Efficient Drone Hijacking Detection using Onboard Motion Sensors

ZHIWEI FENG, Northeastern University, China and University of Illinois at Urbana-Champaign, USA
NAN GUAN, The Hong Kong Polytechnic University, Hongkong
MINGSONG LV, Northeastern University, China
WEICHEN LIU, Nanyang Technological University, Singapore
QINGXU DENG, Northeastern University, China
XUE LIU, McGill University, Canada
WANG YI, Uppsala University, Sweden

With the fast growth of civil drones, their security problems meet significant challenges. A commercial drone may be hijacked by the GPS-spoofing attack for illegal activities, such as terrorist attacks. The target of this paper is to develop a technique that only uses onboard gyroscopes to determine whether a drone has been hijacked.

Ideally, GPS data and the angular velocities measured by gyroscopes can be used to estimate the acceleration of a drone, which can be further compared with the measurement of the accelerometer to detect whether a drone has been hijacked. However, the detection results may not always be accurate due to some calculation and measurement errors, especially when no hijacking occurs in curve trajectory situations. To overcome this, in this paper, we propose a novel and simple method to detect hijacking only based on gyroscopes measurements and GPS data, without using any accelerometer in the detection procedure. The computational complexity of our method is very low, which is suitable to be implemented in the drones with micro-controllers. On the other hand, the proposed method does not rely on any accelerometer to detect attacks, which means it receives less information in the detection procedure and may reduce the results accuracy in some special situations. While the previous method can compensate for this flaw, the high detection results also can be guaranteed by using the above two methods. Experiments with a quad-rotor drone are conducted to show the effectiveness of the proposed method and the combination method.

CCS Concepts: • **Security and privacy** → Systems security;

Additional Key Words and Phrases: Cyber Physical System, Unmanned Aerial Vehicle, GPS Spoofing

Corresponding author: Q. Deng, email: dengqx@mail.neu.edu.cn, School of Computer Science and Engineering, Northeastern University (China), NO. 195, Chuangxin Rd, Hunan District, Shenyang, Liaoning, China, 110000
This work is supported by the China Scholarship Council Grant No. 201706080092, National Natural and Science Foundation of China under Grant No. 61672140, 61528202 and 61472072 , and the project of the State Key Laboratory in China under Grant No.: 2017RALKFKT002.
Authors' addresses: Z. Feng, M. Lv, School of Computer Science and Engineering, Northeastern University (China), NO. 195, Chuangxin Rd, Hunan District, Shenyang, Liaoning, China, 110000 ; N. Guan, Department of Computin, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong; W. Liu, School of Computer Science and Engineering, Nanyang Technological University, Singapore, 50 Nanyang Avenue, Block N4 02a-32, Singapore 639798; X.Liu, Department of Mathematics and Statistics, and Department of Electrical and Computer Engineering, McGill University, Canada, 845 Sherbrooke St W, Montreal, QC H3A 0G4, Canada; W. Yi, Department of Information Technology, Uppsala University, Sweden, Box 337,751 05, UPPSALA..

XXXX-XXXX/2018/10-ART1 $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Zhiwei Feng, Nan Guan, Mingsong Lv, Weichen Liu, Qingxu Deng, Xue Liu, and Wang Yi. 2018. Efficient Drone Hijacking Detection using Onboard Motion Sensors. 1, 1, Article 1 (October 2018), 19 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Drone, also called Unmanned Aerial Vehicle (UAV), is one of the developing directions of Cyber Physical Systems. Compared with manned aircrafts, drones were originally used for missions too "dull, dirty or dangerous" for humans [21], while in recent years there use is rapidly expanding to commercial, scientific, recreational, agricultural and other applications, such as policing, peacekeeping and surveillance, product deliveries, aerial photography, agriculture, smuggling and drone racing. The drone industry has experienced an exponential growth in the last decade, like Parrot, 3D Robotics and DJI. And the global sales of DJI has increased for 80 times in the last three years [4].

The rapid growth of drones has raised significant security challenges, e.g. security and privacy [1]. Civilian drones can be easily equipped with weapons or explosives to operate terrorist attacks. At present, many countries are working on laws to control the entire life cycle of drones, including production, sales and use. However, even under such strict policies, drones still have many challenges that are difficult to solve. One of the main problems is that legitimate drones can possibly be hijacked and launch malicious purposes.

Drone Hijacking by GPS spoofing. Drones rely on GPS navigation in medium - and long-range flights. The attackers can use the devices to fake GPS satellites broadcasting signals to deceive GPS receivers (known as GPS spoofing), and navigate the drone based on the attacker's intention. The interest in GPS spoofing attacks has been raised greatly after [22] shows any number of GPS receiver can easily be spoofed to one arbitrary location and presents how to successfully implement the GPS spoofing attacks. Although researchers have proposed several methods to detect or prevent the GPS spoofing (see Section 2), these methods all require extra hardware devices or expensive signal processing algorithms, which considerably increase both the cost and the weight of drones and thus may not be acceptable to the market of lightweight civil drones.

Onboard Motion Sensors. In this work, we develop a lightweight approach to let a drone detect whether it has been hijacked. Our approach does not require any extra device, but only uses the onboard motion sensors such as gyroscopes and/or accelerometers. The motion sensors can be used as INS (Inertial Navigation System). As suggested by the name, the linear acceleration and angular velocity measured by the motion sensors can be integrated over time to calculate the position of the drone. Ideally, we can detect drone hijacking by comparing the position computed according to the motion sensors and the position reported by GPS: we can judge that the drone is hijacked if the distance between these two positions is sufficiently large. Unfortunately, the above approach does not work in practice due to the significant error accumulation over time [7]. Another method uses gyroscopes and GPS data to estimate the accelerations, and compares with the output of accelerometers [7]. However, it doesn't work well when no hijacking occurs in curve trajectory situations, and in Section 5 we will discuss in details.

Contributions of This Paper. This paper presents a novel hijacking detection method based on gyroscopes and GPS, but can much better overcome the error problem compared with the method proposed in [7] (called DATE method for short). Instead of comparing accelerations in body-fixed coordinate, the main idea is to compare the *trajectory variation trends* between 1) yaw calculated by the angular velocity, and 2) the angle enclosed by its GPS trajectory and the line in the direction of the geographical North Pole, more details will be discussed in Section 4. In this way, the hijacking detection accuracy, especially when no hijacking occurs in curve trajectory situations, could be improved by avoiding some calculation errors due to fewer, simpler calculation procedures and some measurement errors brought from the accelerations measurement procedures compared with DATE method. Experiments show that our method is very effective to precisely detect hijacking in such situations even we use much more complexity randomly generated curves than [7]. While, in general, this method may just work ordinary in the case that the drone flies a straight line, because of lesser information that proposed method considered, i.e. no using any accelerometer in detection method. However, DATE method does it well in such situations. Therefore, in order to compensate both disadvantages, we decide run both methods on the drone to guarantee the high accuracy results. This is **another contribution** in this paper. On the other hand, the most complex calculation procedures, i.e. integrations in both proposed method and DATE method, are reused from INS in autopilots, so the complexity of our method is very low, and is suitable to be implemented on the micro-controllers of common civil drones.

The rest of paper is organized as follows. In the next section, a brief overview of related works is given. The background of INS and DATE method is introduced in Section 3. In Section 4, it presents the proposed method in detail. In Section 5, it evaluates the effectiveness of the proposed method and finally, we conclude the paper in Section 6.

2 RELATED WORKS

Spoofing attacks are extremely destructive and deceitful for GPS receivers. They can make GPS receivers to generate misleading position information while it is very difficult to be detected [10, 22, 24]. Therefore, reliable spoofing detection techniques become more and more important, especially for some critical GPS applications and services. Several GPS anti-spoofing techniques have been proposed in the past few years.

S. Khanafseh et al. developed an INS batch RAIM monitor to detect GPS spoofing attacks in [8]. This monitor allowed to evaluate the integrity risk of the position solution and probability of missed detection. B. Ali et al. introduced a spoofing-aware receiver architecture that is able to detect spoofing attacks, classify the spoofing and authentic signals, and mitigate the harmful effect of counterfeit spoofing signals in [2]. It showed that the spoofing signals generated from a single-point source can be effectively detected using different metrics, namely AGC level. W. Myrick et al. develop a single antenna anti-jam/anti-spoofing method called MAGIC in [14]. It applied a reduced-rank MMSE based C/A code correlator for single antenna GPS receivers that replaces a standard C/A code correlator for enhanced anti-jam/antispoofing capability. J. Mead et al. explored a hardware named sandboxing in [13], to provide runtime monitoring of boundary signals and isolation which can detect and isolate unwanted behavior. A. Ranganathan et al. proposed a detection technique called the auxiliary peak in a novel GPS receiver referred to SPREE tracking enables detection of a strong attacker capable of executing the seamless GPS-spoofing attack in [19]. The common drawback of the above methods is that they require special hardware devices, which significantly increase the weight and cost of the drone. Therefore, these methods are not applicable to lightweight civil drones.

According to the Doppler effect, researchers develop techniques to monitor the behavior and integrity of the GPS signals to detect GPS spoofing, such as [23, 25]. D. Yuan et al. proposed a spoofing detection at the acquisition stage based on the sequential probability ratio test in [26]. It also can report the relationship of the average spoofing detection time, probabilities of detecting the spoofing and genuine signals. Another method was developed that processed GPS beat carrier phase measurements from the single moving antenna to determine whether the GPS signals are being spoofed in [17]. X. Chen et al. developed a novel trust framework based on subjective logic to evaluate the integrity of received GPS signals. They also characterized spoofing detection methods and extracted the causal relation between the measurement validity and signal integrity in [3]. An approach utilizing an antenna array was proposed in order to suppress spoofing attacks in [6]. It was based on the assumption that all spoofing signals are transmitted from a single point source. All the above techniques involve computationally expensive signal processing algorithms, and thus are not suitable for lightweight civil drones, which use micro-controllers with limited computation capacity.

There are still some work mentioned onboard sensors, such as [20]. However, comparing them with the proposed method, our methods have simpler computational procedures, i.e. using simple operations instead of much more integrations, to achieve high accuracy results. On the other hand, their experiments are based on simulation, while this paper uses the real sensor data from a quad-rotor drone flying in an open space.

3 PRELIMINARY

3.1 GPS Spoofing Attack

The Global Positioning System (GPS) is a space-based navigation system that provides position information to any GPS receiver on or near the earth that has an unobstructed line of sight to four or more GPS satellites.

GPS spoofing attacks try to deceive GPS receivers by broadcasting fake GPS signals, structured to resemble a set of normal GPS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. In such a way, these signals may be modified as to cause the receiver to estimate its position to be somewhere rather than where it actually is, as determined by the attacker.

Figure 1 shows the illustration of GPS-spoofing-based hijacking. The drone originally plans to fly from the starting point to the planned destination. When the drone flies at p_0, GPS spoofing starts, and the fake GPS signal reports along the red line of the fake positions, and the drone deviates from its planned trace. For example, when a drone is at p_2, the faked GPS signal reports position p_1, the drone will fly in the same direction as p_1 to the planned destination.

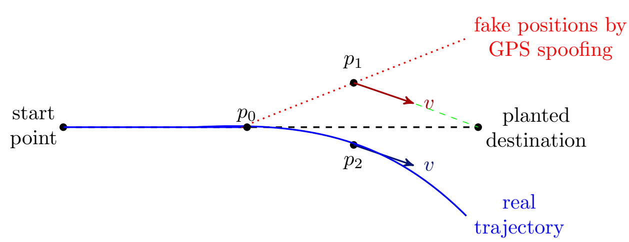


Fig. 1. An example of drone hijacking by GPS spoofing attacks.

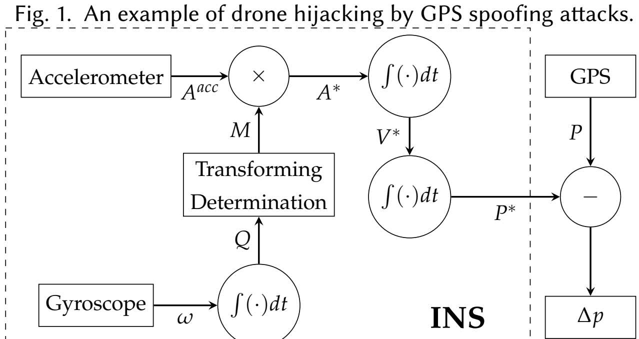


Fig. 2. Detection by comparing the positions reported by GPS and INS.

3.2 INS

The motion sensor (accelerometer and gyroscopes) can be used as an Inertial Navigation System (INS) which uses these sensors to calculate positions and navigates the drone [5]. Unlike GPS, INS does not rely on any external signal. The left part (in the dashed box) of the diagram in Figure 2 illustrates the basic principles of INS. The accelerometer measures the linear acceleration A^{acc} in different directions in the body-fixed coordinates. The gyroscope measures the angular velocity ω of the drone (in the yaw, pitch and roll axis respectively). The integration of angular velocity gives the absolute angle of the drone over time and it is used to export the transformation matrix M. Using M, the accelerations in the body-fixed coordinate are converted into the linear acceleration of the geographic coordinates A^*. The linear acceleration A^* are integrated over time once to get the linear speeds V^*, then to get the estimated position P^*. Note that since the drones fly in low speed, the influences of earth rotation is neglected.

3.3 Hijacking Detection by Comparing INS and GPS

The simple way to detect whether a drone has been hijacked is to compare the two positions of GPS and INS, as shown in Figure 2. However, due to the poor accuracy of the position calculated by INS, this method does not work in practice. Accelerometers and gyroscopes may introduce errors in their instantaneous measurement results. Although the instantaneous error is usually very small, the accumulative error could be very large over time, so the INS estimation positions may significantly deviate from the real ones. Figure 3 shows the experimental results of a drone (the hardware platform of the drone will be introduced in Section 5), and the estimated trajectory does seriously deviate from the real trajectory.

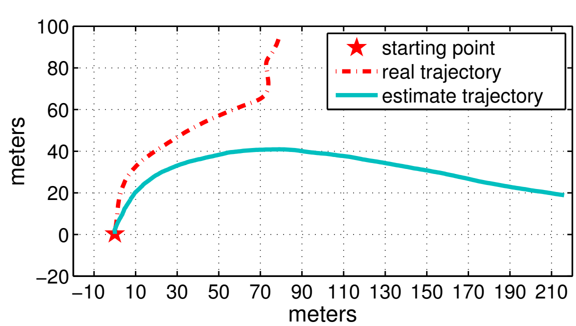


Fig. 3. The estimated positions using INS are far away from the GPS's

3.4 DATE Method

The main idea of [7] is shown in Figure 4. It uses the position information reported by the GPS to estimate the speeds V and then estimate the accelerations A in the geographic coordinate. The angular velocity ω measured by the gyroscopes will be used to compute the transform matrix M, by which the accelerations A in the geographic coordinate are transformed to A^* accelerations in the body-fixed coordinate. Then it can detect drone hijacking if the differences between A^* and the measured accelerations A^{acc} by the accelerometers exceed certain thresholds.

In the experiment of Figure 5, the drone flies normally along a straight line, where $\Delta a_x(t)$ and $\Delta a_y(t)$ are continuously closed to 0. In Figure 6, the drone is hijacked, where $\Delta a_x(t)$ and $\Delta a_y(t)$ significantly deviate from 0.

Compared with the method introduced in Section 3.3, this method avoids the accumulated errors caused by the two integration operations in each iteration with the accelerations measurements,

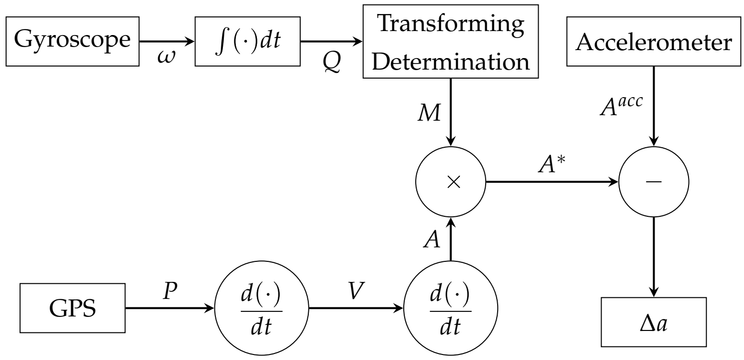
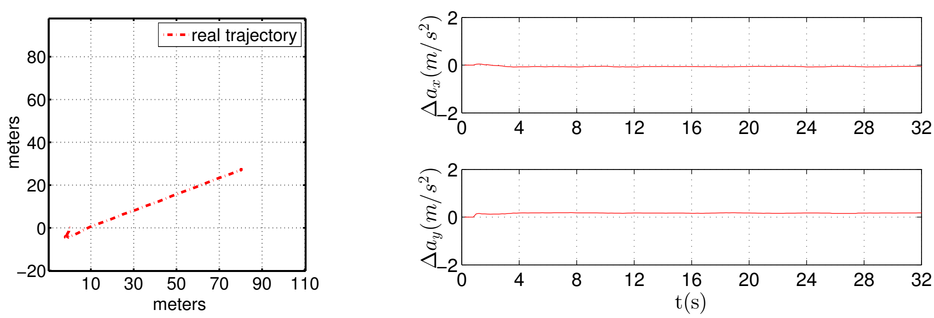


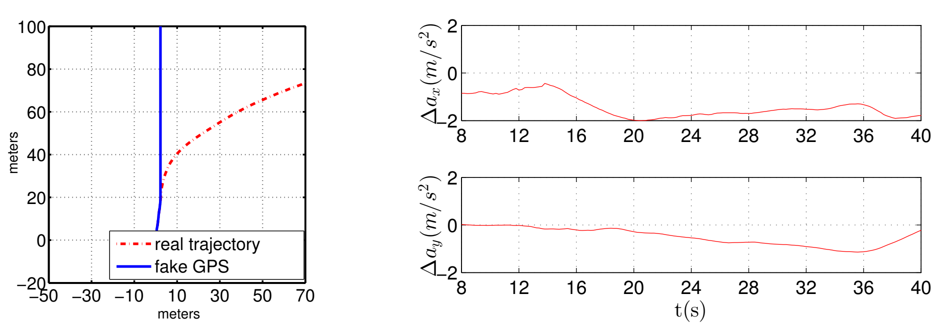
Fig. 4. The block diagram of DATE method

which is the main reason why the INS-estimated position is significantly inaccurate. Therefore, this method can achieve a much higher detection precision.



(a) Trajectory (b) Δa_x and Δa_y

Fig. 5. Example 1: Δa_x and Δa_y of DATE method in a non-hijacked case



(a) Trajectory (b) Δa_x and Δa_y

Fig. 6. Example 2: Δa_x and Δa_y of DATE method in a hijacked case

3.5 Extended Kalman Filter

The gyroscope has the bias, which the initial zero reading of the gyroscope will cause drift over time. All the autopilots, such PX4, Pixhawk, use Extended Kalman Filter (EKF) to estimate this bias over time to reduce the gyroscopes noises. In this section, a brief description of the simple EKF will be introduced. The details can be seen in [5].

There are 15 states in the EKF:

$$\mathbf{x} = [\underbrace{P_x\ P_y\ P_z}_{\text{Position}}\ \underbrace{V_{\text{North}}\ V_{\text{East}}\ V_{\text{Down}}}_{\text{Groundspeed}}\ \underbrace{\theta\ \beta\ \gamma}_{\text{Attitude}}\ \underbrace{b_{ax}\ b_{ay}\ b_{az}}_{\text{Accelerometer Bias}}\ \underbrace{b_{gx}\ b_{gy}\ b_{gz}}_{\text{Gyroscope Bias}}].$$

Then, according to INS, updates position, ground speed and attitude at the current time. Next, The covariance is updated according to

$$\mathbf{P}^{(-)}[k+1] = \theta[k]\mathbf{P}^{(+)}[k]\theta[k]^T + \mathbf{Q}[k].$$

where $\mathbf{P}$ is the posterior error covariance matrix (a measure of the estimated accuracy of the state estimate) and $\mathbf{Q}$ is the process noise covariance matrix. The state transition matrix can be approximated as $[k] = I + F[k]\Delta t$. $\mathbf{F}$ is the state-transition model.

When GPS position and velocity becomes available at time-step k, the measurement $\mathbf{y}$ is defined as follows:

$$\mathbf{y}|_{\text{GPS}} = \left[P_x\ P_y\ P_z\ V_{\text{North}}\ V_{\text{East}}\ V_{\text{Down}}\right]|_{\text{GPS}}$$

where P_x, P_y and P_z are the reported North-East-Down position with respect to a specific location, e.g., the initial position.

Define the state error as:

$$\delta\mathbf{y} = \mathbf{y}|_{\text{GPS}} - \left[P_x\ P_y\ P_z\ V_{\text{North}}\ V_{\text{East}}\ V_{\text{Down}}\right]|_{\text{INS}[k]}.$$

The covariance is updated using

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{0}_{3\times9} \\ \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} & \mathbf{0}_{3\times9} \end{bmatrix}$$
$$\mathbf{K}[k] = \mathbf{P}^{(-)}[k]\mathbf{H}^T\left(\mathbf{R} + \mathbf{H}\mathbf{P}^{(-)}[k]\mathbf{H}^T\right)^{-1}$$
$$\mathbf{P}^{(+)}[k] = (\mathbf{I} - \mathbf{K}[k]\mathbf{H})\mathbf{P}^{(+)}[k](\mathbf{I} - \mathbf{K}[k]\mathbf{H})^T + \mathbf{K}[k]\mathbf{R}[k]\mathbf{K}[k]^T.$$

where $\mathbf{H}$ is the observation model which maps the true state space into the observed space and $\mathbf{R}$ is the covariance of the observation noise.

The state is updated according to:

$$\delta\mathbf{x} = \mathbf{K}[k]\delta\mathbf{y}$$

Then, position and velocity can be estimated by INS.

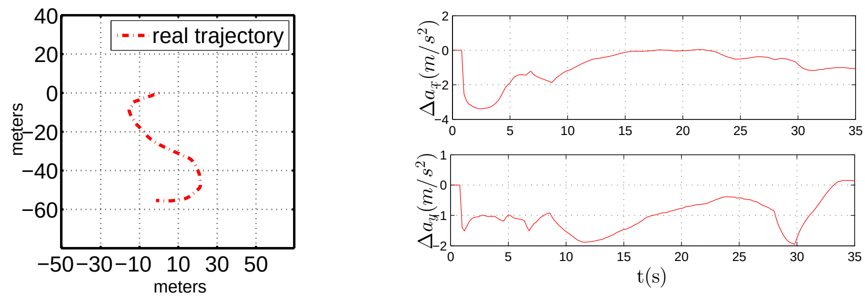
When using Euler angle representation, the attitude is updated using the transformation matrix M by INS. After that, gyros bias can be updated by

$$\mathbf{b}_g^{(+)}[k] = \mathbf{b}_g^{(-)}[k] + \delta\mathbf{x}[13:15].$$

4 OUR METHOD

4.1 The idea of our method

The DATE method in [7] has a high detection precision, though it may not work well in some non-hijacked cases, like Figure 7. In Figure 7(a), the real trajectory of a drone likes a letter "S" during a short distance. Since calculation and measurement errors brought by such sharply turns, Δa_x and Δa_y , shown as Figure 7(b), have much fluctuations (are not closed to zero like Figure 5(b)) which leads to a fault detection result. In order to improve the results accuracy of such curve trajectories in non-hijacked cases, we proposed another detection method just using gyroscopes and GPS data to compare the trajectory variation trends between the drone movement and GPS trajectory.



(a) Trajectory (b) Δa_x and Δa_y

Fig. 7. Example: DATE method doesn't work.

A drone in flight is free to rotate in three dimensions shown as Figure 8: **pitch**, nose up or down about lateral axis running from wing to wing; **yaw**, nose left or right about vertical axis running up and down; and **roll**, rotation about longitudinal axis running from nose to tail [**?**]. These axes are in the body-fixed coordinate of a drone and the Euler angles (pitch, roll and yaw) can be easily calculated by angular velocities, the details will be discussed in Section 4.2.

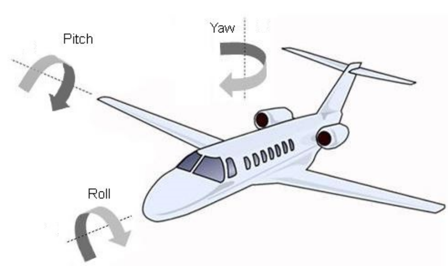


Fig. 8. body-fixed coordinate and Euler angles

If let the three-dimension body-fixed coordinate maps to the two-dimension plan, then a flight procedure of a drone can be seen as a vehicle driving procedure. In other words, yaw (nearly) decides the drone to turn left or right, and it could be reflected on the GPS trajectory. In Figure 1, when the fake GPS signal starts at p_0, the fake GPS trajectory turns left along the forward direction of the drone, while the real trajectory turns to the opposite direction. Our idea just uses this phenomenon to develop a detection method.

However, attackers may hijack a drone to fly downwards and hit the ground or a high mountain when the horizontal trajectory remains the same. While on each commercial drone, it has an altimeter to measure its flight height, so the above scenario can be easily detected.

The main idea of the proposed method is shown in Figure 9. It uses the positions reported by the GPS to estimate the angles φ enclosed by the GPS trajectory and the line in the direction of the geographical North Pole, as shown in Figure 10. In the following, we call the angle φ "GPS angle" for short. The angular velocities measured by the gyroscope will be used to compute the transform matrix M, by which the Euler angles can be calculated, as [5] does. Then it detects the drone hijacking if the variation trend between GPS angles φ and yaws γ is different. The detail will be discussed in the following section.

However, strong wind or the different atmospheric environments can affect detection results. In such a scenario, the GPS trajectory is different with the moving trend estimated by Euler angles. Our detection method focuses on the comparison of the trajectory variation trends triggered by the drone itself, as for the design of our detection method, we may get the false arm in a sideslip. Before the drone doing the planned auto mission, we may not be possible to plan one or several sideslips during the flight, so only wind or atmospheric turbulence can cause unexpected sideslips. According to the design of the drone, especially the fixed-wing drone, it can quickly recover from sideslip or reduce the influence caused by wind or turbulence. If the wind has a long duration and its velocity exceeds the drone affordability, users may not fly the drone in practice. For the normal cases, the sideslip usually caused by the suddenly wind or turbulence. Even if it is failed in the correlation coefficient detection test, the proposed method still has a fault tolerance test. During this test, our method compares the average values in a period of time instead of one sampling time. If it is still failed, we also can wait for the result of DATE method because DATE method compares the difference of accelerations between the output of the accelerator and acceleration estimated by gyro and GPS. When the drone changes its movement after the wind, its acceleration must be changed. The experiments in Section 5 also show that run DATE method and the proposed method together can achieve a higher detection result than using any of them. On the other hand, the drone doing the planted auto mission, and during this mission, we may not be possible to plan the drone to have a sideslip during the flight, so the only thing can cause sideslip is the wind or atmospheric turbulence, and this sideslip is unexpected. According to the design of the drone, especially the fixed-wing drone, it can quickly recover from sideslip or reduce the influence caused by sideslip. If the wind has a long duration and its velocity exceeds the drone affordability, we may not fly the drone in practice. For the normal cases, the sideslip usually caused by the sudden wind, and our method has a threshold called fault tolerance Îij. If the drone has a sudden sideslip and failed in the correlation coefficient comparing phase, but it also has a fault tolerance test. During this test, our method compares the average values in a period of time instead of one sampling time. So the influence of trajectory variation trends caused by suddenly sideslip can be reduced and it can also help to reduce the fault alarm.

Comparing with DATE method in Figure 4, the proposed method reduces some errors respectively caused by the extra calculation procedures and the measurement of accelerometers. Therefore, the detection results accuracy can be improved ideally.

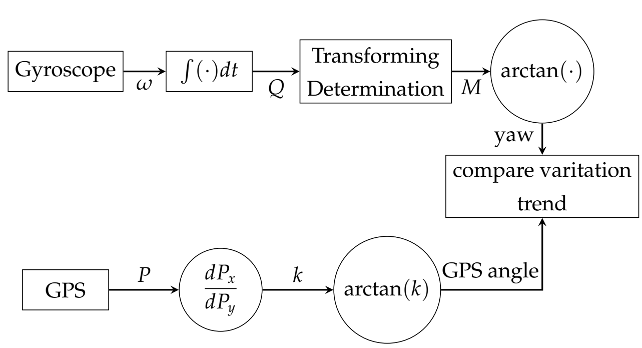


Fig. 9. The main block diagram of our method. In order to improve the detection results, comparing with DATE method, this method avoids the matrix multiplication in each iteration and does not rely on accelerometers which reduces errors brought by the measurements.

In the following, this paper introduces the details of the hijacking detection method. Section 4.2 focuses on how to compute the estimated angles respectively from the GPS and gyroscopes output

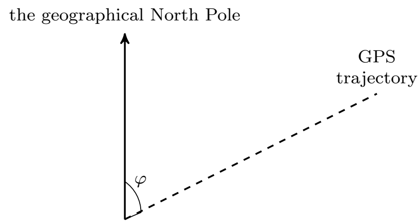


Fig. 10. The illustration of GPS angle φ.

data. Section 4.3 presents an algorithm to decide whether hijacking has happened based on the difference between these two angles variation trends.

4.2 Calculating GPS angle φ and the Euler angle yaw γ

The GPS reports the position $P(t) = [P_x(t), P_y(t), P_h(t)]^T$ of the drone in the geographic coordinate at every sampling time point t. It can easily get the GPS angle φ at each time point t by:

$$\varphi(t) = \begin{cases} \psi(t) & \Delta P_x(t) > 0,\ \Delta P_y(t) > 0 \\ \psi(t) + 2\pi & \Delta P_x(t) < 0,\ \Delta P_y(t) > 0 \\ \psi(t) + \pi & \Delta P_y(t) < 0 \\ 0 & \Delta P_x(t) = 0 \\ \frac{1}{2}\pi & \Delta P_y(t) = 0 \end{cases} \tag{1}$$

where $\psi = \arctan\left(\frac{\Delta P_x(t)}{\Delta P_y(t)}\right)$,$\psi \in [-\frac{1}{2}\pi, \frac{1}{2}\pi]$ and $P(t-1)$ is the position vector reported by the GPS at the previous sampling time point, $\Delta P_y(t) = P_y(t) - P_y(t-1)$ and $\Delta P_x(t) = P_x(t) - P_x(t-1)$.

The Euler angles yaw γ will be calculated by transformation matrix $M(t)$ at time t respectively [5]:

$$\gamma(t) = \begin{cases} \Gamma(t) & \Gamma(t) > 0,\ M_{22}(t) > 0 \\ \Gamma(t) + 2\pi & \Gamma(t) < 0,\ M_{22}(t) > 0 \\ \Gamma(t) + \pi & M_{22}(t) < 0 \end{cases} \tag{2}$$

where $\Gamma(t) = \arctan\left(-\frac{M_{12}(t)}{M_{22}(t)}\right)$, and $M_{22}(t)$ are the elements in matrix $M(t)$, and $M(t)$ is computed by (4):

$$M(t) = \begin{bmatrix} M_{11}(t) & M_{12}(t) & M_{13}(t) \\ M_{21}(t) & M_{22}(t) & M_{23}(t) \\ M_{31}(t) & M_{32}(t) & M_{33}(t) \end{bmatrix} \tag{3}$$

$$\begin{cases} M_{11}(t) = q_0(t)^2 + q_1(t)^2 - q_2(t)^2 - q_3(t)^2 \\ M_{12}(t) = 2(q_1(t)q_2(t) - q_0(t)q_3(t)) \\ M_{13}(t) = 2(q_1(t)q_3(t) + q_0(t)q_2(t)) \\ M_{21}(t) = 2(q_1(t)q_2(t) + q_0(t)q_3(t)) \\ M_{22}(t) = q_0(t)^2 - q_1(t)^2 + q_2(t)^2 - q_3(t)^2 \\ M_{23}(t) = 2(q_2(t)q_3(t) - q_0(t)q_1(t)) \\ M_{31}(t) = 2(q_1(t)q_3(t) - q_0(t)q_2(t)) \\ M_{32}(t) = 2(q_2(t)q_3(t) + q_0(t)q_1(t)) \\ M_{33}(t) = q_0(t)^2 - q_1(t)^2 - q_2(t)^2 + q_3(t)^2 \end{cases} \quad (4)$$

Quaternion $Q(t) = [q_0(t), q_1(t), q_2(t), q_3(t)]^T$ is iteratively computed according to the angular velocity vector

$$\omega = [\omega_x(t), \omega_y(t), \omega_z(t)]^T$$

reported by the gyroscopes:

$$\begin{bmatrix} \Delta q_0(t) \\ \Delta q_1(t) \\ \Delta q_2(t) \\ \Delta q_3(t) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 & -\omega_x(t) & -\omega_y(t) & -\omega_h(t) \\ \omega_x(t) & 0 & \omega_h(t) & -\omega_y(t) \\ \omega_y(t) & -\omega_h(t) & 0 & \omega_x(t) \\ \omega_h(t) & \omega_y(t) & -\omega_x(t) & 0 \end{bmatrix} \begin{bmatrix} q_0(t-1) \\ q_1(t-1) \\ q_2(t-1) \\ q_3(t-1) \end{bmatrix} \Delta t \quad (5)$$

where $\Delta q_i(t)$ is the variation of $q_i(t)$ and we can get Q for the current moment t by

$$q_i(t) = q_i(t-1) + \Delta q_i(t).$$

Before being applied to (4) to compute M, Q need be normalized to be more robust to measurement errors, i.e. carries much less gyroscope bias errors:

$$q_i(t) \leftarrow \frac{q_i(t)}{\sqrt{q_0^2(t) + q_1^2(t) + q_2^2(t) + q_3^2(t)}}, \quad i = 0, 1, 2, 3 \quad (6)$$

such that it satisfies:

$$q_0(t)^2 + q_1(t)^2 + q_2(t)^2 + q_3(t)^2 = 1 \quad (7)$$

The iterative computation of $\overline{Q}$ starts with the initial values obtained as follows. The initial attitude angles of the drone are θ (pitch), γ (yaw) and β (roll), then we compute the initial value of M, denoted by $\overline{M}$ by:

$$\begin{cases} \overline{M}_{11} = cos\beta \cdot cos\gamma - sin\beta \cdot sin\theta \cdot sin\gamma \\ \overline{M}_{12} = -cos\theta \cdot sin\gamma \\ \overline{M}_{13} = sin\beta \cdot cos\gamma + cos\beta \cdot sin\theta \cdot sin\gamma \\ \overline{M}_{21} = cos\beta \cdot sin\gamma + sin\beta \cdot sin\theta \cdot cos\gamma \\ \overline{M}_{22} = cos\theta \cdot cos\gamma \\ \overline{M}_{23} = sin\beta \cdot cos\gamma - cos\beta \cdot sin\theta \cdot sin\gamma \\ \overline{M}_{31} = -sin\beta \cdot cos\theta \\ \overline{M}_{32} = sin\theta \\ \overline{M}_{33} = cos\beta \cdot cos\theta \end{cases} \quad (8)$$

When a drone starts to fly, we assume that $\gamma = \beta = 0$ and γ can be calculated by the first two successive GPS points. Then according to (9), the initial absolute value of Q can be calculated.

$$\begin{cases} |\overline{q_1}| = \frac{1}{2}\sqrt{1 + \overline{M}_{11} - \overline{M}_{22} - \overline{M}_{33}} \\ |\overline{q_2}| = \frac{1}{2}\sqrt{1 - \overline{M}_{11} + \overline{M}_{22} - \overline{M}_{33}} \\ |\overline{q_3}| = \frac{1}{2}\sqrt{1 - \overline{M}_{11} - \overline{M}_{22} + \overline{M}_{33}} \\ |\overline{q_0}| = \sqrt{1 - \overline{q_1}^2 - \overline{q_2}^2 - \overline{q_3}^2} \end{cases} \tag{9}$$

The sign of $\overline{q_i}$ is decided as follows:

$$\begin{cases} \text{sign}(\overline{q_1}) = + \\ \text{sign}(\overline{q_1}) = \text{sign}(M_{32} - M_{23}) \\ \text{sign}(\overline{q_2}) = \text{sign}(M_{13} - M_{31}) \\ \text{sign}(\overline{q_3}) = \text{sign}(M_{21} - M_{12}) \end{cases} \tag{10}$$

Note that the computation of the transformation matrix M is the same as the standard position estimation in INS [5].

In addition, the proposed method also uses EKF (Extended Kalman Filter) to reduce bias errors caused by gyroscopes. It is wildly used in many autopilots, and it processes sensor measurements then provides the gyroscope delta angle bias estimates [5, 11]. In the experiment, the proposed method directly uses them from the outputs of the autopilot.

ALGORITHM 1: Pseudo-code of calculating GPS angle φ and yaw $\gamma(t)$

```
1: Calculate the initial transformation matrix M̄ by (8)
2: Calculate the initial quaternion Q̄ by (9) and (10)
3: for each sampling time t do
4:     Calculate quaternion Q(t) with Q(t − 1) by (5), (6)
5:     Calculate transformation matrix M(t) with Q(t) by (4)
6:     Calculate yaw γ(t) by (2) respectively
7:     Calculate GPS angle φ(t) by (1)
8: end for
```

4.3 Detection method

Now we present how to decide whether the drone has been hijacked by comparing GPS angle φ and the Euler angles: yaw γ. Assume $\varphi'(t)$ and $\gamma'(t)$ are respectively GPS angle and yaw at time point t. We apply a simple median filtering algorithm to GPS angle $\varphi(t)$ and yaw $\gamma(t)$ sequence by

$$\varphi(t) = \sum_{i=t-n}^{t} \varphi'(i)/n$$

$$\gamma(t) = \sum_{i=t-n}^{t} \gamma'(i)/n$$

where n is the window size of the median filtering and the size of n is relatively small. This step also reduces angular random walk caused by the gyroscope. It can be thought of like the variation (or standard deviation). And ARW can be seen as random, independent and distribution irrelevant.

Figure 11 shows an example of median filtering, where we see $\varphi(t)$ and Euler angles become much smoother. In the following, we use φ and γ for hijacking detection.

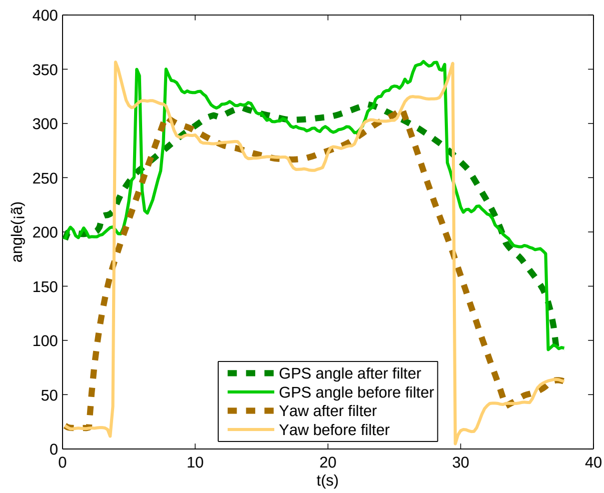
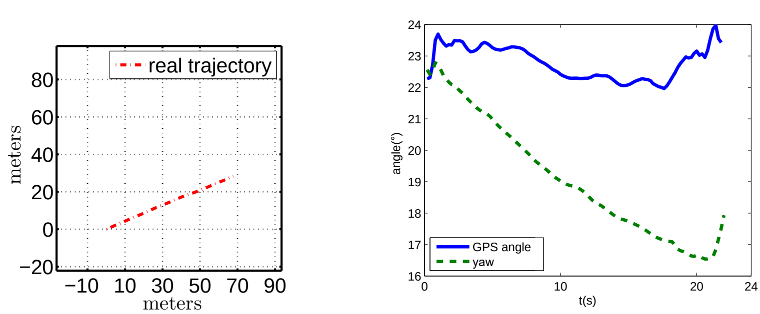


Fig. 11. The waveforms of φ and γ before and after Median Filtering

Before presenting the hijacking detection rules, we first look into some data collected from experiments with a realistic drone (the parameters of the drone and experiment methodology will be introduced in Section 5), and use these examples to motivate the design of the proposed hijacking detection rules.

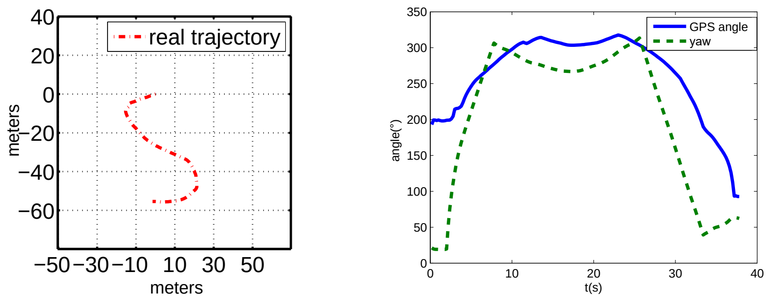


(a) Trajectory (b) GPS angle and yaw

Fig. 12. Detection rule motivating example 1.

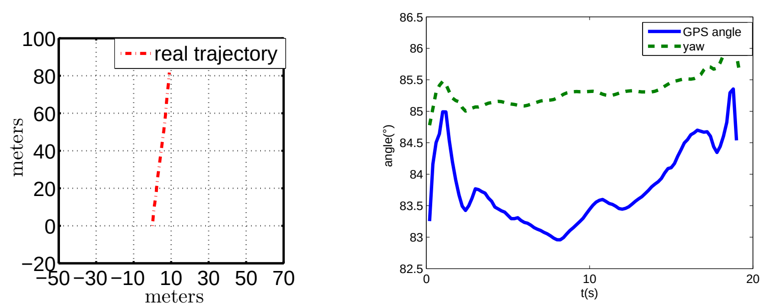
As we mentioned before, since yaw γ is the primary angle referred to the trajectory turning left or right, and GPS angle φ is calculated by GPS trajectory which also reflected on the moving forward directions (left or right). So in some way, we can assume γ and φ are the linear correlation about the trajectory variation trend. In order to compare the variation trends of these two angles, in this method, it mainly calculates the linear correlation coefficient ρ that a number represents the linear dependence. It has a value between +1 and -1, where +1 is the total positive linear correlation, 0 is no linear correlation, and -1 is the total negative linear correlation, calculated by (11).

$$\rho = \frac{cov(\varphi, \gamma)}{\sigma_\varphi \sigma_\gamma} \tag{11}$$



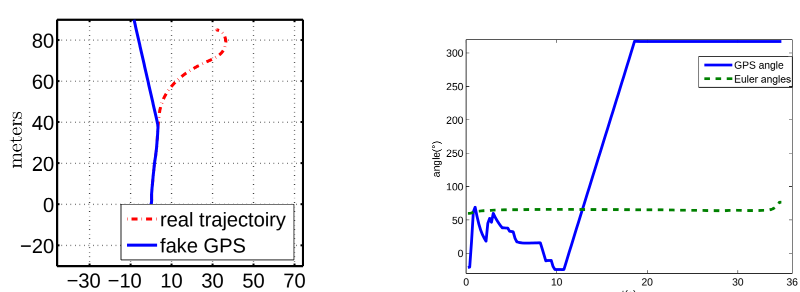
(a) Trajectory (b) GPS angle and yaw

Fig. 13. Detection rule motivating example 2.



(a) Trajectory (b) GPS angle and yaw

Fig. 14. Detection rule motivating example 3.



(a) Trajectory (b) GPS angle and Euler angles

Fig. 15. Detection rule motivating example 4.

where *cov* is the covariance function, σ_φ is the standard deviation of φ, σ_γ is the standard deviation of γ.

In the experiment of Figure 12, the drone flies normally along a straight line, where GPS angle φ and Euler angles nearly has the same variant trend. In other words, the correlation coefficient is closed to 1. So does a zigzag route, shown in Figure 13. However, only relying on the correlation coefficient may give wrong results. In the experiment of Figure 14, the drone is not hijacked, while the correlation coefficient in practice isn't close to 1 (actually is about 0.6). An interesting observation is the averages respectively of GPS angle and Euler angles are closed in the above case.

On the other hand, in the experiment of Figure 15, the drone is hijacked, where GPS angle φ and Euler angles don't have the same variant trend, and their averages aren't closed either. By the way, we planned the trajectory is a straight line, and in this experiment, the fake GPS trajectory is closed to the planned trajectory.

ALGORITHM 2: Pseudo-code of the Detecting procedure

```
1:  while not hijacked do
2:      Calculate γ(t), φ(t)in Algorithm 1
3:      Calculate linear correlation ρ(t)
4:      if ρ(t) < ε then
5:          Calculate avg(φ(t)) and avg(γ(t)) from t − N to t
6:          Calculate Δavg(t) = avg(φ(t)) − avg(γ(t))
7:          if Δavg(t) > μ then
8:              Claim hijacked; break
9:          end if
10:     else
11:         Claim non-hijacked
12:     end if
13: end while
```

By the above observations, we design the detection procedure as shown in Algorithm 2. Note that the window size N used to compute the average or the correlation coefficient is subject to the designer's choice. In all the experiments in this paper, we set $N = 100$. Correlation coefficient ε and fault tolerance μ, respectively in Line 4 and Line 7, are two thresholds set by observations, the more details will be discussed in Section 5. Moreover, the design of hijacking detection rules heavily depends on the flight control algorithm of the drone. The detection algorithm in this paper is designed with observations from experiments with a particular drone. In the future work, we may conduct experiments to different drones and study detection algorithms that are more general to a different flight control algorithms.

5 EXPERIMENTS

Experiments are conducted with a Quadrotor drone (same as [7]) shown in Figure **??**, which uses the Pixhawk™ flight control system [16]. It uses L3GD20H gyroscopes [9] and LSM303D accelerometers [12], for both of which we set the sampling rate of 50HZ (inter-sampling separation of 0.2 seconds). The drone uses the NEO-M8N GPS system [15], for which we set the data rate to 5Hz (inter-sampling separation of 0.2 seconds). Therefore, the GPS outputs are updated every 10 sampling points. The onboard micro-controller is PX4FMU [18], a 168MHz Cortex-M4F processor with 1024KB Flash and 192KB SRAM. We let the drone fly in an open space for 100 times with low speed, among which the hijacked and non-hijacked cases are half-half. For the non-hijacked cases, half of the flight routes are straight lines and half are randomly generated curves. Because of (measurement and accumulated) errors and noises especially in the Zigzag trajectory, [7] may not work well when no hijacking occurs in curve trajectory situations. In the proposed method, it doesn't need any accelerometer in the detection procedure, in other words, it reduces some measurement errors which makes the results more accuracy in some way. So in the experiment, we let the generating curve procedure be more complexity than [7], i.e. 80% curves with at least two continuous turns during a short time interval, while in [7] is no more than 50%. The hijacked cases are implemented as follows. We use an array to store the fake GPS signals on the micro-controller, and set a timer to trigger the hijacked mode, in which the GPS signal processing the program reads inputs from this array instead of from the GPS receiver. We implement our hijacking detection method on the micro-controller and modify the flight control algorithm so that the drone will land immediately when it detects hijacking.

The hijacking precision is evaluated with the metric correctness ratio α:

$$\alpha = \frac{succ}{total},$$

where $total$ is the total number of experiments, and $succ$ is the number of experiments that our method correctly judges whether the hijacking has occurred. In other words, in the hijacked case $1 - \alpha$ is the false-positive ratio while in the non-hijacked case $1 - \alpha$ is the false-negative ratio.

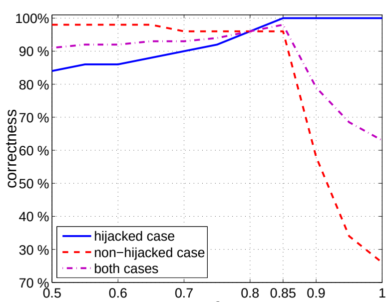


Fig. 16. The correctness vs. ε when $\mu = 10$

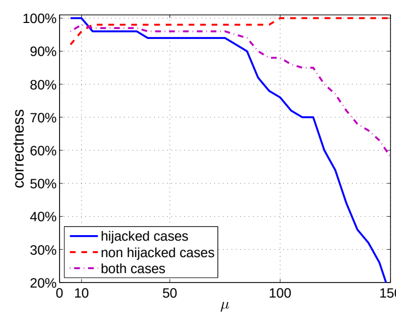


Fig. 17. The correctness vs. μ when $\varepsilon = 0.85$

The thresholds ε and μ greatly affect the correctness ratio. If ε and μ are too tight, the correctness ratio in the hijacked cases will be higher but it will be lower in the non-hijacked cases, and the other way around if ε and μ are too loose. Therefore, in the following we evaluate the correctness ratio in both hijacked and non-hijacked cases with varying ε and μ.

Figure 16 and Figure 17 show how the correctness ratio changes (for both the hijacked cases and non-hijacked cases) with one of the two thresholds while keeping another constant. In the first experiment shown in Figure 16, the success ratio in hijacked case improves as the threshold increase, while the success ratio in the non-hijacked case decreases due to the threshold is too tight for non-hijacked cases. The second experiment is shown in Figure 17, the success ration in the non-hijacked case improves as the threshold increases, while the success ratio in hijacked case decrease due to the detection condition is too loose so that more hijacked cases get fault results.

According to the above experiment results and observations, the following thresholds appear to be a good choice for our drone in this section: $\varepsilon = 0.85$ and $\mu = 10$.

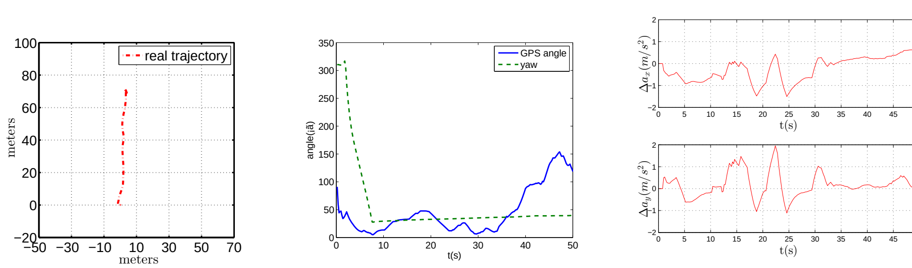
The detection accuracy of the proposed method is based on IMU sensors (such as gyro) readings, and even the same type gyros placed at the different positions of one drone, the readings are totally different during the same flight task. The proposed method is doing a comparison based on these "uncertainty" sensors readings. So to achieve a high detection accuracy, we strongly suggest users adjust the thresholds by doing several flight tests before using this method, it just like a baseline test. First, fly the drone in an open space several times, and then download the flight data. Next, slightly adjust the values of thresholds based on the values set in this paper and run the proposed method using the IMU data and GPS data offline. Finally, find the satisfied values and implement the detection method on the drone.

We also implement the straightforward approach by comparing DATE method and the proposed method, and using both methods, as shown in Table 1. It turns out that in non-hijacked cases, the

DATE method is good at straight line trajectory situations, while the proposed method is good at curve trajectory situations. The reason is that the proposed method doesn't use any accelerometer and simplify the calculation procedures, which means it reduces some errors to make the results much more accuracy especially in curves trajectory situations. However, only using gyroscopes and GPS data without accelerometers makes the proposed method has less information to get detection results and the drifting of gyroscopes brings from the slow variation of angular velocities also may decrease the results accuracy especially when no hijacking occurs in straight line trajectory situations. Therefore, using both methods to detect the drone hijacking can make the results much more accurate than using any single one. When the results of all the methods are hijacked, then the final result is hijacked, otherwise, the result is non-hijacked. For example, in this experiment, shown in Figure 18, we plan the drone to fly a straight line without hijacking, but actually, the GPS trajectory has some fluctuations around the planned trajectory, because of the wind. The proposed method gives a fault result (correlation coefficient is -0.074), while it gets the right result from DATE method (average of Δa_y is 0.10 which is closed to 0).

Table 1. Correctness ratio comparison of different methods

	non-hijacked cases (line trajectories)	non-hijacked cases (curve trajectories)	hijacked cases
our method	92%	100%	100%
DATE method	100%	84%	100%
both method	100%	100%	100%



(a) Trajectory (b) GPS angle and yaw (c) Δa_x and Δa_y in DATE method

Fig. 18. The proposed method is failed but DATA method detects successfully

6 CONCLUSIONS

This paper presents an efficient method to let a drone detect whether it has been hijacked. This method reduces some error problems with a novel approach that only uses the gyroscopes and GPS data and simplifies the calculation procedures comparing with DATE method, this is easy to be implemented on any drone. On the other hand, the accuracy of this method may not high enough comparing with DATE method in straight line trajectory situations when the drone has not been hijacked, due to the measurement and calculation error problems. So another contribution in this paper is using both DATE method and the proposed method to guarantee the high results accuracy of the GPS spoofing attacks detection. In addition, the most complex calculation procedures of both methods are based on INS, most of the variables in the proposed method can be directly taken from the operating autopilot, so the complexity of run both methods is low.

In future work, we will implement our proposed method in different types of drones, evaluate and refine the detection algorithms. Another important direction of our future work is to extend the work in this paper to anti-hijacking flight control, so that the drone can not only detect the hijacking, but also improve the flight control algorithm design to make them resilient to false or low-quality GPS signals.

ACKNOWLEDGMENTS

The work is supported by the China Scholarship Council under Grant No.: 201706080092, National Natural and Science Foundation of China under Grant No.: 61672140,61528202,61472072 and the project of the State Key Laboratory in China under Grant No.: 2017RALKFKT002.

REFERENCES

[1] Riham Altawy and Amr M Youssef. 2016. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems* 1, 2 (2016), 7.
[2] Ali Broumandan, Ali Jafarnia-Jahromi, and Gerard Lachapelle. 2015. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solutions* (2015).
[3] X. Chen, G. Lenzini, M. Martins, S. Mauw, and J. Pang. 2013. A Trust Framework for Evaluating GNSS Signal Integrity. In *2013 IEEE 26th Computer Security Foundations Symposium*. 179–192. https://doi.org/10.1109/CSF.2013.19
[4] DJI Comany 2017. DJI Comany. (2017). https://en.wikipedia.org/wiki/DJI_(company)
[5] Gabriel Hugh Elkaim, Fidelis Adhika Pradipta Lie, and Demoz Gebre-Egziabher. 2015. *Handbook of Unmanned Aerial Vehicles*. Springer Netherlands, Chapter Principles of Guidance, Navigation, and Control of UAVs.
[6] S. Daneshmand et al. 2014. A GNSS structural interference mitigation technique using antenna array processing. In *2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop*. 109–112. https://doi.org/10.1109/SAM.2014.6882352
[7] Zhiwei Feng, Nan Guan, Mingsong Lv, Weichen Liu, Qingxu Deng, Xue Liu, and Wang Yi. 2017. Efficient drone hijacking detection using onboard motion sensors. 1414–1419. https://doi.org/10.23919/DATE.2017.7927214
[8] S. Khanafseh, N. Roshan, S. Langel, F. C. Chan, M. Joerger, and B. Pervan. 2014. GPS spoofing detection using RAIM with INS coupling. In *2014 IEEE/ION Position, Location and Navigation Symposium*. 1232–1239. https://doi.org/10.1109/PLANS.2014.6851498
[9] L3GD20H gyroscopes 2017. L3GD20H gyroscopes. (2017). http://www.st.com/web/catalog/sense-power/FM89/SC1288/PF254039
[10] Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Isaac Miller. 2010. An in-line anti-spoofing device for legacy civil GPS receivers. *Institute of Navigation - International Technical Meeting 2010, ITM 2010* 2 (2010), 868 – 882.
[11] Wenjing Liang. 2017. *Attitude Estimation of Quadcopter through Extended Kalman Filter*. Ph.D. Dissertation. Lehigh University.
[12] LSM303D accelerometers 2017. LSM303D accelerometers. (2017). https://www.pololu.com/product/2127
[13] Joshua Mead, Christophe Bobda, and Taylor J. L. Whitaker. 2016. Defeating drone jamming with hardware sandboxing. In *2016 IEEE Asian Hardware-Oriented Security and Trust, AsianHOST 2016, Yilan, Taiwan, December 19-20, 2016*. 1–6.
[14] Wilbur L Myrick, Michael Picciolo, J Scott Goldstein, and Vernon Joyner. 2015. Multistage anti-spoof GPS interference correlator (MAGIC). In *IEEE Military Communications Conference*. IEEE, 1497–1502.
[15] NEO-M8N GPS system 2017. NEO-M8N GPS system. (2017). https://www.u-blox.com/en/product/neo-m8qm8m-series
[16] PIXHAWK 2017. PIXHAWK Project. (2017). https://pixhawk.org/
[17] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon. 2013. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. *Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation* (2013), 2949–2991.
[18] Px4fmu 2017. Px4fmu autopilot/flight management unit. (2017). https://pixhawk.org/modules/px4fmu
[19] Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun. 2016. SPREE: Spoofing Resistant GPS Receiver. *arXiv preprint arXiv:1603.05462* (2016).
[20] Çağatay Tanıl, Samer Khanafseh, and Boris Pervan. 2017. Detecting Global Navigation Satellite System Spoofing Using Inertial Sensing of Aircraft Disturbance. *Journal of Guidance, Control, and Dynamics* (2017).
[21] Brian P Tice. 1991. Unmanned aerial vehicles: The force multiplier of the 1990s. *Airpower Journal* (1991), 41–54.
[22] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 75–86.
[23] L.A. van Mastrigt, A.J. van der Wal, and P.J. Oonincx. 2015. Exploiting the Doppler effect in GPS to monitor signal integrity and to detect spoofing. *2015 International Association of Institutes of Navigation World Congress (IAIN)*, 8 pp. –.

http://dx.doi.org/10.1109/IAIN.2015.7352259
[24] Jon S Warner and Roger G Johnston. 2002. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of Security Administration* 25, 2 (2002), 19–27.
[25] Dingbo Yuan, Hong Li, and Mingquan Lu. 2014. GNSS spoofing mitigation based on joint detection of code doppler and carrier doppler in acquisition. In *China Satellite Navigation Conference (CSNC) 2014 Proceedings: Volume I*. Springer, 763–774.
[26] Dingbo Yuan, Hong Li, and Mingquan Lu. 2014. A method for GNSS spoofing detection based on sequential probability ratio test. In *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*. IEEE, 351–358.