Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform

Ahmad Danial Bin Abdul Rahman¹, Kamaruddin Abdul Ghani¹, Nor Hisham H Khamis², Abd Rahim Mat Sidek³

¹Electrical & Electronic Engineering, National Defence University of Malaysia, 57000 Kuala Lumpur, Malaysia
²School of Electrical Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
³Mindmatics Sdn Bhd, 43000 Kajang, Selangor, Malaysia

ahmaddanial@mindmatics.my, kamaruddin@upnm.edu.my, hisham@fke.utm.my, abdrahim@mindmatics.my

Abstract—This paper discusses the existing jamming method from previous publication and how the method is modified to accomplished the GPS jamming of Unmanned Aerial Vehicle (UAV). This paper also presents the result from the field test of UAV GPS jamming by using Software Defined Radio (SDR) and GNU Radio software. The field test is carried out to study the performance of the jamming signal produced and the effect of elevation angle on the jamming range. The test subject used in this field test is DJI Phantom 4 Pro, a commercial consumer grade drone.

Keywords—Unmanned Aerial Vehicle, Drone, GPS, Jamming, SDR, Jammer.

1. Introduction

In recent decades, Unmanned Aerial Vehicle (UAV) or popularly knowns as drones appear to be a game changer in all over the world. Although this technology was originally developed for military use, in recent years there have been a significant increase of interest among civilians due to the affordable cost and ease of use [1]. Few decades back, UAVs were operated by an experienced pilot in the military mission without any stabilization mechanism or autopilot. Nowadays, these drones are surprisingly user friendly since they are equipped with electronic stabilization, autopilot and GPS for the navigation. The increase of drone ownership among the civilian is a good sign of the technology rapid grow but also creates an enormous potential of hazard because of misuse of UAVs. Although drone legislations exist, not all the drone users comply with the rules. There are some individual or groups started to use drone for malicious purposes such as smuggling and spying. It just a matter of time for the misuse of these commercial drone become a serious threat.

Aware of these possible threats, a lot of companies started making money by developing anti-drone system or spectrum jammers as a counter-measure for drone mis-usage. This kind of system usually
being sold hundreds of thousands of dollars and some parties are willing to pay the cost in order to protect them from privacy breach. There are also a lot of researchers and publications discussing about UAVs jamming techniques and methods by using low-cost Software Defined Radio (SDR) platforms [5,10,11,12].

2. Global Positioning System (GPS)

Global Positioning System (GPS) is one of Global Navigation Satellite System (GNSS) that widely available all over the globe [2]. Nowadays, GPS is commonly used in various applications such as car navigation, missile operation and UAV autonomous operations. GPS easily provides an accurate location and timing with 24 satellites located in six orbital planes [3].

![Figure 1. Spectrum of the Course/Acquisition (C/A) code Global Positioning System (GPS)](image)

Figure 1 show the spectrum of the C/A code of the GPS with the bandwidth of 2MHz. GPS signal is modulated onto two carrier frequencies which are L1 band (1575.42MHz) and L2 band (1227.60MHz). L1 is widely use by civilian receiver and drone while L2 is specifically for military use. GPS signal travelled more than 20,000km from satellite to Earth. This resulting a very weak signal received by the receiver mainly due to the signal transmission path lost. The minimum power received by the receiver according to the GPS specifications is -158.5dBW for the L1 and -160dBW for the L2 [4]. GPS signal is very vulnerable to interference since the signal is very weak and there is no encryption.

3. GPS Jamming Method

Radio frequency interference or noise can affect the performance of the GPS receiver. There are two types of interferences which are unintentional and intentional interference. Unintentional interferences are unwanted noises that may come from any similar frequency transmitted. Intentional interferences in GPS can be classified into two types which are blanket jamming and deception jamming or spoofing [9]. Blanket jamming is an intentional act of blocking or interfering a signal in order to make the GPS receiver malfunction while spoofing is intentionally imitating the real signal source by giving wrong information in order to fools the receiver. This paper will focus on blanket jamming method of the GPS. Jamming a GPS can be by using narrow-band jamming or broad-band jamming. In [9],[10] & [11] all agree that broad-band jamming perform well than narrow-band jamming. In [10] & [11], GPS jamming method is classified into 5 types:

3.1. Tone Jamming

Tone jamming or spot jamming or also known as single frequency jamming is classified as narrow-band jamming as shown in Figure 2. This technique is suitable for the target with low bandwidth and if we
know the exact target frequency. The advantage of this technique is very simple and easy to generate and the power density is high and concentrated at single frequency. The disadvantage of this technique is useless against frequency hopping and spread spectrum.

![Figure 2. Tone Jamming](image)

3.2. Barrage Jamming
Figure 3 shows a Barrage jamming transmit noise to a specific bandwidth of frequency causing the interference to whole targeted spectral. This broad-band jamming is best to be used for the target with wide bandwidth or the target with frequency hopping capability. The main drawback of this technique is that the jammer spreads its power across the spectral, making it comparatively less powerful at a single frequency.

![Figure 3. Barrage Jamming](image)

3.3. Sweep Jamming
Sweep jamming as in Figure 4 is a combination of barrage jamming and tone jamming technique. The result of this jamming technique is quite similar to the barrage jamming because it operates throughout the frequency band. The difference is, barrage jamming transmits a static noise on a multiple frequency at a time, but sweep jamming change from one frequency to another in a period of time and this signal is known as chirp signal [6]. The advantage of this technique is, it can concentrate the power density since the signal is low bandwidth but it does not affect all the frequencies at the same time.

![Figure 4. Sweep Jamming](image)

3.4. Pulse Jamming
Pulse jamming can be narrow-band or broad-band jamming as shown in Figure 5. It transmits signal according to the interval which is set depending on the target. The signal might be a barrage signal or a single tone signal. The result of this jammer depends on the signal type transmitted whether low bandwidth or high bandwidth. This technique is considered as energy saving technique but the interval itself is the downside of this jamming technique since it gives time for the real signal to reconnect.
3.5. Protocol-Aware Jamming

Protocol-aware jamming shown in Figure 6 is a technique where the signal imitates the protocol parameters of the target. This method is best to be used against drone communication link (Spread spectrum and frequency hopping) since it prevents interference with other communication systems operating on the same RF band. It was concluded that these can reach interference with very low energy requirements and low probability of detection [7][8]. The downside of this method is the complexity of the architecture.

All the presented techniques above are widely discussed in [10,11,12]. To achieve a successful GPS jamming of the UAV the jamming signal must cover the whole bandwidth of the GPS C/A Code and the power density must concentrated at the center frequency.

4. Jamming Test Setup

In order to evaluate the performance of signal produced, a field test is conducted by using a DJI Phantom 4 Pro drone as the target. The DJI Phantom 4 Pro is designed with the GPS antenna on the top under the ABS cover. Figure 7 shows copper tape under the GPS antenna which works as the protection layer against unwanted signal from the ground.

4.1. GNU Radio Block

To produce a signal that can blanket jam the GPS receiver, the signal is constructed using Noise Source block with Additive White Gaussian Noise (AWGN) in the GNU Radio software as shown in Figure 8. The method is quite similar with the method used in [10] to produce tone jamming signal. The main different is the source block is replaced with noise block to produce a broad spectral signal.
The signal is processed in the SDR and transmitted by using SDR. In order to analyse the spectrum of the transmitted signal, SDR is connected directly to the spectrum analyser. Figure 9 shows the spectrum of the jamming signal produced. The jamming signal is transmitted at the centre frequency of 1575.42MHz which is the frequency of L1 GPS band. The signal produce is more than 10MHz broad enough to cover the whole C/A code of the GPS.

4.2. Hardware Configuration

For the field test purpose, a power amplifier and a directional antenna is added to the hardware configuration as shown in the Figure 10. In this test, the maximum jamming range is tested at the different altitude. The aim is to evaluate the performance of the jamming signal against real drone. Other than that, this test is conducted to analyse the relationship of the range and angle of jamming towards the GPS of the drone.
5. Experimental and Results

The antenna is levelled at approximately 1.5 meter from the ground. The drone is tested at 4 different altitude levels, 1.5-meter, 25-meter, 50-meter and 100-meter. At 1.5-meter, the drone and the antenna of the jammer is levelled with 0-degree of angle. At each altitude, the drone is tested at 50-meter, 100-meter and 150-meter from the jammer antenna.
The distance and altitude are retrieved from the DJI apps when flying the drone as shown in Figure 1. The jamming is considered successful when the satellite count is 0 to 3 causing the GPS in unusable as shown in Figure 12. For each test point, the absolute distance and the elevation angle is calculated and recorded in the Table 1 below. At altitude of 15 meter, the elevation angle is 0 degree. Hence, the distance and the absolute distance is same. The maximum jamming distance archive is 150 meters.

\textit{Table 1. Jamming result at 15-meter altitude}

| Altitude | 15 |
|----------|----|
| Distance (m) | 50 | 100 | 150 |
| Elevation Angle | 0 | 0 | 0 |
| Absolute Distance (m) | 50 | 100 | 150 |
| Result | ✓ | ✓ | ✓ |

At altitude of 25-meter, the elevation angle is decreasing with the distance increase. The maximum successful jamming distance is at 100 meters with the angle of elevation 14.04 degree and the absolute distance is 103.08-meter shown in Table 2.

\textit{Table 2. Jamming result at 15-meter altitude}

| Altitude | 25 |
|----------|----|
| Distance (m) | 50 | 100 | 150 |
| Elevation Angle | 26.57 | 14.04 | 9.46 |
| Absolute Distance (m) | 55.90 | 103.08 | 152.10 |
| Result | ✓ | ✓ | x |

At altitude of 50 meter, the maximum successful jamming distance is 100-meter with elevation angle of 26.57 degree and the absolute distance 111.80-meter as shown in Table 3.

\textit{Table 3. Jamming result at 15-meter altitude}

| Altitude | 50 |
|----------|----|
| Distance (m) | 50 | 100 | 150 |
| Elevation Angle | 45 | 26.57 | 18.44 |
| Absolute Distance (m) | 70.71 | 111.80 | 158.11 |
| Result | ✓ | ✓ | x |

At altitude of 100-meter, none of the jamming test is successful as shown in Table 4. At altitude of 50-meter and 100-meter, there are two similar absolute distance which is 111.80 meter with different result. At 50-meter altitude with angle of 26.57 degree, the GPS is successfully jammed while at 100 meters of altitude with angle of 63.44 degree the test is not successful. This is because of the protection layer that applied by the DJI under the GPS antenna. The copper tape successfully blocks the jamming signal or at least reduce the jamming effect.

\textit{Table 4. Jamming result at 15-meter altitude}

| Altitude | 100 |
|----------|-----|
| Distance (m) | 50 | 100 | 150 |
| Elevation Angle | 63.44 | 45 | 33.69 |
| Absolute Distance (m) | 111.80 | 141.42 | 180.28 |
| Result | x | x | x |
6. Conclusion

The performance of the jamming signal can be measured with the maximum distance of successful jamming tests. The best performance of the jamming signal produced is at the 0-degree of elevation angle, which it achieves the maximum distance of 150-meter. At 111.80-meter of absolute distance, the elevation angle effect can be concluded when the jamming test is successful at 26.57-degree of elevation while the test is failed at the same absolute distance with 63.44-degree of elevation. Thus, it can be concluded that, jamming capability decreases with the increase of elevation angle and distance.

The effectiveness of the protective layer under the GPS antenna that designed by DJI is also verified in this experiment. Hence, it can be also applied to other UAV design in order to protect them from GPS Jamming. From this experiment, it also can be concluded that, drone jammer is best to be mounted on the top of building compared to hand held jammer since the jamming signal from the ground is less effective to be compared to a drone-levelled jamming signal.

References

[1] I. Colomina and P. Molina, “Unmanned aerial systems for photogrammetry and remote sensing: A review,” ISPRS Journal of Photogrammetry and Remote Sensing, vol. 92, pp. 79-97, 2014.
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[3] E. Ayrapetian, Electronic Designs for Space: Radiation, http://www.nuvation.com/blog/electronic-design-services/electronic-designs-space, online; Last accessed:18-July-2015 (November 2013).
[4] P. Misra and P. Enge, Global Positioning System: Signals, Measurements and Performance. Lincoln, Massachusetts: Ganga-Jamuna Press, 2010.
[5] J. Gaspar, R. Ferreira, P. Sebastião and N. Souto, "Capture of UAVs Through GPS Spoofing." 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 2018, pp. 21-26, doi: 10.1109/GWS.2018.8686727.
[6] S. Smith, “The Scientist and Engineer's Guide to Digital Signal Processing” Chapter 11: Fourier Transform Pairs/Chirp Signals.
[7] Abid Hussain, Nazar A Saqib, Usman Qamar, Muhammad Zia, and Hassan Mahmood. Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks. Journal of communications and networks, 16(4):397–406, 2014.
[8] David Thuente and Mithun Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proc. of MILCOM, volume 6, page 100, 2006.
[9] H. Hu, N. Wei, “A study of GPS jamming and anti-jamming" Published in: 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS)
[10] R. Ferreira, N. Souto, J. Gaspar and P. Sebastião, “Effective GPS Jamming Techniques for UAVs using low-cost SDR platforms”, 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 2018, pp. 27–32, doi:10.1109/GWS.2018.8686672
[11] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, “Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms,” Wireless Pers Commun (2020). doi/10.1007/s11277-020-07212-6
[12] A. Brito, P. Sebastião and N. Souto, "Jamming for Unauthorized UAV Operations-Communications Link," 2019 International Young Engineers Forum (YEF-ECE), Costa da Caparica, Portugal, 2019, pp. 94-98, doi: 10.1109/YEF-ECE.2019.8740828.
[13] what-when-how - In Depth Tutorials and Information, “GNSS Antennas and Front Ends (GPS and Galileo Receiver) Part 1” [Online]. Available: http://what-when-how.com/a-software-definedgps-and-galileo-receiver/gnss-antennas-and-front-ends-gps-andgalileo-receiver-part-1/. [Accessed: 14-July-2018].