IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 January 2024, accepted 23 March 2024, date of publication 27 March 2024, date of current version 3 April 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3382543*

RESEARCH ARTICLE

# An Analysis of GPS Spoofing Attack and Efficient Approach to Spoofing Detection in PX4

**JI HYUK JUNG, MI YEON HONG, HYEONGJUN CHOI, AND JI WON YOON**
School of Cybersecurity, Korea University, Seoul 02841, South Korea

Corresponding author: Ji Won Yoon (jiwon_yoon@korea.ac.kr)

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea Government Ministry of Science and ICT (MSIT) (No.2020-0-00913, Study on Wireless Covert Channel Risk Verification.

**ABSTRACT** Unmanned Aerial Vehicles (UAVs) are aerial vehicles that can go to a particular position without human control or with remote human control. It is because unmanned control mainly relies on position estimation that a lot of research has been studied on GPS spoofing attacks. Detection methods against GPS spoofing attacks mainly include monitoring RF signals or IMU sensor values inside UAVs. In this work, we analyze GPS attack and detection in an advanced autopilot system, PX4 without excluding RF detection. Recent studies have shown that GPS spoofing is unable to evade the detection using EKF sensor fusion. Therefore, this paper experiment whether the detection could be evaded by strengthening the attacker model. This paper classifies attacker models according to whether an attacker knows the true position of UAVs or the estimated position by UAV and proposed attack methods depending on each model in PX4. We inject GPS value which our attack method intends to UAV during mission flight in simulation environment. By manipulating the GPS driver code of PX4 controller, we inject GPS value the attack method wants into UAV in physical environment. Finally, we observed the innovation test ratio during GPS spoofing and demonstrate that GPS spoofing attack is possible keeping the innovation test ratio under the anomaly detection criterion. After that, we proposed our approach which scales the EKF's Kalman gain randomly to increase the detection method's efficiency and experiment with the attack methods. This detection method has little effect on the test ratio without the attack. But during the attack, the innovation test ratio was increased higher than the anomaly detection criterion so that the attack could be detected.

**INDEX TERMS** Detection, GPS spoofing attack, position estimation, PX4, UAV.

## I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) are used in many fields like the military, agriculture, geography, and commerce. The reason UAVs are used in many of these applications is based on the fact that UAVs can go to dangerous or high places without human and human control. This capability of UAVs mainly depends on Global Positioning System (GPS) technology, other sensors like Inertial Measurement Unit (IMU), and an advanced control system. Because UAV's position estimation is a core factor in unmanned control, there are a lot of research about the attack and defense on this positioning function. Especially, GPS spoofing attack are focused on due to the importance of positioning function and the property of GPS signal, which is unencrypted and one-way radio signal. Although [1], [2], [3], [4] proposed to use the encryption or radio signal's strength and direcion for countermeasure, there are vulnerable to a deliberate attacker. Considering these limits, many studies have made efforts to detect spoofing using UAV's internal sensor data which is very difficult for an attacker to access [5], [6]. Many researchers have studied detection method against GPS attacks, and on the other side, GPS attacks against the detection have also been proposed. However, most of the research has focused on the detection techniques, and the research on attack methodologies has not been conducted strictly. Conversely, the research focusing on GPS attack on UAV often are conducted ignoring the detection. References [7] and [8] proposed an attack methodology in commercial UAVs, it mainly focused on GPS spoofing

The associate editor coordinating the review of this manuscript and approving it for publication was Bidyadhar Subudhi.

attack in the absence of any detection techniques. A study of GPS attacks to bypass detection techniques experiments in the theoretically modeled system and assuming the attack model that can access to the internal system state [9], [10]. Reflecting these issues, this paper examines whether GPS attacks are possible in the presence of a strict detection model of widely used UAV system and studies countermeasures.

PX4 is an autopilot system developed by industry and academia. This autopilot system consists of several modules which include control, estimation (EKF Sensor Fusion), communication, and so on. References [5], [6], [11], [12], and [13] have proposed methods to defend GPS spoofing by experimenting with PX4. However, attack models and methods have not been systematically classified and proposed for PX4, and there was no in-depth analysis regarding the detection of GPS spoofing attacks using EKF sensor fusion.

In this paper, we design attacker models for PX4 and proceed with experiments of each attacker model to analyze the results. We validate how secure PX4 is against each attacker model and propose a detection method. In this paper, we study mainly GPS spoofing attacks and detection related to the position estimation in PX4 assuming an attacker can transmit any GPS signal to UAV. In this work, the contribution is as follows.

- We analyzed the possibility of GPS spoofing attack against the detection system which use EKF sensor fusion.
- Assuming that an attacker took control of the RF signal, we classified attacker models according to how much information an attacker has access to UAV and the proposed attack method respectively.
- We analyzed our attack method in the simulation and real environment and proposed a detection method for our attack.

## II. BACKGROUND

### A. GPS SPOOFING ATTACK AND DEFENSE

In the navigation system, there are two main methods that estimate the position of the vehicle. One is Inertial Navigation System (INS) and the other is the GPS. UAVs estimate position using both GPS and INS. Commercial UAVs mainly rely on GPS because of INS's low precision. Of course, There is INS with high precision but it is very expensive. Since GPS is one-way communication and has no security protocol, it is convenient to use but vulnerable to spoofing attacks. GPS's importance in UAV and security vulnerability led many researchers to study GPS Spoofing attack and defense. In GPS spoofing attack, the attacker transmits a stronger fake signal than a satellite's legitimate signal and deceives the receiver [14]. In most studies, the concept of defending against these spoofing attacks corresponds mainly to detecting spoofing signals. Of course, the concept of defense can even be said to detect and receive legitimate signals [11]. This paper focuses on detection methods as a countermeasure to spoofing attacks.

There are two most representative spoofing detection methods. One is using the GPS signal's strength or directionality [15]. The other is continuously detecting attacks using the position estimated from the IMU sensor (Inertial Navigation System) [16], [17]. In the detection method using RF, there is still a possibility that external attackers interfere and detection of RF equipment is relatively expensive in small UAVs. Namely, external signals must have a vulnerability to attacker interference by nature. Therefore, detecting only in UAV's internal will be the simplest and most complete. In this paper, we experimented with the assumption that an attacker can transmit any signal to UAVs at the RF layer and we only focus on detecting attacks using UAV's internal structure.

### B. EKF SENSOR FUSION

Kalman filter is used for estimating the true value from the observation from sensors. The basic framework of the Kalman filter consists of predicting the current state using the previously estimated state and then correcting the predicted current state using the observed sensor value. EKF is an extension of the Kalman filter to the non-linear domain. Sensor fusion refers to combining multiple sensor sources to more accurately estimate. Most UAVs estimate the UAV's state by combining sensor values through EKF sensor fusion [17], [18]. The number of states processed by PX4's EKF is a total of 24. For example, Quaternions (rotation from body to nav frame), NED (North, East, Down) Position, and NED Velocity are processed by UAV's EKF system. In EKF sensor fusion, the position states are estimated when the IMU sensor or GPS sensor is updated. A simple description of this process is as algorithm 1. $P$, $V$, and $K$ mean estimated position, velocity, and Kalman gain respectively. The $var$, $ino$, $cov$ and are variance, innovation, and covariance respectively. Innovation means the difference between the previous estimate and the observed value. In the IMU update, the IMU sensor can only measure acceleration, so the speed and position are predicted using the integration of acceleration. In GPS update, without the need for an integration process, the value observed from the GPS sensor is reflected on the estimated value using the difference between the current estimated value and the observed value.

**Algorithm 1** EKF Sensor Fusion (IMU, GPS)

```
while True do
    Update covariance
    if IMU is updated then
        $P_{cur} \leftarrow P_{pre} + V_{cur} \times (t_{cur} - t_{pre})$
    else if GPS is updated then
        $K_{fusion} \leftarrow cov_{pos} \times var_{gps}$
        $P_{cur} \leftarrow P_{pre} + ino_{gps} \times K_{fusion}$
    else
        pass
    end if
end while
```

### C. GPS SPOOFING ATTACK DETECTION IN PX4

As mentioned earlier, this paper assumed that an attacker could have all control in the RF layer. Thus, the detection of the attack only depends on using UAV's internal system like the IMU sensor, and EKF algorithm. Many works [5], [6], [12], [16], [17], [19] have been conducted on the detection of GPS spoofing attacks using the estimated by IMU sensor or machine learning. Currently, PX4 has a function that does not reflect the position observed by GPS if there is a difference between the position estimated by EKF (mainly using IMU) and the position observed by GPS above a certain level. Especially, the latest detecting methodology [11], [20], [21] directly used the EKF sensor fusion algorithm to detect spoofing attacks. The innovation test ratio which refers to the degree of difference between the measured sensor value and the estimated value can be a criterion in the spoofing detection and updated every sensor fusion. For example, if the innovation test ratio exceeds the predefined threshold during a certain period, UAVs can assume that the spoofing attack progressed. The innovation test ratio is calculated in PX4 as follows. The innovation gate is a scale parameter for monitoring Innovation's consistency. Increasing this parameter reduces the test ratio, so even if the innovation test ratio is large, it can pass certain criteria,

$$TestRatio = Innov/(Var\ of\ \ Innov) \times (Innov\,Gate). \tag{1}$$

## III. PROPOSED APPROACH

In this work, we classified attack models and proposed ways to increase the efficiency of detection for the attack models. Contrary to the complete control attack [21], the primary goal of the attack models in our work is to change only the final destination. We suppose UAVs move to a target position. UAVs stop when the estimated position equals the target position. The error accumulated by the attacker in UAV's EKF estimation. The summation of the EKF estimation error during the entire UAV's mission is eventually reflected as a change in the UAV's position. Eventually, however, the ground truth position of the UAV is not the position of the target, but the position that the attacker wants.

**Algorithm 2** UAV Mission Model

```
$MissionStart$
while $True$ do
    $UAV\ Move\ to\ \ TargetPosition$
    $Position\ Estimation$
    if $EstimatedPosition$ is $TargetPosition$ then
        $break$
    end if
end while
$MissionEnd, Hold$
```

To represent our attacker's goal mathematically, we simply define the fuseGPS function as follows. This function receives the previously estimated value and the measured sensor value as input and outputs the current estimated value using the sensor fusion algorithm

$$est_t = fuseGPS(est_{t-\Delta t}, s_t) \tag{2}$$

, where $est_t$ is the estimated position of UAV at time $t$. $s_t$ is the sensor value at time $t$ which contains GPS information.

$$ERR(t) = est_{t-\Delta t} + \Delta pos_{true} - fuseGPS(est_{t-\Delta t}, s_t)$$
$$P_{fianl} \cong P_{target} - \sum_{t=0}^{t=T} ERR(t) \tag{3}$$

In figure 1, we represent each attack model in this paper. The most basic premise is that attack models have unlimited control at the RF layer. Each model is classified according to how much information about UAVs they can access. After that, we propose a method of attacking PX4 according to each model. The summary of the attacker's goals and conditions is as follows.

- The goal of the attacker is to accumulate errors during the UAV's mission and change the final position.
- GPS value transmitted by UAV can be manipulated at the attacker's will without any detection in the RF layer.
- The attack should be carried out by keeping the invocation ratio as low as possible in the UAV's GPS fusion (In this paper, the criterion for attack detection was set at 0.5).

In particular, in order to meet the third condition, the attacker must continuously predict the position estimated by the UAV. Because the estimated position considerably differs from the true position because of the accumulation of errors by the attacker, the attack method should be designed under this condition.

### A. BLACK BOX ATTACK

This model assumes that GPS spoofing attacker can not estimate the exact position of the UAV in real-time. In PX4, if the innovation test ratio is high during the GPS sensor fusion, the GPS sensor's information is not reflected in the position estimation. However, if the fusion is rejected for a certain period of time, UAV resets the position using the GPS information without any verification. Therefore, the attacker continues to transmit a spoofing signal that makes the test ratio high in EKF estimation to induce the UAV to reset its positioning. We proposed the following algorithm.

**Algorithm 3** Black Box GPS Spoofing Attack

```
$ResetTime \leftarrow time()$
for $t = 0$ to $T$ do
    $CurruntTime \leftarrow time()$
    if $ResetTime - CurruntTime$ is $ResetInterval$ then
        $Transmit\ sig_{reset}$
        $ResetTime \leftarrow CurruntTime$
    end if
    $Transmit\ sig_{rejected}$
end for
```

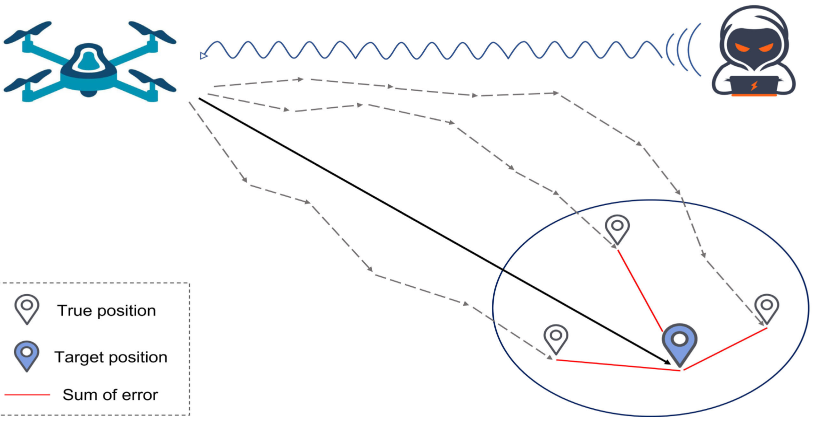

**FIGURE 1.** Our attack model's goal.

Algorithm 3 is the most basic form of black box attack, and it is possible to be transformed. In algorithm 3, *time*() outputs the current time. This attack method is possible to change the UAV's position, but the invocation test ratio should be kept at more than 1 for a certain time so that the third condition is not satisfied.

### B. WHITE BOX ATTACK

In a White box attack, the attacker can access the internal state of the UAV so that the estimated position of the UAV can be obtained. This assumption is the most powerful but practically impossible. However, most papers mainly assume these models when demonstrating spoofing attacks mathematically [9], [22]. Since the attacker can know the position estimated by UAV, the attacker can simply calculate the GPS value of which the innovation test ratio is below a certain ratio. The basic form of the attack method is as algorithm 4. *TestRatio* outputs the innovation test ratio of two inputs.

**Algorithm 4** White Box GPS Spoofing Attack

```
for $k = 0$ to $N$ do
    $Choose\ sig_k \in \{X|TestRatio(est_{k-1}, X) < 1\}$
    $transmit\ sig_k$
end for
```

### C. GRAY BOX ATTACK

Gray box attack assumes that an attacker can estimate accurately UAV's true position but can not know the internal states such as the covariance of EKF required to accurately predict the estimated position by UAV's EKF. Recent or future UAV tracking systems or tailgating UAV [23] enable this model to be the most powerful and possible in the real world. EKF constantly calculates the innovation test ratio using the estimated position of the previous step. For spoofing without being detected by UAV, an attacker should estimate the GPS position value that outputs the test ratio below a certain level in UAV's EKF estimation. Therefore, this attack model should predict the UAV's estimated position using the true position of the UAV continuously. In this work, we roughly predict the estimated position and accumulate errors in the UAV seamlessly using the following algorithm 5. The true position change is used for the change of the position estimated by the UAV's IMU, and the change by the attacker's GPS spoofing is calculated by roughly estimated Kalman gain. In this paper, the attack was successful when we set Kalman gain in a certain range.

**Algorithm 5** Gray Box GPS Spoofing Attack

```
for $k = 0$ to $N$ do
    $Est_{t_k} \leftarrow Est_{t_{k-1}} + (P_{t_k} - P_{t_{k-1}}) + EstIno$
    $Choose\ Error_t\ in\ \{X|TestRatio(est_{t-\Delta t}, X) < 1\}$
    $sig_{t_k} \leftarrow Est_{t_k} + Error_{t_k}$
    $transmit\ sig_t$
    $EstIno \leftarrow Error_{t_k} \times Kalman\ Gain$
end for
```

### D. DETECTION METHOD

In this work, we proposed a method for increasing the efficiency of detection in gray box attacks. Because of the assumption that an attacker in the gray box model knows the observed values from the outside of the UAV like the true position, the UAV generates its internal process that the attacker can not predict. Through this process, UAVs can predict the results reflected by this process, but an attacker does not know this reflection. According to our observations, there was no significant variance of PX4's Kalman gain in GPS fusion, which enables the attacker to predict the position by estimated by UAV. Therefore, we propose making Kalman gain fluctuate continuously by multiplying a random value to make it difficult for an attacker to predict the estimated position at every GPS fusion.

## IV. EXPERIMENTS

For each attack model situation, an attacker injects GPS value using the actual position or internal estimated position of the

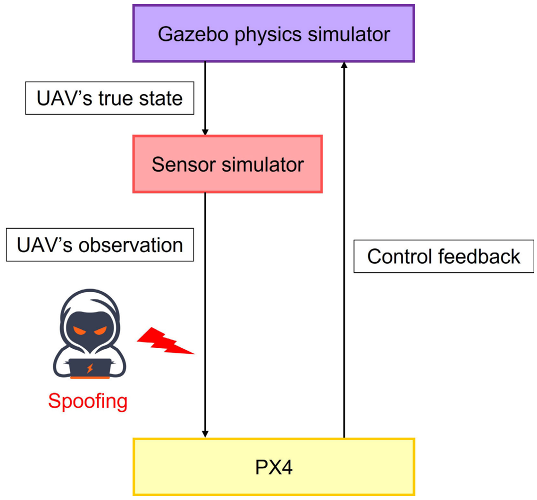

**FIGURE 2.** Simulation environment.

UAV. In the simulation experiment, the actual position of the UAV could be obtained from the Gazebo environment and the estimated position could be also obtained in PX4. After that, the UAV estimates its own position using the injected GPS. In the physical environment, PX4's real GPS sensor could be used for the actual position and obtained from the GPS driver. This value is assumed as the actual location of the observation through radar or tailgating in the gray attacker model. The estimated positions are obtained in the same way as simulation experiments.

In our experiments, we find out the attacker can change the UAV's final position when our spoofing attack is performed during the UAV movement to a target location. In each model, we calculate the position to transmit depending on each attack algorithm from the UAV's actual or estimated position and inject it into the UAV. During this process, we measured the innovation test ratio during GPS fusion which is the standard for anomaly detection.

## A. SIMULATION

We simulate the X500 model in the Gazebo environment as shown in figure 2. The Gazebo environment provides an accurate physical environment like the physical state resulting from the UAV's action. The sensor simulator receives the observed state from the physical simulator, adds gaussian noise to the observed state like a real sensor, and delivers it to the UAV.

### 1) BLACK BOX ATTACK

We experiment with an attack in which an attacker does not know the UAV's position in a simulation environment. Figure 3 demonstrates the mission's path (solid line, orange) and the true path (dotted line, purple) of the UAV during this attack. In figure 4, it can be seen that the estimated position equals the position received by the attacker every certain period because of the reset position function in PX4. This experiment shows that it is possible to move the UAV to wherever an attacker wants, but the innovation test ratio is large enough to be detected.

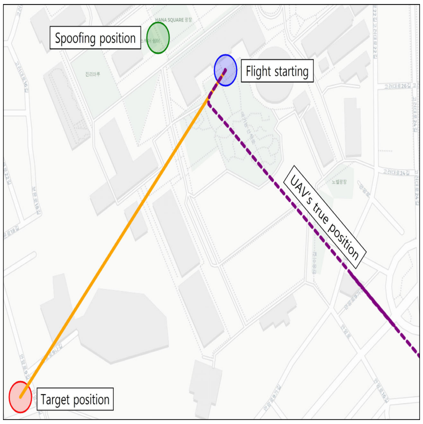

**FIGURE 3.** UAV's mission route and true route during black box attack.

### 2) GRAY BOX ATTACK

An attacker must be able to constantly predict the estimated UAV in order to spoof the GPS signal. In this experiment, it is assumed that the change of the UAV's estimated position by other sensors like IMU can be corrected to some extent using the position change from the actual position. Therefore, it is important to correct the change of the estimated position by GPS spoofing. The states of the estimated position by UAV during the attack are simply summarized as follows.

$$\begin{aligned} att(t) &= att(t-\Delta t) + \Delta pos_{true} + \hat{K} \times error(t-\Delta t) \\ spoof(t) &= att(t) + error(t) \\ est(t) &= est(t-\Delta t) + \Delta pos_{true} + K \times (spoof(t) \\ &\quad - (est(t-\Delta t) + \Delta pos_{true})) \end{aligned} \tag{4}$$

where $est(t)$ is the estimated position of UAV at time $t$. $att(t)$ is the position where an attacker predicts the estimated position. An attacker added the error to $spoof(t)$ for changing the final position of the UAV. $K$ and $\hat{K}$ are the UAV's Kalman gain and the Kalman gain predicted by an attacker. It is assumed that the change of the estimated position by the IMU sensor is the same as the change of the actual observed position, as which we represents $\Delta pos_{true}$. $\hat{K} \times error(t-\Delta t)$ is the correction for the change by $error(t-\Delta t)$ in $att(t-\Delta t)$. The inertial estimation ($\Delta pos_{true}$) is removed in the equation so that we only consider about the error by spoofing injection for observing the change of the difference between $att(t)$ and $ett(t)$. The maximal difference theoretically diverges or converges according to the rate of $(K - \hat{K}) \times error$ and $K \times (att(t) - est(t)$. The difference between $att(t)$ and $est(t)$ converge because Kalman gain is mainly less than 1 in the PX4 setting. When est(t) is obtained, the innovation ratio test is calculated through $(spoof(t) - (est(t - \Delta t) + \Delta pos_{true})$ which equals $(att(t-\Delta t) - (est(t-\Delta t) + error(t))$. Figure 5 shows the result of the simulation using python script and how the difference changes depending on the state of $K$ and $\hat{K}$

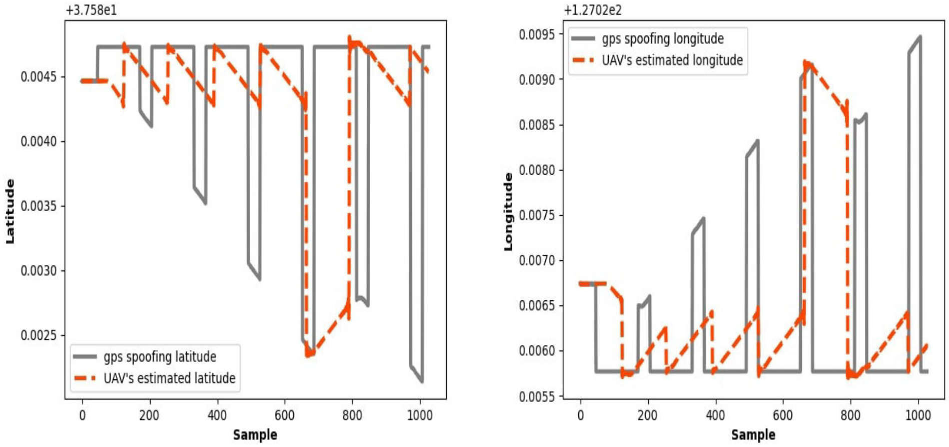

**FIGURE 4.** **(a): Received(gray) and estimated(orange) latitude according to attack (b): Received(gray) and estimated(orange) longitude according to attack.**

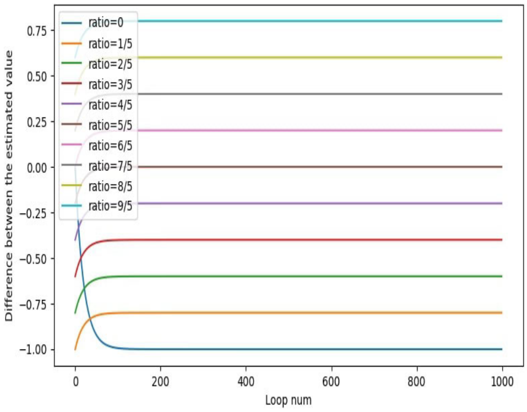

**FIGURE 5.** **The attack simulation in Python simulation for observing the difference between the position estimated by UAV and the position estimated by an attacker as the predicted Kalman gain changes.**

with *error* and *pos* set to a constant 1 and random number respectively. This result shows that the difference converges to $(\frac{\hat{T}}{T} - 1) \times error$.

Figure 6 displays the UAV's true route and mission route during the attack in which an attacker can know the UAV's true position. Figure 6 (a) and (b) are the results of attacking using the Kalman gain with 0.06 and 0.1 respectively (0.06 is good for attack, 0.1 is for comparison).

The innovation test ratio during the attack is shown in figure 7 when using the Kalman gain from 0.01 to 0.1. The results of this experiment show that the spoofing attack can be carried out with the innovation test ratio kept below a certain value although an attacker estimates the UAV's Kalman gain approximately. However, if the Kalman gain predicted by the attacker is out of a certain level (over 0.09), the attack can be failed. The innovation test ratio is calculated from the sum of the difference between the estimated positions and error, $((\frac{\hat{T}}{T}) \times error)$. In PX4, Kalman gain was between 0.06 and 0.07. The innovation test ratio will be obtained approximately $1.5 \times error$ when an attacker predicts the Kalman gain as 0.09.

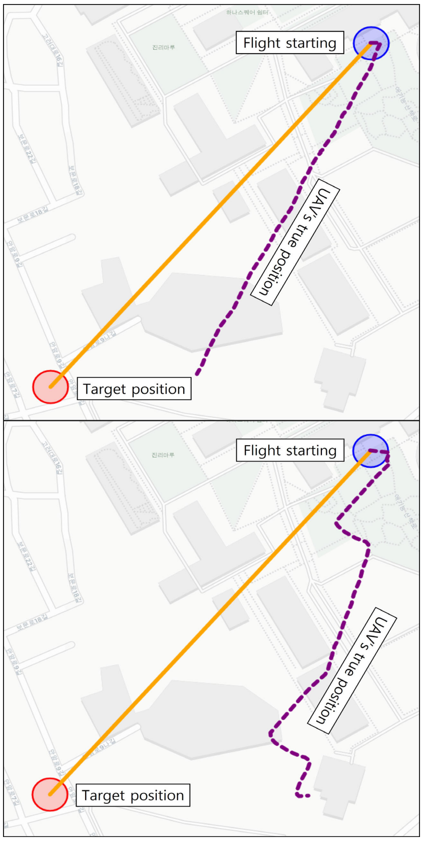

**FIGURE 6.** **(a): The result of the UAV's route attacking using the estimated Kalman gain with 0.06. (b): The result of UAV's route attacking using the estimated Kalman gain with 0.1.**

Assuming that an error is given constant, it can be seen that the stealthy attack depends on the predicted Kalman gain.

### 3) DETECTION

In this experiment, we analyzed how much the innovation test ratio was affected when Kalman gain was randomly changed for each fusion without the attacker knowing. Figure 8 and

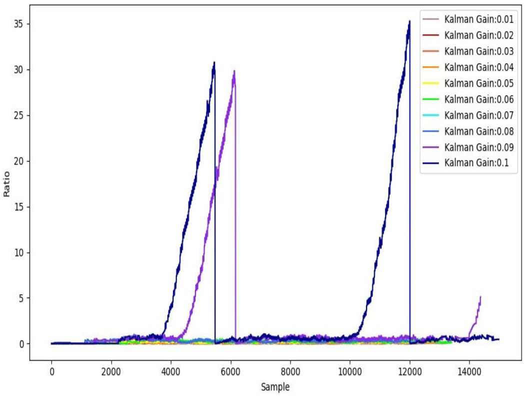

**FIGURE 7.** The results of innovation test ratio attacking using the estimated Kalman gain from 0.01 and 0.1.

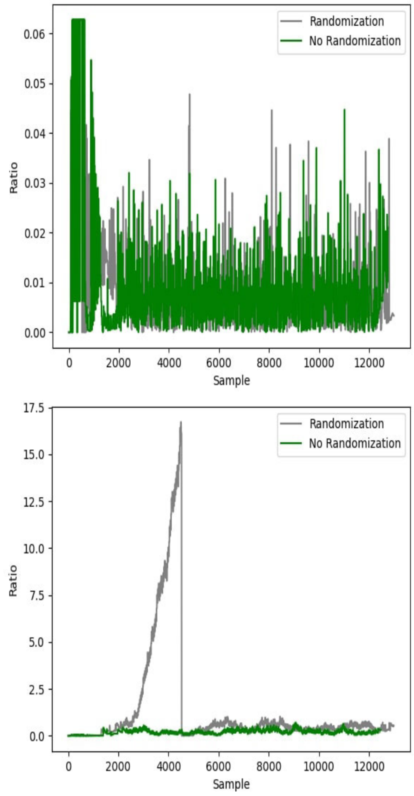

**FIGURE 8.** (a): The results of innovation test ratio without and with randomization Kalman gain. (b): The results of innovation test ratio without and with randomization Kalman gain during the attack.

table 1 show that randomized Kalman gain has a small effect on the innovation test ratio in the absence of an attack, but greatly increases the test ratio value in the presence of an attacker. In table 1, when calculating the average and maximum values, the ratio exceeding 1 was excluded because PX4 doesn't reflect the position received by GPS that outputs the test ratio exceeding 1.

### B. PHYSICAL RESULT

Pixhawk4 is a flight controller in which there are all sensors including the IMU sensor and PX4 software is implemented.

**TABLE 1.** The randomization's effect on the max and mean value of the innovation test ratio during movement of the specific route without and with the attack in a simulation environment.

| Attack | Randomization | Max of Test Ratio | Mean of Test Ratio |
|---|---|---|---|
| X | X | 0.062 | 0.0092 |
| X | O | 0.062 | 0.0098 |
| O | X | 0.7 | 0.2 |
| O | O | 1 | 0.39 |

**TABLE 2.** The randomization's effect on the max and mean value of the innovation test ratio during movement of the specific route without and with the attack in a real environment.

| Attack | Randomization | Max of Test Ratio | Mean of Test Ratio |
|---|---|---|---|
| X | X | 0.0051 | 0.0002 |
| X | O | 0.0112 | 0.0006 |
| O | X | 0.0028 | 0.002 |
| O | O | 1 | 0.12 |

Figure 9 (left) shows the gray box attack model of this paper, and the right shows the real experimental design to experiment with the attack model. To verify the attack model of this paper in a real-world environment, we inject the spoofing data using the position obtained through the GPS driver while moving pixhawk4. This injecting environment is equivalent to the attack model in which an attacker knows the UAV's true position described in the gray box attack. This assumption of equivalent is similarly used in [24] and [23]. Experiments using real sensors were verified only in the gray box model because white box attacks or black box attacks are almost difficult or inevitably detectable in real environments.

This experiment observed how much the estimated position by the real controller could differ from the true position of the controller and analyzed the innovation test ratio during the attack to verify if the attack is possible. Additionally, to assess the efficacy of the proposed detection method (randomization Kalman gain) delineated within this paper, we conducted experiments encompassing four distinct situations: one without attacks or one without detection method, another one with attacks or one with detection method. In this experiment, the Kalman gain value of 0.06, which was well attacked in the simulation, was used and the variance of randomization of Kalman gain ranged from 0.01 to 1.

Figure 10 represents the estimated location (green line) of pixhawk4 with and without attack in the real environment and figure 11 shows the innovation test ratio of each attack environment. As shown in figure 11, there was not much difference between test ratios measured with or without randomized Kalman gain in the absence of an attack. On the contrary, there was a significant difference between innovation test ratios measured with or without randomized Kalman gain in the presence of an attack.

## V. DISCUSSION

In the experiment of this paper, it was shown that UAV equipped with PX4 could be moved anywhere although an

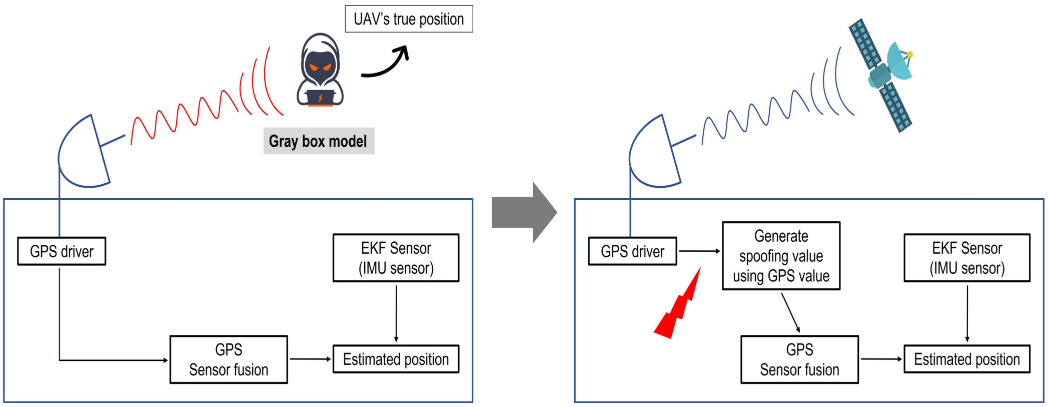

**FIGURE 9.** Experimental setup for real environment.

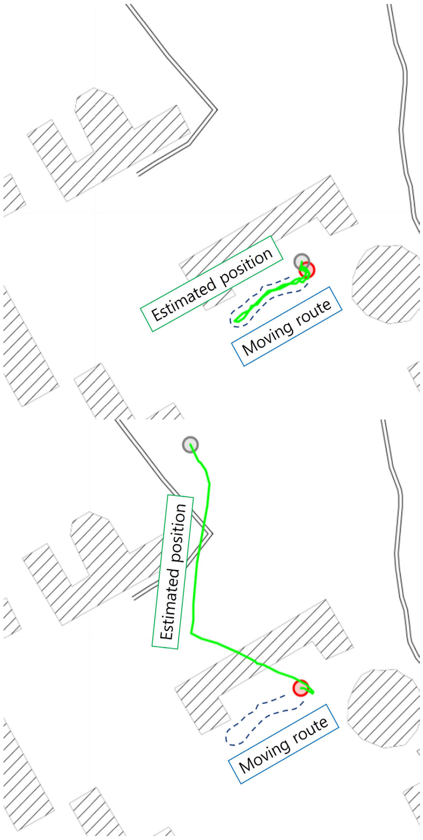

**FIGURE 10.** (a): Estimated position during movement of the specific route without attack in a real environment. (b): Estimated position during movement of the specific route with the attack in a real environment.

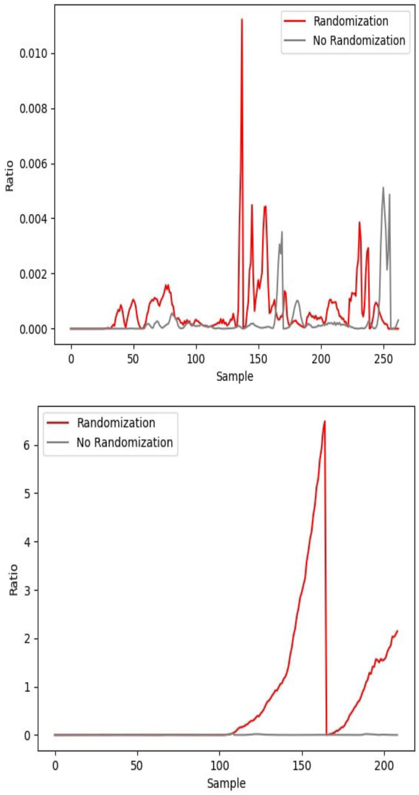

**FIGURE 11.** (a): The results of innovation test ratio without and with randomization Kalman gain in a real environment. (b): The results of innovation test ratio without and with randomization Kalman gain during an attack in real environment.

attacker has any information related to UAV's position (black box model). This attack is based on the reset position function of PX4. However, in order to spoof the UAV based on the reset position, the test ratio must exceed 1 during a certain period of time. Therefore, detecting this type of attack is not as difficult as detecting GPS jamming for UAVs. Black box attack by reset position has clear limitations.

Most research about detecting GPS spoofing assumed the attack model based on the black box model. However, these attack model is simply detected by comparing estimated values using other sensors like IMU sensor (EKF sensor fusion). The difficulty of GPS spoofing against EKF sensor fusion detection is that the estimated position must be constantly estimated during the mission flight.

However, we show that the attacker tracking the true position of the UAV can attack without being detected. The possibility for the stealthy attack is based on the facts that an attacker can correct the change of estimated position by UAV's movement using the UAV's actual position and the change of UAV's estimated position by GPS spoofing. As we can see in fig. 5, even if the Kalman gain is not accurately predicted, the change during GPS sensor fusion does not always diverge so that can be estimated within a certain value by an attacker. So, the attacker can approximately predict the estimated position using the UAV's true position. The efficiency of the stealthy attack proposed in this paper depends on the innovation test ratio value in PX4. If the innovation test ratio is large, an attacker can more freely adjust the range of attack values. On the contrary, if the test ratio is kept small to defend this, the UAV will respond to general gaussian noise and cause an EKF error. Therefore, the important metrics is the innovation test ratio in the spoofing attack and detection. In detection experiments, we show that randomized Kalman gain has no effect on the innovation test ratio when there is no attacker, and has an effect when there is an attacker. This sufficiently enables detecting the strongest model in PX4. Although this paper proposed the methodology, it is also possible to consider using other random processes. From the attacker's point of view, it can be transmitted by changing the velocity or attitude. However, the attacker's ultimate goal in this experiment is to change the position of the UAV. In addition, unlike position measurement, the velocity or attitude of the UAV is measured by using the Doppler effect. it is impossible for the attacker to spoof. Therefore, in this experiment, it is assumed that the velocity or attitude of the UAV can not be spoofed. From UAV's point of view, EKF sensor fusion already estimated the position using all the information containing the velocity and attitude. There was no need to add velocity or attitude to the detection separately. There will be multi-dimensional cases or possibilities for attacks. For example, [8] safely hijacking the UAV's using EKF failsafe. Other research [21] shown that spoofing can be used to control UAV's velocity. But these are based on GPS spoofing attack. This paper concentrated on the contents which discuss the possibility of the GPS spoofing attack against anomaly detection and the anomaly detection algorithm against the attack. The research on stealthy GPS attack that evades anomaly detection was mainly approached mathematically, and the attacker model was a powerful attacker model with access to UAV's internal sensor values. But it is almost impossible in real-world. Therefore, our paper has shown that detection can be avoided by using a more realistic attack model which uses only UAV's position information.

## VI. CONCLUSION

Recent technological advances have created many security threats, and many countermeasures have been studied [25], [26], [27]. This paper studies the attack and detection techniques of UAV among these cybersecurity threats. To date, recent papers have not classified attack models and explicitly presented attack methods with respect to EKF sensor fusion's spoofing detection in PX4. Especially, the recent spoofing detection for PX4 mainly depends on machine learning [5], [6], [12]. In this paper, we classified the attack model and analyzed attack methods avoiding EKF sensor fusion detection in PX4. In addition, we proposed methods to increase the efficiency of detection for attacks. This paper manipulates GPS receive driver of PX4 to design the attacker who can know the position of the UAV. Although this design of experiment is sufficient to analyze EKF sensor fusion of PX4 and GPS spoofing attacks in the real world, future works will be necessary to experiment with the real UAV tracking system. Although this paper mainly analyzed only attacks on position for some reasons, but anomaly detection of velocity and attitude is also a subject to be researched.

## REFERENCES

[1] X.-J. Cheng, J.-N. Xu, K.-J. Cao, and J. Wang, "An authenticity verification scheme based on hidden messages for current civilian GPS signals," in *Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, Nov. 2009, pp. 345–352.

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

[3] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," in *Proc. Int. Tech. Meeting Inst. Navigat.*, 2016, pp. 181–192.

[4] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[5] R. A. Agyapong, M. Nabil, A.-R. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2021, pp. 1–8.

[6] M. Nayfeh, Y. Li, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification," *Comput. Secur.*, vol. 126, Mar. 2023, Art. no. 103085.

[7] S. P. Arteaga, L. A. M. Hernández, G. S. Pérez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS spoofing vulnerability in the drone 3DR solo," *IEEE Access*, vol. 7, pp. 51782–51789, 2019.

[8] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–26, May 2019.

[9] J. Su, J. He, P. Cheng, and J. Chen, "A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 291–296, 2016.

[10] K.-C. Kwon and D.-S. Shim, "Performance analysis of direct GPS spoofing detection method with AHRS/accelerometer," *Sensors*, vol. 20, no. 4, p. 954, Feb. 2020.

[11] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, "SemperFi: Anti-spoofing GPS receiver for UAVs," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2022, pp. 1–17.

[12] O. Jullian, B. Otero, M. Stojilović, J. J. Costa, J. Verdú, and M. A. Pajuelo, "Deep learning detection of gps spoofing," in *Proc. Int. Conf. Mach. Learn. Optim. Data Sci.*, 2021, pp. 527–540.

[13] E. Basan, A. Basan, A. Nekrasov, C. Fidge, N. Sushkin, and O. Peskova, "GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence," *Drones*, vol. 6, no. 1, p. 8, Dec. 2021.

[14] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Oct. 2011, pp. 75–86.

[15] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surveys*, vol. 48, no. 4, pp. 1–31, May 2016.

[16] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position, Location Navigat. Symp. - PLANS*, May 2014, pp. 1232–1239.

[17] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An efficient UAV hijacking detection method using onboard inertial measurement unit," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, pp. 1–19, Nov. 2018.
[18] G. H. Elkaim, F. A. P. Lie, and D. Gebre-Egziabher, "Principles of guidance, navigation, and control of UAVs," in *Handbook Unmanned Aerial Vehicles*, 2015, pp. 347–380.
[19] Ç. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2016, pp. 1027–1034.
[20] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, Jul. 2019.
[21] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, "An experimental study of GPS spoofing and takeover attacks on UAVs," in *Proc. 31st USENIX Secur. Symp. (USENIX Secur. 22)*, 2022, pp. 3503–3520.
[22] Z. Zhang, L. Zhou, and P. Tokekar, "Strategies to design signals to spoof Kalman filter," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 5837–5842.
[23] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing," in *Proc. 29th USENIX Secur. Symp. (USENIX Secur. 20)*, 2020, pp. 931–948.
[24] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, and Z. Lin, "SAVIOR: Securing autonomous vehicles with robust physical invariants," in *Proc. 29th USENIX Secur. Symp. (USENIX Secur. 20)*, 2020, pp. 895–912.
[25] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023.
[26] Y. Tang, H. He, and Y. Wang, "Hierarchical vector transformer vehicle trajectories prediction with diffusion convolutional neural networks," *Neurocomputing*, vol. 580, May 2024, Art. no. 127526.
[27] I. de Zarzà, J. de Curtò, G. Roig, and C. T. Calafate, "LLM multimodal traffic accident forecasting," *Sensors*, vol. 23, no. 22, p. 9225, Nov. 2023.

**JI HYUK JUNG** was born in Seoul, South Korea, in 1990. He received the B.S. degree in veterinary medicine from Seoul National University and the M.S degree in information security from Korea University, where he is currently pursuing the Ph.D. degree in information security. His research interests include machine learning, signal processing, and security. In particular, he is working on electric network frequency (ENF) signals and has also written an article on the side-channel attack.

**MI YEON HONG** received the B.S. degree in biology education from Seowon University and the M.S degree in information security from Korea University, in 2018, where she is currently pursuing the Ph.D. degree in information security. Her research interests include privacy-preserving, homomorphic encryption, and de-identification.

**HYEONGJUN CHOI** received the B.S. degree in cyber security from Korea University, South Korea, where he is currently pursuing the Ph.D. degree in information security. He was an Intern with NAVER Corporation, in 2020. His research interests include artificial intelligence, covert channels, and web hacking.

**JI WON YOON** received the B.S. degree in information engineering from Sungkyunkwan University, South Korea, in 2003, the M.S. degree in informatics from The University of Edinburgh, U.K., in 2004, and the Ph.D. degree in statistical signal processing from the University of Cambridge, U.K., in 2008.

From 2008 to 2009, he was a Postdoctoral Research Assistant with the Robotics Group, University of Oxford, U.K. From 2009 to 2011, he was a Research Fellow with the Statistics Department, Trinity College Dublin, Ireland. He was a Research Scientist with the IBM Research Laboratory, from 2011 to 2012. From 2012 to 2016, he was an Assistant Professor with the Cyber Defense Department, Korea University. Since 2016, he has been an Associate Professor with the School of Cybersecurity, Korea University. His research interests include all areas of intelligence, such as signal intelligence, crypto intelligence, artificial intelligence, and open-source intelligence.