International Journal of Engineering & Technology, 7 (3.24) (2018) 100-103

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Reactive Jamming for Commercial Drones

Gyeong-Mo Nam[1], Gun-Ho Lee[1], Jae-Sin Lee[2], Heang-Bok Kil[3], Eui-Rim Jeong[1*]

[1]Department of Mobile Convergence Engineering, Hanbat National University, Daejeon, 34158, Korea
[2]Department of Alternative Navigation, Navcours Co., Daejeon, 123124, Korea
[3]Department of Communication System, Comesta Inc., Daejeon 1241241, Korea
[1]Department of Information and Communication Engineering, Hanbat National University, Daejeon, 34158, Korea*
[*]Corresponding author E-mail:erjeong@hanbat.ac.kr

Abstract

Background/Objectives: Increasing use of UAVs causes many social problems. The purpose of this paper is to develop drone-jamming technique that protects social safety against indiscreet and illegal use of UAVs
Methods/Statistical analysis:First, we analyze the frequency hopping pattern of the commercial drones in order to design jamming system. Specifically, the instantaneous Tx frequency is detected within several micro seconds. Therefore, the frequency analyzer tracks the communication frequency of the drone that changes every hop. After that, it transmits a strong jamming signal to the corresponding frequency, thereby disrupting the communication of the drones. All these procedures are completed in one-hop period, which enables reactive jamming.
Findings: As commercial drones become widespread, drones are often used for malicious purposes. One example is the problem of drones flying into restricted areas. In this paper, we propose reactive jamming to disable unauthorized drones. The proposed method is as follows. When a jamming signal is transmitted to drones that use FHSS communication, the communication between the drones and the controller is disabled. In this case, we confirmed that the drone was switched to failsafe mode, and the connection to the drones was disabled on the controller screen. When the transmission of the jamming signal is turned off, the communication between the controller and the drone is connected again. When using the reactive jamming technique proposed in this paper, it is possible to prevent bomb terrorist, unauthorized reconnaissance, narcotics smuggling etc.
Improvements/Applications: The conventional jamming method transmits a strongwideband interference for frequency hopping signals.The proposed reactive jamming technique, however, transmits a relatively weak interference signal to the narrow band to disable the frequency hopping communication.

Keywords: *Reactive jammer, Commercial drone, Frequency hopping spread spectrum, Anti drone, real-time jammer*

1. Introduction

Unmanned Aerial Vehicle (UAVs), commonly known as aerial drone is widely used for commercial and military environments [1]. UAV often refers to the shape of airplanes and helicopters that can fly and adjust through radio waves, rather than maneuvering directly on board.The first form of drone was invented in Austria in 1849 to Bombing by Balloon. Itwas used in the fight against Venice which was a system of blowing a hot air balloon with a bomb[2]. During the initial development phase of drone, it was developed for military use. But now it is used in various commercial fields. The dronesare classified as follows: Military drones for reconnaissance and attack purposes used in warfare, Commercial drones used throughout society such as leisure, broadcasting photography, observation, parcel delivery service, agriculture, recreation[3-4]. The worldwide market size of UAVs is expected to grow to about 5.2 billion dollars in 2010 and about 11.2 billion dollars in 2022[5].Among them, commercial drone market is about 500 million dollars in 2016, and it is forecasting that it will grow annually on average 19% or more each year, and will expand to 3 billion dollars in 2022[6].

Research on how to prevent problems caused by drones has not been developed yet as compared with the drone developments and diffusion speeds. In the case of military use, drones which had the existing maximum takeoff weight (MTOW) transport capacity within 10% has recently increased the transport capacity up to 25% level. This means that drones can use and carry killing weapons such as various firearms and explosives. This can lead to terrorism against nuclear power plants and important facilities of the country. Also, monitoring and control with the control radar can demonstrate ability only at altitudes of 150 m or more. Therefore, we cannot monitor or track highly intrusive drones of 150 m or less. Also, in the private sector, there is the possibility of causing damage such as infringement of privacy due to illegal housing invasion using drone. It can be seen that a new social problem has arisen due to the rapid growth of the drones. The nation or individual's safety and property must be protected in such a way as to disable the unauthorized drones.The technique of disabling drones is called *anti-drone*. Anti-drone technology is divided into soft kill and hard kill. The soft kill method is to electronically disable the drone, which includes jamming, geo-fencing, and spoofing. This paper considers soft kill method by jamming. There are various kinds of radio jamming methods. Jammers come in various designs: the simple constant jammer that transmits a jamming signal continuously; the random jammerwhich only transmits intermittently; and more complex ones such as the reactive jammer where a signal is only sent when target transmission is sensed[7–9].We have researched and developed the reactive jammer among the existing radio

interference methods like this.

The proposed jamming system has two part: frequency hopping signal sensing and jamming signal generation. For frequency hopping signal sensing, a wideband signal path is needed include RF path and A/D converters. We implement a 70MHz bandwidth signal path to detect frequency hopping signals. Based on the fact that the frequency hopping signal uses only small bandwidth at certain time but changes its center frequency time to time, we detect the current center frequency of the signal with high speed FFT (fast Fourier transform). Once the signal is detected, a narrow band interference is generated at the same frequency and transmitted. The proposed jamming systems is implemented with FPGA board and verified through field experiments with a commercial drone. According to the results, it is confirmed that the drone is disabled by the proposed reactive jammers.

2. Jamming Signal Generation

In this paper, we use a Graupner MZ-12 controller as shown in Figure 1 to control commercially available drone.

Figure 1:.Commercial drone controller: Graupner MZ-12

The center frequency of the Graupner MZ-12 controller is 2.44 GHz. It has total bandwidth of about 76 MHz.The communication signal is frequency hopping and the hopping period is 10ms within the total bandwidth.The number of frequency hopping frequencies is 76. Since the hoppingperiodis 10ms, the hopping speed is100 hops/sec. Figure 2 shows the communication signal of the controller measured by a digital oscilloscope (upper) and a spectrum analyzer (lower) [10].

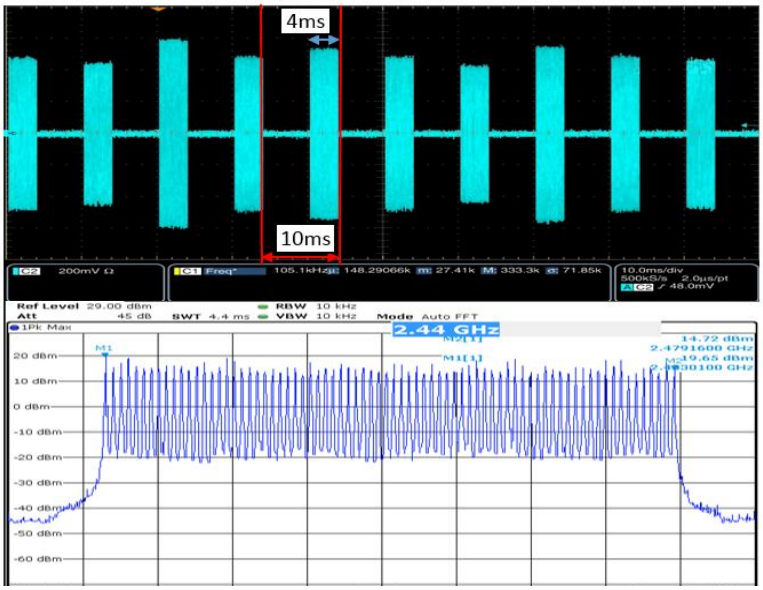

Figure 2:.Measurementresults of communication signal between drone and controller

In figure 2, we can see the signal bandwidth, the number of hopping frequencies, and the hopping interval.In this paper, in order to execute reactive jamming, we detect the frequency hopping signal, transmitted by the controller in real time.Next, a jamming signal larger than the detected hopping signal is generated and transmitted.At this time, every time a frequency hopping signal is detected, reactive jamming is performed by transmitting a jamming signal along the center frequency for continuous jamming.Figure 3 is a block diagram of the above mentioned process.

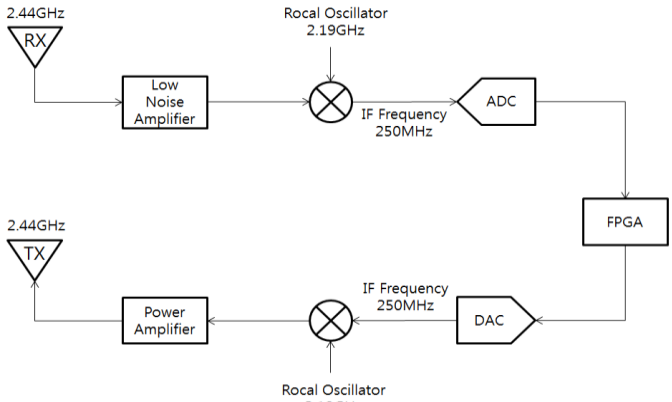

Figure 3:.Overall block diagram

First, a frequency hopping signal transmitted by the controller is received using a dipole antenna in the frequency range of 2.4 to 2.5 GHz band. The center frequency of the received signal is frequency hopped within a bandwidth of about 76 MHz around 2.44 GHz.Next, the signal received through the antenna is passed through the Low Noise Amplifier (LNA).In order to convert the RF signal to the IF frequency of 250 MHz, the frequency of the local oscillator is set to 2.19 GHz, and down conversion is executed by passing through the mixer. After that, the IF signal is converted to a baseband digital signal by passing through theanalog-to-digital converter (ADC). Since the ADC with the sampling rate of 200 MHz is used, the center frequency of the signal passed through the ADC is 50 MHz.This signal is input to the FPGA to perform signal processing such as signal detection and jamming signal generation.The FPGA uses a direct digital synthesizer (DDS) to generate a jamming signal at the detected frequency of the drone.The DDS implements the frequency synthesizer digitally to compensate for the shortcomings of the phase locked loop (PLL) structure. The following Figure 4 shows the basic operation structure of the DSS.

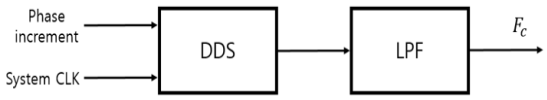

Figure 4:.DDS basic operation structure

DDS generates the jamming signal of the desired output frequency by receiving the phase increment and the system clock value.After the signal processing, the generated jamming signal is passed through the digital-to-analog converter (DAC) and converted into an analog signal. Since the DAC uses the same sampling rate as the ADC, the signal passed through the DAC has a center frequency of 250 MHz.The IF signal is passed through the mixer to convert it into an RF signal having a center frequency of 2.44 GHz. The frequency of local oscillator is 2.19 GHz. After passing the RF signal of 2.44 GHz through the Power Amplifier, it releases the jamming signal to the drone via the yagi antenna of 2.4 to 2.48 GHz.

3. Experiments

The following Figure 5 is testbed of the reactive jamming.

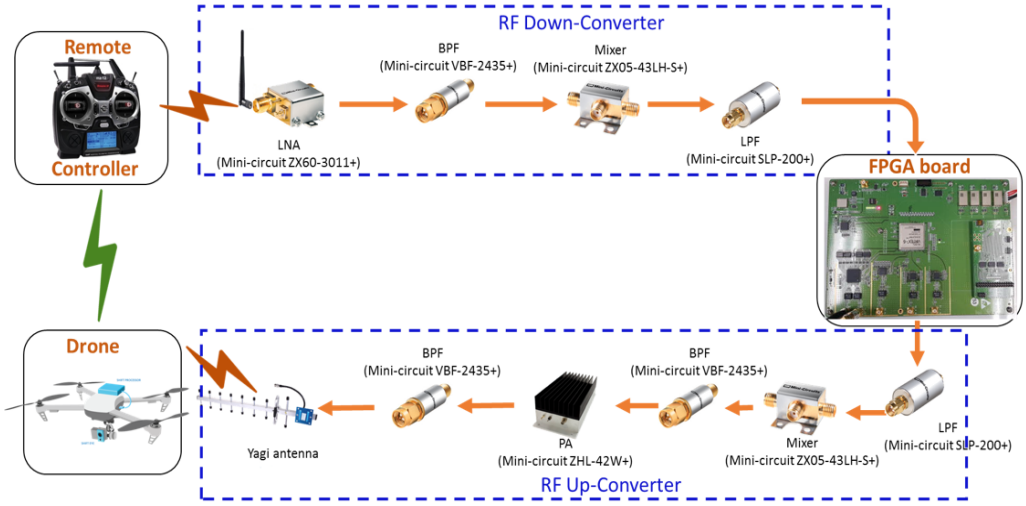

Figure 5:. Drone reactive jamming testbed

We implemented RF Down-Conversion part and RF Up-Conversion part using Mini-Circuit elements.First, the received signal is passed through an LNA that amplifies the signal by minimizing the amplification of the noise. The signal passes through a band pass filter (BPF) and blocks signals of other bands. After that, the mixer then lowers the frequency band and passes the low pass filter (LPF). It then sends the signal to the FPGA. The FPGA receives the signal and performs signal processing for reactive jamming. The signal processed signal is transmitted in the FPGA. The next step is performed to reverse the previous step.

The following Figure 6 is photos of reactive jamming experiment using a testbed[11-12].

Figure 6:. Experiments for reactive jamming

In Figure 6, the first photoisdemonstration using a Graupner: MZ-12 controller, and the photo below is experiment withanother controller.The demonstration process is as follows. First, the hopping signal of the drone controller is observed and analyzed through a spectrum analyzer.Next, the frequency of the controller signal received via the antenna is detected via a frequency tracking algorithm uploaded to the FPGA board.After that, it generates and outputs a jamming signal to that frequency detected by the FPGA board.The amplifier is installed in order to transmit the jamming signal with a signal stronger than the power which the controller and the drone communicate with.In order to transmit jamming signals, yagi antenna was used.As a result of the demonstration, the drones perform the operation as instructed by the controller before transmitting the jamming signal.When sending the jamming signal, communication between the controller and the drone was disconnected and drones that were not controlled and changed to failsafe mode.According to the experiment, it is confirmed that the reactive jamming is successful and we can intentionally block the communication between the controller and the drone.

The following figure 7 shows the controller switching to failsafe mode.

Figure 7:.Screen of the Graupner MZ-12 controller

In figure 7, the controller screen on the left is when the jamming signal has not been transmitted.It can be seen that the controller and the drone are connected (red box).The controller screen on the right is when jamming signal is transmitted.Looking at the red box, it is seen that the connection between the controller and the drone is disabled by the jamming signal.

4. Conclusion

In this paper, we provide reactive jamming technology for commercial drone using FHSS communication method.We confirmed that it was able to execute the role of Anti drone by interrupting communication between drones and controllers through reactive jamming.After tracing the frequency of the drone performing frequency hopping using the algorithm studied and developed in this paper,jamming signals are transmitted by using Yagi Antenna.Through the above experiments, it was confirmed that using the reactive jammer, it was possible to execute anti drone function to interrupt the communication between the actual drones and the controller.By using the proposed reactive jamming technique, it might be able to protecting some attack by drones such as bomb terror, drug smuggling, and privacy infringement of individuals.

References

[1] Joshua Mead, Christophe Bobda, Taylor JL Whitaker, “Defeating drone jamming with hardware sandboxing”, 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)
[2] “Remote Piloted Aerial Vehicles: An Anthology”. RPAV(Remote Piloted Aerial Vehicles), http://www.ctie.monash.edu/hargrave/rpav_home.html#Beginnings
[3] C. Anderson, "Stopping hardware trojans in their tracks", a few adjustments could protect chips against malicious circuitry, Jan. 2015.
[4] Drones: What are they and how do they work, [online] Available: http://www.bbc.com/news/world-south-asia-10713898.
[5] GuoweiCaia, Jorge Diasa,b, LakmalSeneviratnea,c, “A Survey of Small-Scale Unmanned Aerial Vehicles: Recent Advances and Future Development Trends”, Unmanned Systems, Vol. 2, No. 2 (2014) 1–26 World Scientific Publishing Company
[6] THE DRONES REPORT: Market forecasts, regulatory barriers, top vendors, and leading commercial applications’, businessinsider.com, 2016. 06. 10.[online] Available: https://www.businessinsider.com/the-drones-report-market-forecasts-key-players-and-use-cases-and-regulatory-barriers-to-the-proliferation-of-drones-2016-3
[7] K. Grover, A. Lim, Q. Yang, "Jamming and anti-jamming techniques in wireless networks A survey", Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197-215, Dec. 2014.
[8] W. Xu, K. Ma, W. Trappe, Y. Zhang, "Jamming sensor networks: attack and defense strategies", IEEE Network, vol. 20, no. 3, pp. 41-47, May 2006.
[9] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, B. Thapa, "Performance of ieee 802.11 under jamming", Mob. Netw. Appl., vol. 18, no. 5, pp. 678-696, Oct. 2013.
[10] HaengBok, kil, JaeSin Lee and Eui-Rim Jeong, Analysis of Communication RF Signals for Commericial Drones, ijpam, Volume 118, No. 19, pp. 2015-2024, 2018
[11] YouTube, http://youtu.be/oAmOop_JSoU
[12] YouTube, https://youtu.be/GAaaCVl8OOk