

4.2 Experimental Results

In actual experiments, when the target drone flies to the inflection point of its original mission, F-UAV needs to re-determine the mission point of the target drone. At this time, the false position information and the original trajectory obtained by the attacking drone are recalculated. A large deviation occurs, and then the trajectory resumes continuously. The target drone deviated slightly from the predetermined trajectory at this time, and then quickly recovered. When the target UAV flies to the inflection point of the expected trajectory, the false position information deviates greatly from the original trajectory, and then the trajectory resumes continuously. Eventually, the target drone arrives at the designated target point of attack.

It can be seen from the drawn false information trajectory map that, in addition to the false position information offset at the beginning of the attack, the false position information appears in segments when the target UAV has a turning point and when the expected flight path is turning. The target UAV mission trajectory turning number is equal to the expected trajectory turning number.

5 Conclusion

In the research content of this paper, the basic framework of the multi-UAV cooperative GPS deception scheme based on YOLO Nano is first proposed. Then, based on the aerial image correction method of the attack drone, multi-UAV coordinated target detection and positioning scheme based on YOLO Nano is proposed to achieve high-precision and rapid positioning of the target drone. Then, based on accurate target detection and positioning, an attack signal calculation scheme for the unmanned aerial vehicle in the moving state is proposed to realize the fixed-point deception and trajectory deception against the unmanned aerial vehicle in the moving state. Finally, the actual flight experiment verified the feasibility and effectiveness of the scheme.

In the future, we will study the multi-sensor fusion target detection and positioning scheme. The target detection and positioning scheme used in this article is based on monocular vision target detection using information sharing between multiple F-UAVs to accurately determine the target location. With the increase of the UAV’s endurance and load capacity, the airborne With the improvement of computer computing power, multiple sensors can be used to collect information of the target drone at the same time, and the positioning accuracy can be further improved based on multi-sensor fusion.

Funding Statement: This work is supported by the National Natural Science Foundation of China under

Grants U1836110, U1836208; by the Jiangsu Basic Research Programs-Natural Science Foundation under Grant No. BK20200039.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Fahlstrom and T. Gleason, *Introduction to UAV Systems*, John Wiley & Sons, 2012.

[2] L. Li, T. Xiong, X. Hu and J. Xiong, "Application areas and future of UAV," *Geospatial Information*, vol. 5, no. 8, pp. 7–9, 2010.

[3] D. He, S. Chan and M. Guizani, "A survey on security of unmanned aerial vehicles," *Chinese Journal of Computers*, vol. 42, no. 5, pp. 1076–1094, 2016.

[4] D. He, G. Yang, H. Li, S. Chan, Y. Cheng *et al.,* "An effective countermeasure against UAV swarm attack," *IEEE Network*, pp. 1–6, 2020.

[5] D. He, H. Liu, S. Chan and M. Guizani, "How to govern the non-cooperative amateur drones?" *IEEE Network*, vol. 33, no. 3, pp. 184–189, 2019.

[6] M. G. Wing, A. Eklund and L. D. Kellogg, "Consumer-grade global positioning system (GPS) accuracy and reliability," *Journal of Forestry*, vol. 103, no. 4, pp. 169–173, 2005.

[7] M. Liu, "Global positioning systen and fiscussion on its use GPS," *China Measurement Technology*, vol. 32, no. 6, pp. 5–11, 2006.

[8] D. M. Lin and J. B. Tsui, "A software GPS receiver for weak signals," in *Proc. 2001 IEEE MTT-S International Microwave Sym. Digest*, Phoenix, AZ, USA, vol. 3, pp. 2139–2142, 2001.

[9] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[10] M. Trinkle and D. Gray, "GPS interference mitigation; overview and experimental results," in *Proc. the 5th Int. Sym. on Satellite Navigation Technology & Applications*, Canberra, Australia, pp. 1–14, 2001.

[11] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. the 18th ACM Conf. on Computer and Communications Security*, Chicago, IL, USA, pp. 75–86, 2011.

[12] D. P. Shepard, J. A. Bhatti, T. E. Humphreys and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proc. Radionavigation Laboratory Conf. Proc.*, Austin, TX, USA, 2012.

[13] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. Radionavigation Laboratory Conf. Proc.*, Austin, TX, USA, 2008.

[14] Y. Liu, W. Su and S. Yan, "Efficiency analysis of repeater deception jamming GPS repeater," *Journal of Air Force Rader Academy*, vol. 18, no. 4, pp. 4–6, 2004.

[15] J. Yang, F. Zeng, H. Sheng and L. Zhu, "A jamming system through section mapping for GPS navigation," *Acta Electronica Sinica*, vol. 33, no. 6, pp. 1036–1038, 2005.

[16] S. Zhang, J. Yang, G. Pan and T. Dong, "The time-delay algorithmic in GPS area-mapping deceiving unites battlefield navigation integrative system," *Journal of Anhui University (Natural Science Edition)*, vol. 35, no. 1, pp. 64–68, 2011.

[17] S. Zhang, J. Yang, G. Pan and L. Wang, "Station embattling optimization and moving model of the GPS area-mapping deceiving unites battlefield navigation integrative system," *Journal of University of Science and Technology of China*, vol. 41, no. 8, pp. 746–752, 2011.

[18] S. Zhang, M. Miao, S. Shuai, Z. Han and D. Peng, "A study on the performance between multi-transmitters and single transmitter GPS inducing system," *Modern Radar*, vol. 35, no. 1, pp. 1–5, 2013.

[19] Z. Yan, D. Wu and H. Liu, "Analysis of time-dalay in GPS repeater deception jamming," *Journal of Air Force Engineering University (Natural Science Edition)*, vol. 14, no. 4, pp. 67–70, 2013.

[20] Z. Yan, D. Wu, J. He, H. Liu and H. Mao, “Deployment method of jammer in GPS repeater deception jamming,” *Modern Radar*, vol. 37, no. 3, pp. 75–79, 2015.

[21] L. He, “The design and implementation of GNSS spoofing jamming simulation system,” M.S. thesis, University of Elecatronic Science and Technology of China, 2016.

[22] D. He, Y. Qiao, S. Chen, X. Du, W. Chen *et al.,* “A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles,” *IEEE Network*, vol. 33, no. 2, pp. 146–151, 2018.

[23] J. S. Warner and R. G. Johnston, “A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing,” *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[24] J. Gaspar, R. Ferreira, P. Sebastião and N. Souto, “Capture of UAVs through GPS spoofing using low-cost SDR platforms,” *Wireless Personal Communications*, pp. 1–26, 2020.

[25] D. P. Shepard, J. A. Bhatti, T. E. Humphreys and A. A. Fansler, “Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks,” in *Proc. the 25th Inter. Technical Meet. of the Satellite Division of the Institute of Navigation,* Nashville, TN, USA, pp. 3591–3605, 2012.

[26] L. Huang, Z. Lv and F. Wang, “Spoofing pattern research on GNSS receivers,” *Journal of Astronautic*, vol. 33, no. 7, pp. 884–890, 2012.

[27] K. Ma, X. Sun and Y. Nie, “Research on key technologies of GPS generated spoofing,” *Aerospace Electronic Warfare*, vol. 30, no. 6, pp. 24–26, 2014.

[28] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[29] Y. Hu, S. Bian, K. Cao and G. Feng, “Spoofing power control strategy for GNSS receiver,” *Journal of Chinese Inertial Technology*, vol. 23, no. 2, pp. 207–210, 2015.

[30] Q. Liao, J. Hao, N. Zheng and W. Liu, “Research on GPS navigation interference method based on trajectory deeption,” *Journal of Information Engineering University*, vol. 21, no. 2, pp. 141–145, 2020.

[31] S. Yi, X. Li and L. You, “Research on improvement of code phase synchronization accuracy in GPS spoofing,” in *Proc. the 5th Information Technology and Mechatronics Engineering Conf.*, Chongqing, SC, China, pp. 385–390, 2020.

[32] Y. Sheng, H. Li, S. Zhou and B. Zhang, “Research on GPS generative deception jamming method,” *Foreign Elecironic Measurement Technology*, vol. 37, no. 8, pp. 39–43, 2018.

[33] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li *et al.,* “All your GPS are belong to us: Towards stealthy manipulation of road navigation systems,” in *Proc. the 27th USENIX Security Sym.,* Baltimore, MD, USA, pp. 1527–1544, 2018.