Signal Analysis of Remote Control (RC) UAV Used Software Defined Radio (SDR) HackRF One

Yetti Yuniati[1], Ardian Ulvan[2], Sitronella Nurfitriani Hasim[3]

[1]University of Lampung
[2,3] Electrical Engineering Department, Faculty of Engineering, University of Lampung
[1]yetti.yuniati@eng.unila.ac.id,[2]ardian.ulvan@eng.unila.ac.id,[3]sitro.ninas@gmail.com

Abstract

UAV (Unmanned Aerial Vehicle) is the unmanned aircraft which is controlled by Remote Control (RC) when flying. The operation of the UAV needs to be regulated to maintain air traffic security, one of which is by taking over the UAV. This study discussed the FSK modulation and demodulation mechanism in the process of taking over the UAV with HackRF One. The transfer mechanism of the UAV that done is to look for the RC frequency, channels, record the RC signals, determine the period and frequency carriers, and modelling the modulation and demodulation of FSK with Simulink. One parameter that is set in the process of this mechanism is to change the value of the different carrier frequencies. Then, the data obtained from the signal sent modulated results are the same as when the demodulated signal. Of T0= 79 µsandT1= 70 µs, so that fc0= 12658,22 Hz and fc1= 14285,71 Hz. To determine the size of the signal quality, it is necessary to determine the Bit Error Rate (BER) value. In this research, the obtained the BER values depend on the change of the energy value of Bit per Noise (Eb / No). When the Eb/No value is 10 (dB), then the BER is 0.038. Moreover, when the Eb/No value are 8 and 6 (dB), then the BER will be 0.078 and 0.23 respectively. It can be concluded that the greater Eb/No, the lower of BER.

Keywords: *UAV, Remote Control (RC), FSK Modulation, Simulink, HackRF One*

1. INTRODUCTION

Development of technology from time to time is increasingly sophisticated in the field of UAV (Unmanned Aerial Vehicle). UAV (Unmanned Aerial Vehicle) is a drone system controlled by Remote Control (RC). UAVs (Unmanned Aerial Vehicle) are generally known as drones, these planes are different from other types of aircraft because there are no pilots in the UAV in them.The beginning of the use of UAVs was used for world war by military forces in various countries because of fears of losing pilots over enemy territory. Now UAVs have been used in various fields such as marine security monitoring tools, monitoring the rate of vehicle traffic, aerial videos, and hobbies for their owners.

Until now the use of UAVs is no stranger to the wider community, so it needs a policy from the government to make security laws to use UAVs. Maintaining air traffic security for UAV usage can be done by taking over the UAV.

This research will discuss the mechanism of FSK demodulation in the process of taking over the UAV with HackRF One. Remote Control Signal (RC) UAV that has been recorded by the Universal Radio Hacker (URH) software followed by modeling the Simulink circuit to find out the modulation and demodulation processes to take over the UAV.

1.1 State Of Art

The latest research, hacking over the UAV can be done by making Maldrone a special Malware to attack the UAV. This research was carried out by an Indian man named Rahul Sasi. Maldrone is able to take over UAVs that are flying by hacking UAV controlling computer units and passing control to hackers. Research conducted by Sasi has tried with Maldrone which is found in Parrot UAVs which are exploited by attack methods. Sasi can infect UAV with Malware that acts as a link or proxy between flying machines with hackers even though they are near the UAV. Then the information will be sent back to hackers and they can interact with the UAV navigation function [1].

The author has difficulty finding references regarding hacking over the UAV. This research is rarely carried out by other researchers because it is very confidential. In addition, the tools used by the author are very few references that explain how the UAV takes place.

1.2 Software Defined Radio (SDR)

Software Defined Radio (SDR) was first accessed by Joseph Mitola in 1991 as an identifier of class radio that can be programmed and configured by software devices used by software[2]. Software Defined Radio (SDR) is a platform for radio communication systems and hardware regulated by computer software. This software can be adjusted to any frequency and modulation with a large frequency spectrum [3].

1.3 Diagram Of Receiver Software Defined Radio (SDR) System

Figure 1, shows the block diagram of the Software Defined Radio (SDR) receiver. The RF Tuner converts analog RF (Radio Frequency) signals to analog IF (Intermediate Frequency) frequencies. The sample fed to the next stage is the Digital Downconverter (DDC) which outputs a broken direction. Digital Mixer and LO (Local Oscilator) translate digital IF samples to the baseband. The FIR lowpass filter limits the signal and baseband bandwidth to attenuate the lowpass filter. The digital baseband sample is then fed to the DSP (Digital Signal Processing) block which functions as demodulation, decoding, and other processes [4].

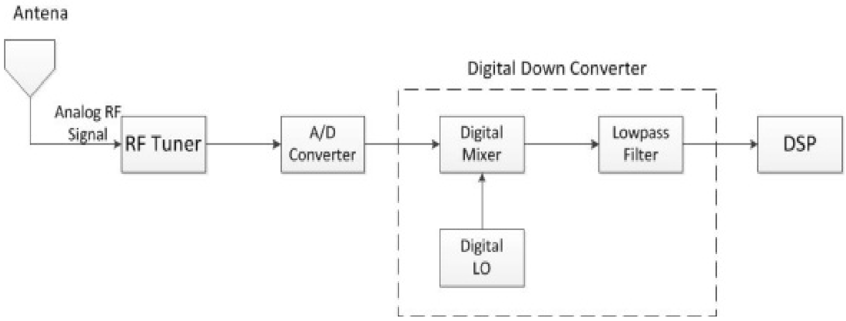


Figure 1. Diagram system *Software Defined Radio* (SDR)

1.4 HackRf One

HackRF One is a pheripheral Software Defined Radio (SDR) that is capable of transmitting or receiving radio signals from 1 MHz to 6 GHz. HackRF One is designed for testing and developing modern generation radio technology and so on. HackRF One is a hardware platform that can be used for USB devices or programmed for stand-alone operations [5].

1.5 Bit Error Rate (BER)

The Bit Error Rate (BER) is the number of bit errors per unit of time used as a measurement of radio system performance in digital communicationm [6].

1.6 UAV (Unmanned Aerial Vehicle)

UAV is an acronym for Unmanned Aerial Vehicle which is a pilotless aircraft controlled by a Remote Control (RC). UAVs can be controlled remotely where pilots control RCs on land or can fly independently based on flight plans that have been previously programmed. UAVs are often used for traffic monitoring, search, rescue, weather monitoring, and fire fighting [7].

1.7 Frequency Used in UAV

The 1980-1990 remote control used licenses of 27 MHz and 35 MHz bands. The 27 MHz system is for toys and a 35 MHz system for remote control. Since a few years later the 2.4 GHz band has become the most frequent frequency for remote control because it has switched to digital technology and is cheaper. The 2.4 GHz system often uses Spread Spectrum technology and is not susceptible to interference. Transmitters and receivers are tied together, possibly removing other transmitters connected to the receiver. ransmitters with a 35 MHz band on the same channel can take control and can also cause interference with each other [8].

2. METHOD

This study uses experimental methods by analyzing mathematically.The discussion begins with studying the FSK demodulation as a demodulator from the receiving side, determining the calculation parameters, followed by mathematical calculations of FSK modulation and demodulation equations. Then modeled using the Simulink circuit.

2.1 Research Flow Chart

The following are research stages in the form of flowchart:

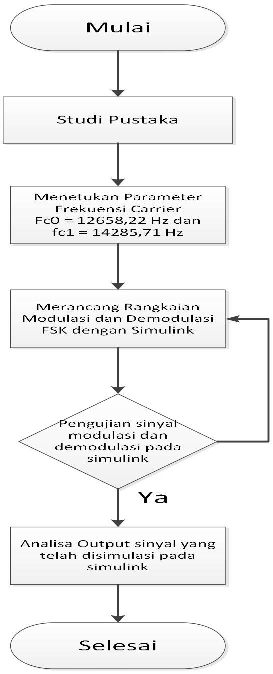

Mulai
Studi Pustaka
Menetukan Parameter Frekuensi Carrier Fc0 = 12658,22 Hz dan fc1 = 14285,71 Hz
Merancang Rangkaian Modulasi dan Demodulasi FSK dengan Simulink
Pengujian sinyal modulasi dan demodulasi pada simulink
Ya
Analisa Output sinyal yang telah disimulasi pada simulink
Selesai

Figure 2. Research flow chart

2.2 Flow Chart Take Over RC Signals on UAVs

The following is a flow chart taking over the RC signal:

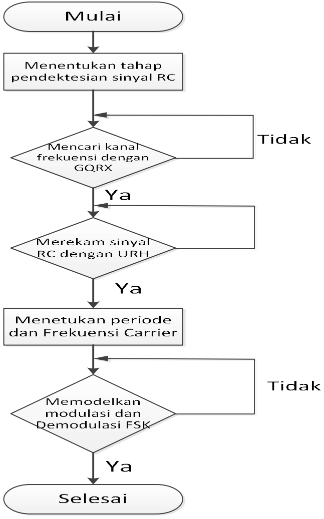

Mulai
Menentukan tahap pendektesian sinyal RC
Mencari kanal frekuensi dengan GQRX
Tidak
Ya
Merekam sinyal RC dengan URH
Ya
Menetukan periode dan Frekuensi Carrier
Memodelkan modulasi dan Demodulasi FSK
Tidak
Ya
Selesai

Figure 3. Flow chart take over RC signals

2.3 Equations

The process of taking over the UAV is done in several stages. One step that is done is the modulation process. The modulation used for this process is FSK modulation because the signal recording in the URH that is suitable for the UAV takeover process is FSK modulation. The equation for generating FSK signal frequencies will be described as below:

$$s(t) = \begin{matrix} A\cos(2\pi fc1t) \\ A\cos(2\pi fc2t) \end{matrix} \tag{1}$$

To get fc1 and fc2 can be obtained by:

$$fc1 = \frac{1}{T} \tag{2}$$

$$fc2 = \frac{1}{T} \tag{3}$$

Bit Error Rate (BER) can be formulated as follows:

$$BER = \frac{error}{totalbit} \tag{4}$$

3. RESULTS AND DISCUSSION

3.1 How to take over UAV signals

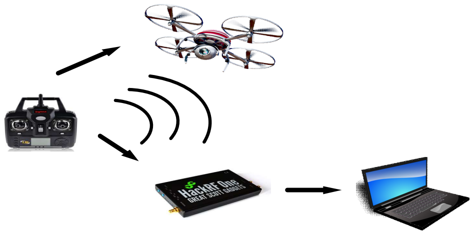
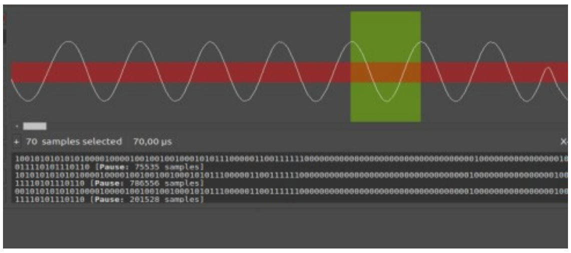


Figure 4. Diagram of take over UAV signals

The first stage of the UAV signal acquisition process starts from the Remote Control (RC) signal which emits waves of electromagnetic signals in all directions. The transmitted Remote Control (RC) signal is captured by HackRF One. HackRF One in this study was processed by several software such as GQRX and Universal Radio Hacker (URH).

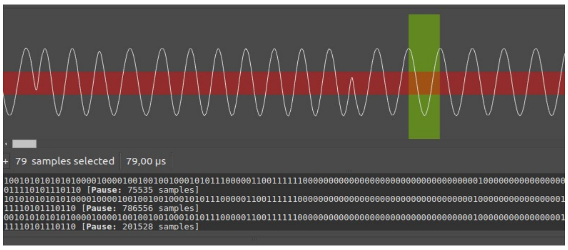
3.2 Record Result of UAV Remote Control (RC) Signal by HackRF One



+ 70 samples selected 70,00 µs

```
1001010101010101000010000100100100100010101110000011001111111000000000000000000000000000000000000010000000000000000010
011110101110110 [Pause: 75535 samples]
1010101010101010000100001001001001000101011100000110011111110000000000000000000000000000000000000100000000000000000100
11110101110110 [Pause: 786556 samples]
0010101010101010000100001001001001000101011100000110011111110000000000000000000000000000000000000100000000000000000100
11110101110110 [Pause: 201528 samples]
```

Figure 5. Signal wave when T_0



+ 79 samples selected 79,00 µs

```
100101010101010100001000010010010010001010111000001100111111100000000000000000000000000000000000001000000000000000000
011110101110110 [Pause: 75535 samples]
10101010101010100001000010010010010001010111000001100111111100000000000000000000000000000000000001000000000000000001
11110101110110 [Pause: 786556 samples]
00101010101010100001000010010010010001010111000001100111111100000000000000000000000000000000000001000000000000000001
11110101110110 [Pause: 201528 samples]
```

Figure 6. Signal wave when T1

Figures 5 and Figures 6 that each binary 0 and 1 represent different periods. One wave consisting of one hill and one valley highlighted in Figure 5 shows the sample period is 70µs (T1 = 70µs) which represents binary 1. Whereas one wave consisting of one hill and one valley highlighted in Figure 6 shows the sample period worth 79µs (T0 = 79µs) which represents binary 0.

3.3 FSK Modulation and Demodulation Modeling

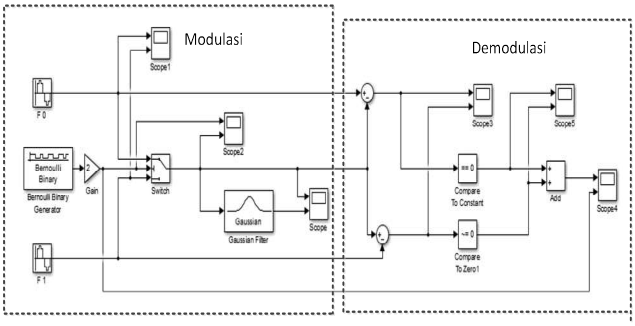


Figure 7. Modulation and demodulation circuits

In the Simulink circuit there is also a sine wave block that produces a carrier frequency wave. There are two sine wave blocks, namely f0 and f1. The wave output of these two carrier frequencies can be seen in Figure 8.

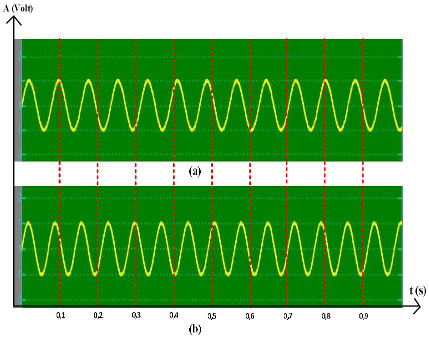


Figure 8. (a) Sine wave at carrier frequency f0 and (b) sine wave at carrier frequency f1

Seen in Figure 8 has a time delay difference of 0.001 x 10-3 second. The next circuit in the Simulink there is block scope 2 to display the waveform of the transmitted signal data.

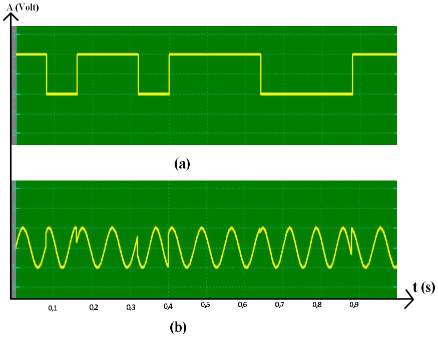


Figure 9. (a) Bernoulli data signal and (b) Modulated Signal

Figure 9(a) and 9(b) can be seen that the carrier signal varies according to the presence and absence of the data signal. The data signal sent is binary digit 1011011100011.

The next process is the modulated data signal is passed through the Gaussian Filter block. The results of this wave can be seen in Figure 10.

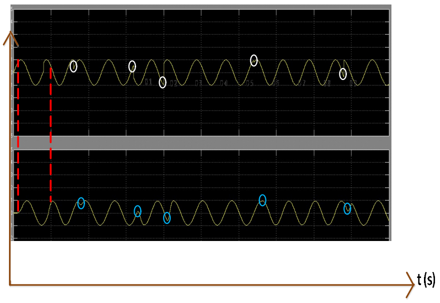


Figure 10. Signal modulation before and after passing the gaussian filter

Figure 10 has a difference when and after passing the Gaussian Filter. Conditions before passing through the filter are FSK modulation. This modulation displays a very broken signal pulse as shown in Figure 10 which is marked with a white circle, so to display the signal pulses become smooth then use the Gaussian Filter as shown in Figure 10 which is marked with a blue circle. The modulation signal wave that has passed the Gaussian Filter is passed to the SUM block in the Simulink circuit. The output of this stage is shown in Figure 11.

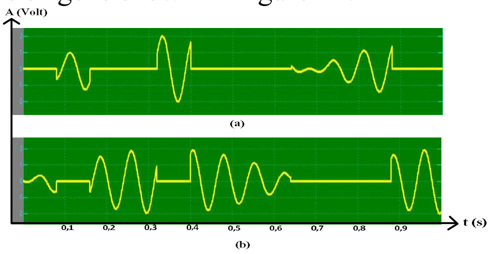


Figure 11.(a) Data signal at fc0 and (b) data signal at fc1

The carrier frequency fc0 can be said to be a space condition because there is a pulse signal when the condition is 0, while the carrier frequency fc1 can be said to be a mark condition because there is a pulse signal signal when condition 1.

The next step is compared with constan and compared to zero. Once seen in Figure 12.(a) and 12.(b) to display the original results that have escaped compared to instant and compare it to zero 1.

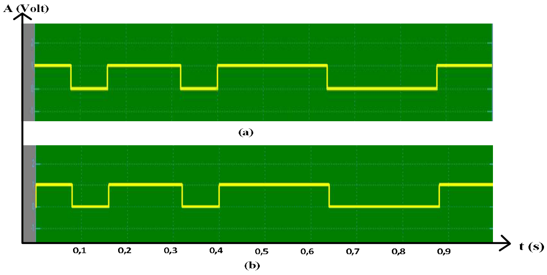


Figure 12. (a) Original Signal Form at fc0 and (b) Original Signal Form when fc1

Figure 12.(a) is a signal resulting from demodulation when the carrier frequency is fc0 while Figure 12.(b) is a signal resulting from demodulation when the carrier frequency is fc1.

The next step is to pass the add block in the Simulink circuit. The form of the original signal that has passed the add block can be seen in Figure 13.

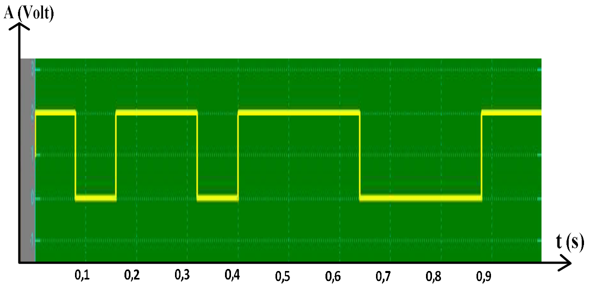


Figure 13. Original signal form after passing add

This add block aims to combine carrier frequency signals fc0 and fc1. The binary digit of the number above is 1011011100011.

3.4 Bit Error Rate (BER)

This research was conducted a simulation to determine the size of the Bit Error Rate (BER) in the Simulink circuit regarding the modulation mechanism and the FSK demodulation takeover of the UAV. Table 1 shows the difference in the Bit Error Rate (BER) value due to changes in the Eb / No value, so it can be concluded that the greater the Eb / No value the smaller the Bit Error Rate (BER) value. The result of the Bit Error Rate (BER) value that has been obtained can be seen that the performance of this digital transmission is very good.

Table 1.
Comparison Of Value Between Eb / No And BER

b/No] (dB)	*Bit Erro r Rate* (BE R)
0	.038
8	.078
6	.23

4. CONCLUSIONS

Based on the discussion and analysis that has been done, it can be concluded that:

1) In the theoretical concept the takeover mechanism of the UAV is to look for the RC frequency channel, record the RC signal, determine the period and frequency of the carrier, and model the modulation and demodulation of FSK with Simulink
2) The signal data sent when modulated is the same as when the signal has been demodulated. T_0 = 79 µs and T_1 = 70 µs, so that fc_0 = 12658.22 Hz and fc_1 = 14285.71 Hz

5. ACKNOWLEDGMENT

This research was support by DIPA PNBP FT Unila 2018. The authors thank the team members who helped complete this research.

REFERENCES

[1] Fox-Brewster,Maldrone: Watch Malware That Wants To Spreadts Wings Kill A Drone Mid-Flight, Forbes Magazine, URL:http://www.forbes.com/sites/bernardmarr/2015/09/01/7-technology-trends-that-will-make-or-break-many-careers/, Visited on: 30.08.2015.

[2] E. Marpanji, 2007, "Aplikasi *Platform* Komputasi *Software Defined Radio* (SDR) Untuk *Digital Spectrum Analyzer*," Prosiding Pertemuan Ilmiah XXV HFI Jateng & DIY.

[3] "*Software Enabled Wireless Interoperability Assessment Report—Software Defined Radio Subscriber Equipment*", PSWN Program, 2002.

[4] R. H. Hosking, 2017, "*Software-Defined Radio Handbook*", New Jersey: Pentek, Inc.

[5] M. Ossman. (2016, Agustus 2017) *.HackRF One* [*online*]. Available: http://greatscottgadgets.com/hackrf.

[6] N. Vlajic, 2010, "*Analog Transmission of Digital Data*: ASK, FSK, PSK, QAM", CSE 3213.

[7] Gheorghe Udeanu, 2016, " Unmanned Aerial Vehicle In Military Opertaions", Land Forces Academy, Romania.

[8] "Drone Technology: Types, Payloads, Applications, Frequency, Spectrum Issuses and Future Developments," Netherlands: t.m.c. asser press, 2016.