Analysis of Frequency Hopping Signals in Commercial Drones

Haeng-Bok Kil\textsuperscript{1}, Jae-Sin Lee\textsuperscript{2}, Eui-Rim Jeong\textsuperscript{3}

\textsuperscript{1,3}Department of Information and Communication Engineering, Hanbat National University, Daejeon, 34158, Korea
\textsuperscript{2}Navcours Co., Ltd., Yuseong-gu, Daejeon, 34014, Korea
\textsuperscript{1}hngbokk@hanbat.ac.kr, \textsuperscript{2}ljlsjls@navcours.com, \textsuperscript{3}erjeong@hanbat.ac.kr

February 4, 2018

Abstract

Background/Objectives: A jamming technique was proposed for frequency hopping signals in commercial drones to raise awareness of secure communication, and it can be used for disabling flight of unauthorized drones.

Methods/Statistical analysis: We analyze the characteristics of the communication signal between the drone and the controller of a commercial drone, and show that the communication system is vulnerable to jamming attacks. The wideband sampling, windowing and fast Fourier transform (FFT) are employed to observe the frequency characteristics. RF signal measurement equipment and MATLAB are used to analyze the frequency hopping signal of the commercial drone.

Findings: Unmanned aerial vehicles, or drones, have attracted considerable attention due to their versatile availability as military and civilian uses. However, as interest on the drones grows, they may be exposed to various harmful environments such as ambient noise/signal interference.
or intentional communication disturbance attacks. Therefore, it is essential to design a secure communication system between the drones and the controllers.

In this paper, we first analyze the communication signal between a commercial drone and the controller, which is turned out to be a frequency hopping signal.

**Improvements/Applications:** Frequency hopping signals are considered as one of the most secure communication technologies. This paper shows that the hopping signals are not secure and can be damaged by an intentional reactive jammer.

**Key Words:** Commercial Drone, Unmanned aerial vehicles, Frequency hopping spread spectrum, Reactive jammer.

1 Introduction

Recently, unmanned aerial vehicles (UAVs), or drones, have attracted considerable attention since their availability increases as military\(^1\) and civilian\(^2\). In particular, it has become an indispensable weapon in contemporary warfare\(^1,3\), as exemplified by the case of the attack insurgents with Helfire missile in the 2013 Iraq war. As they become more popular, the drones are increasingly exposed to various harmful environments, such as intentional or unintentional interference and communication disturbance attacks as well\(^4\).

Therefore, a security communication system against such interference and communication disturbance attacks is essential. As can be seen in the case of the drone kidnap by Iranian forces (an American Lockheed Martin RQ-170 Sentinel UAV in 2011), even military drones do not have secure communication systems\(^5\). From a different point of view, illegal and unauthorized drones are emerging and they are becoming social problems such as infringement of privacy and invasion of secure airspace. In this case, transmitting intentional jammers can block or disable the illegal drones flight.

Many communication signals used by drones are frequency hopping spread spectrum (FHSS) signals\(^5,6\). FHSS is a method of transmitting radio signal whose carrier frequency is changing rapidly. The changing frequency looks random in general, but it is predesignated and shared by the drone and the controller. FHSS signals
are widely used in military communications because of its high security. However, even FHSS signals are not safe from jamming threats. While there are problems that are difficult to implement in reality, high-energy wideband jammers can block the entire hopping space used by an FHSS system. In addition, FHSS is vulnerable to reactive jammers with a sufficiently high reaction speed. The reactive jammers are relatively easy and simple to implement than wideband jammers. In this paper, we analyze the communication signal between a commercial drone and the controller, which is turned out to be a frequency hopping signal. Through the analysis, we can find the hopping speed, carrier frequencies and the total bandwidth where the hopping signals can exist.

2 Frequency Hopping Signal Analysis

The overall block diagram for analyzing the frequency hopping signal is shown in figure 1. The hopping signal transmitted from a radio frequency (RF) communication module is received by the antenna. Then, the signal is converted into an intermediate frequency (IF) by a mixer. The analog to digital converter (ADC) makes digital signals and the digital down-converter converts the IF signals into baseband signals. Digital signal processing is performed by a PC using MATLAB tool. The baseband signal is represented as follows

\[ r_{BB}(n) = r(n) \times e^{-j2\pi f_c T_s n} \]  

Figure 1. Block diagram for drone communication signal analysis

\[ r_{BB}(n) = r(n) \times e^{-j2\pi f_c T_s n} \]
where \( r(n) \) is a digitally converted complex IF signal, \( f_c \) is the center frequency of the signal, \( T_s \) is the Sampling period, and \( n \) is the time index.

The down-converted signal is passed through a low-pass filter (LPF) to remove the frequencies of the remaining bands outside the signal band. The LPF is designed to prevent aliasing by out-of-band signals when performing down sampling.

\[
x(n) = \sum_{l=0}^{L} r_{BB}(n-l) \times h(l)
\]

where \( L \) is the length of LPF, and \( h(l) \) is the coefficient of filter.

After passing through the LPF, down sampling is performed to decrease the sampling rate. This reduces signal processing burden by lowering the signal processing clock. Then, windowing and fast Fourier transform (FFT) are performed for each \( N \) signal blocks. The window is used for suppressing the side-lobes as shown in figure 2.

\[
y(n) = \sum_{m=0}^{N-1} w(m+n)x(m)dm
\]

\[
C_k(\tau) = \sum_{n=0}^{N-1} y(n)e^{-j2\pi \tau n/N}
\]

where \( w, \tau, \) and \( x \) are the window, index of FFT and the signal at the LPF output, respectively.

Finally the frequency characteristics of \( K \) block can be obtained. Then, the power spectral density of the frequency characteristics is measured and we analyze the frequency hopping signal according to the existence of the frequency exceeding the predefined threshold.

Figure 2. Windowing and N-point FFT for spectrum measurement
value. The threshold value is obtained by multiplying the average received power by a factor, $\alpha$. When the power at the frequency exceeds the threshold, the frequency is recognized that a (hopping) signal exists.

$$TH_k = \frac{\alpha}{N} \sum_{\tau=0}^{N-1} \left| C_k(\tau) \right|^2$$  \hspace{1cm} (5)

$$\hat{h}_{hop} = \tau \times \frac{f_s}{N} \text{iff} \left| C_k(\tau) \right|^2 > TH_k$$  \hspace{1cm} (6)

where $TH_k$ and $\hat{h}_{hop}$ are $k^{th}$ threshold value and estimated hopping frequency, respectively.

3 Experiment Environment and Result

The experiment environments are shown in figure 3. FlySky FH-TH9X Transmitter is used for the transmitter body, FrSKY DJR Radio Telemetry for the RF module, FrSKY V8FR-II 8CH Receiver for the receiver.

![Commercial drone controller](image)

Figure 3. Commercial drone controller: (a) FlySky FH-TH9X Transmitter (transmitter body); (b) FrSKY DJR Radio Telemetry (RF module); (c) FrSKY V8FR-II 8CH Receiver (receiver)

The overall configuration for the experiment is shown in figure 4. A spectrum analyzer (Advantest R3477) and a digital oscilloscope (TDS 7254 by Tektronix) were used for RF signal measurement from a commercial drone controller.
The RF signal is converted into IF signal through the analog mixer (ZX05-43LH-S+ by mini-circuit) and the LPF (SLP-200+ by mini-circuit). The IF signals are transferred to the PC by a digital oscilloscope in order to analyze the signal at the PC. MATLAB tool is used to perform baseband signal analysis.

We use a LPF with a 20-tap length, Hanning window, and the number of FFT points is 32,768 to analyze the signals. According to the results, the RF signal transmitted from the controller has 70MHz total bandwidth with a center frequency of 2440MHz. The frequency hopping is performed among 50 channels and hopping occurs every 9ms, so the hopping speed of the system is obtained as 111Hops/s as shown in figure 5.
Figure 5. Time domain RF signal (upper) and spectrum (lower)

Figure 6 shows the signal pattern in the time-frequency domain using the frequency characteristic obtained from each FFT block. The first part of the signal was repeatedly observed to obtain information about the initial hop channel between the drone transceivers. As a result of observation, it is confirmed that the initial carrier frequency at which signal hopping starts is a fixed frequency of 2421.35 MHz, and the subsequent carrier frequency also has a static pattern.

In equation-(5), set threshold factor, $k$, to 15 and find $k$th threshold value, $TH_k$. Also, a signal having a power larger than $TH_k$ is
regarded as existence of a signal and the frequency index of the signal is saved. The experiment results for the analysis are shown in Table 1.

From the results generating FHSS jammers looks possible if we quickly analyze and chase the hopping frequencies of the received signal and generate the intentional signal at the same frequency.

<table>
<thead>
<tr>
<th>Index of hops</th>
<th>Estimated hopping frequency [MHz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>-35.7757</td>
</tr>
<tr>
<td>2nd</td>
<td>-5.7831</td>
</tr>
<tr>
<td>3rd</td>
<td>6.2103</td>
</tr>
<tr>
<td>4th</td>
<td>-17.7795</td>
</tr>
<tr>
<td>5th</td>
<td>-22.2809</td>
</tr>
<tr>
<td>6th</td>
<td>3.2104</td>
</tr>
<tr>
<td>7th</td>
<td>-23.7823</td>
</tr>
<tr>
<td>8th</td>
<td>27.2064</td>
</tr>
<tr>
<td>9th</td>
<td>25.7202</td>
</tr>
<tr>
<td>10th</td>
<td>34.7045</td>
</tr>
<tr>
<td>11th</td>
<td>10.7086</td>
</tr>
</tbody>
</table>

By performing a frequency hopping signal analysis, we were able to detect the hopping signal and track frequency hopping patterns and frequency components over time.

4 CONCLUSION

In this paper, the hopping signals used in commercial drone are analyzed via simple FFT. According to the analysis, it was confirmed that the target controller signal has the bandwidth of about 70 MHz, the hopping period of 9ms, and 50 hopping channels. It is conjectured that generating FHSS jammer is possible if we analyze the received signal and generate jammer without much time delay. As a future research topic, we will make a real-time reactive FHSS jammer for commercial drones.
References


