Unmanned Aerial Vehicle Design for Application in Cyber Security

M.K. Gambaryan

Yerevan State University, 1 Alex Manoukyan St, 0025 Yerevan, Armenia

E-mail: martin.gambaryan@gmail.com

(Received: September 10, 2021; Revised: September 30, 2021; Accepted: October 1, 2021)

Abstract. In this paper a small copter size unmanned aerial Vehicle (UAV) has been designed as a platform for a flying computer station to carry out cyber-attacks (Jamming, Spoofing, Man in the Middle, etc.) on devices that utilize wireless technologies, WiFi in particular. A yagi-patch hybrid antenna designed for 2.4 GHz freely rotates on two axes, thus allowing the drone to perform attacks on low power devices up to ranges of 300 meters. The modular design of the UAV allows for quick swapping of modules depending on the specific wireless technology used by the target device.

Keywords: UAV, directional antenna, yagi antenna, WiFi, cyber security

https://doi.org/10.52853/18291171-2021.14.3-151

1. Introduction

Cyber security issues in devices that use wireless communication has become an important field of research as the wireless technologies get integrated with more and more devices [1-4]. The design of the Unmanned Aerial Vehicles (UAV) in this paper is intended for carrying out long range cyber-attacks on wireless devices, in particular WiFi.

In other projects, copter-style drones have been used as platforms to attack other drones. The attacking drone uses a device called the "WiFi Pineapple" to attack drones also controlled 2.4 or 5 GHz WiFi. However, this method is limited by its range, the WiFi Pineapple not being effective from more than 20 meters. Also the design of the drone does not allow attack on other frequencies and wireless technologies.

The design that's suggested in this paper allows the user to change modules on the drone according to the target frequency or wireless technology. The yagi antenna designed for 2.4 GHz can be easily switched for another directional or non-directional antenna, designed for the specific application. The computer on the drone, the Raspberry Pi, has programmable GPIO pins, which can be used to add additional electronically controlled modules.

2. UAV Design for Long Range Security Testing of WiFi Devices

The design of the drone can be separated into 3 parts -

1. The main drone structure, including motors, ESC-s and the frame
2. The computer and antenna
3. The communication system

The frame of the drone is a carbon-fiber hexacopter frame with a diameter of 690 mm. The size of the drone’s frame is chosen proportional to the antenna that is used. Use of a lower frequency, therefore larger size antenna means larger size of the frame to insure stable flight. The parts such as the motors, ESC-s and battery have been chosen to support longer flight times. All the used parts for the drone build are listed below and also presented in Fig. 1.

- Frame - Tarot FY690S
- Flight Controller - Pixhawk Pro 2.4.8
- ESC - 6x Simonk Firmware 30A

- Motors - 6x Racestar BR2212 920KV
- Main Computer - Raspberry Pi 3B
- The Antenna - 2.4GHz yagi-patch hybrid antenna
- Servo Motors For Antenna Control- 2x MG996r

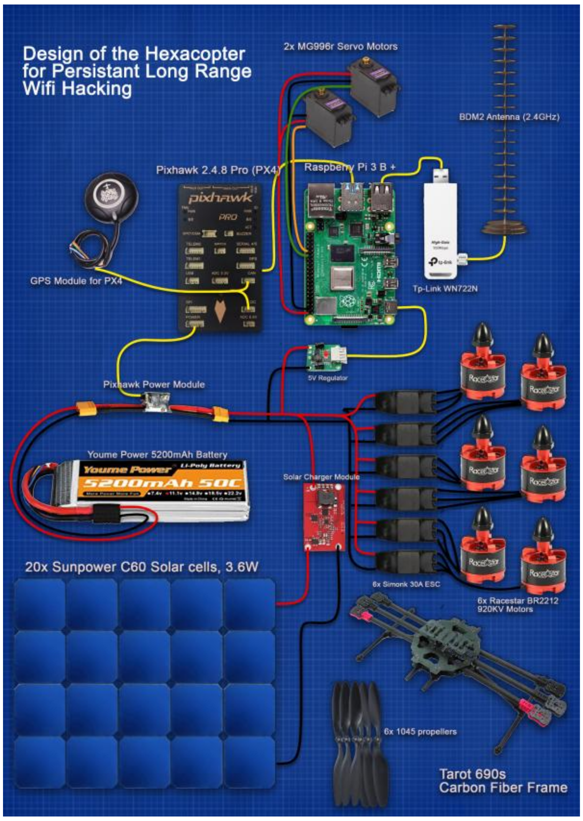

Fig. 1. Parts and connections for the drone build. (Note the solar module in the picture is not discussed in this paper).

The antenna is a hybrid type antenna between a yagi-uda and a patch antenna and is designed after an antenna called BDM-2, using 11 parasitic elements instead of 17 which make it more compact and light. This type of antenna has the property of being extremely directional, and has a very small angle of electromagnetic radiation. Although the range of highly directional antennas is big, the narrowness of its radiation pattern means that it has to be aimed at the target device [1]. On the drone this is achieved by mounting the antenna on it using two small servo motors, which are controlled by the main computer using GPIO. This process of aiming the antenna is programmed to be controlled by the base station's keyboard, or can later be automated to follow or lock onto targets while the drone is in flight.

The mount for the antenna has been designed using 3D design software called Blender, and later 3D printed. The mount is designed to hold both of the servos controlling the movement of the antenna and allow the antenna to move freely (Fig. 2).

The communication and control of the drone is implemented using mobile networks (3G/4G/LTE). A computer connected to the internet can be used as a control base station or a mobile device with a touch screen display if manual control with a virtual joystick is necessary. Because the flight controller of the drone does not have the capability to connect to mobile networks, the drone utilizes a 3G/4G Modem device, which on one end is connected to the Raspberry Pi with USB, and on the other to the mobile network [2]. The Raspberry Pi acts as a proxy, which relays all communications between the base station and the drone’s flight controller using MAVLink and MAVProxy [3,4].

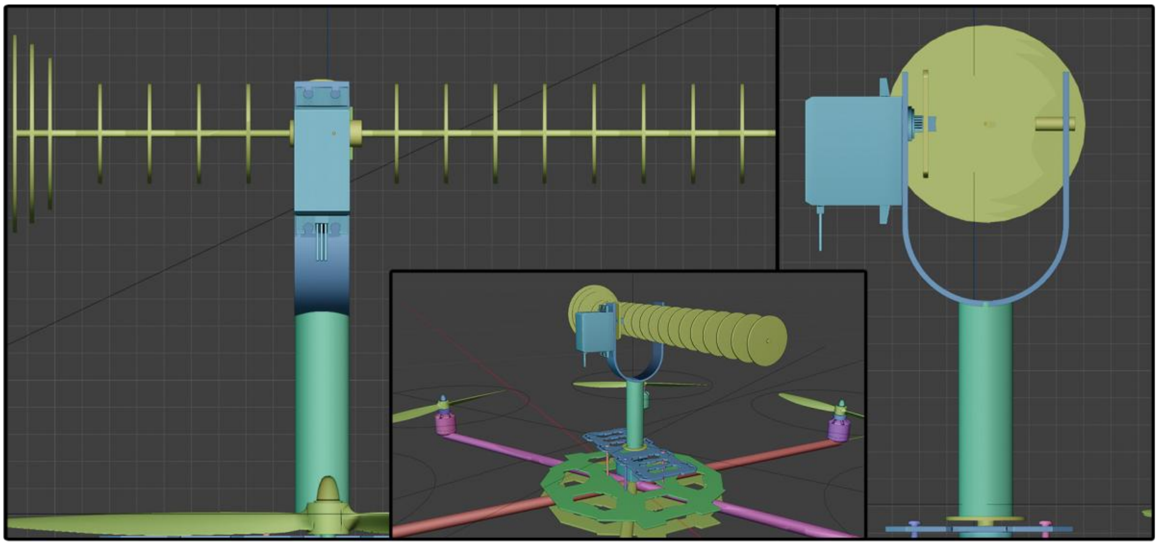

Fig. 2. The design of the antenna and the mount into Blender 3D.

An OpenVPN server is used to connect the drone and the base station. This way, the drone is always connected to VPN (Virtual Private Network) which ensures that the drone stays connected to the base station while the drone is in flight and being so, frequently connecting to different mobile towers. Connecting the drone and the base station with OpenVPN also ensures that all communications between the two are encrypted. This design showed good reliability and also low latency (<10ms) between the base station and the drone when both were connected to the same ISP's network (Ucom), even when streaming video and relaying communications data simultaneously. This design also allows the drone to be controlled from anywhere if the drone is connected to a mobile network.

The drone was tested with a test flight mission. The flight was controlled manually using a mobile device running QGroundControl and a virtual joystick. The drone successfully landed on its landing area to start the process of auditing the wireless device. The drone showed the ability to conduct Denial of Service, Deauthentication, Man in the Middle and Sniffing attacks reliably at a distance of 300 meters.

3. Conclusions

Thus, the UAV design suggested can work as a flying platform for carrying out cyber-attacks on WiFi devices. In a practical test it showed (*i*) reliable connectivity with a target WiFi Access Point at a range of 300 meters, (*ii*) can carry out attacks that do not require perfect wireless connection at ranges up to 450 meters (WiFi Deauthentication, Sniffing) and (*iii*) can be used as a development platform for security testing of other wireless technologies.

References

[1] H.-N. Dai, K.-W. Ng, M. Li, M.-Y. Wu, Int. J. Commun. Syst. **26** (2013) 413.

[2] L. Sundqvist, Cellular Controlled Drone Experiment: Evaluation of Network Requirements (Aalto University, School of Electrical Engineering, 2015).

[3] Saif Aldeen Saad Obayes Al-Kadhim, Communicating with Raspberry Pi via MAVLink (January 18, 2019).

[4] T.C. Mallick, M.A.I. Bhuyan, M.S. Munna, Intern. Conf. on Innovations in Science, Engineering and Technology (2016) 1.