# Technology Review - Security for Robotics

*Zach Rogers*

**CS461 Capstone**

**16 Feb 2017**

**Abstract**

Our goal as a group is to identify vulnerabilities, both hardware and software related, within our drone system. A big part of that will have to do with the drone's communication channel, which describes how a user controls a drone during flight and general operation. In order to attack the communication channel, we must first understand how the drones communicate with the user, and how the user sends commands to the drone. This will involve lots of data capturing. So my focus right now is to determine how we will be capturing that data, and how we will use that data to reverse-engineer the drone's methods of communication for the purpose of developing attack methods.

## Drone Communication Channel

The two drones that we have use a 2.4Ghz data-link between the drone and the receiver ground-station unit. That receiver unit then uses a Bluetooth connection to connect to the user's controller, which is a physical controller or device such as a laptop or tablet.[1] With this in mind, there are two communication channels that can be targeted; the connection from the drone to the ground-station unit, and the connection from the ground-station unit to the controller, this can be seen on Figure 1[1].

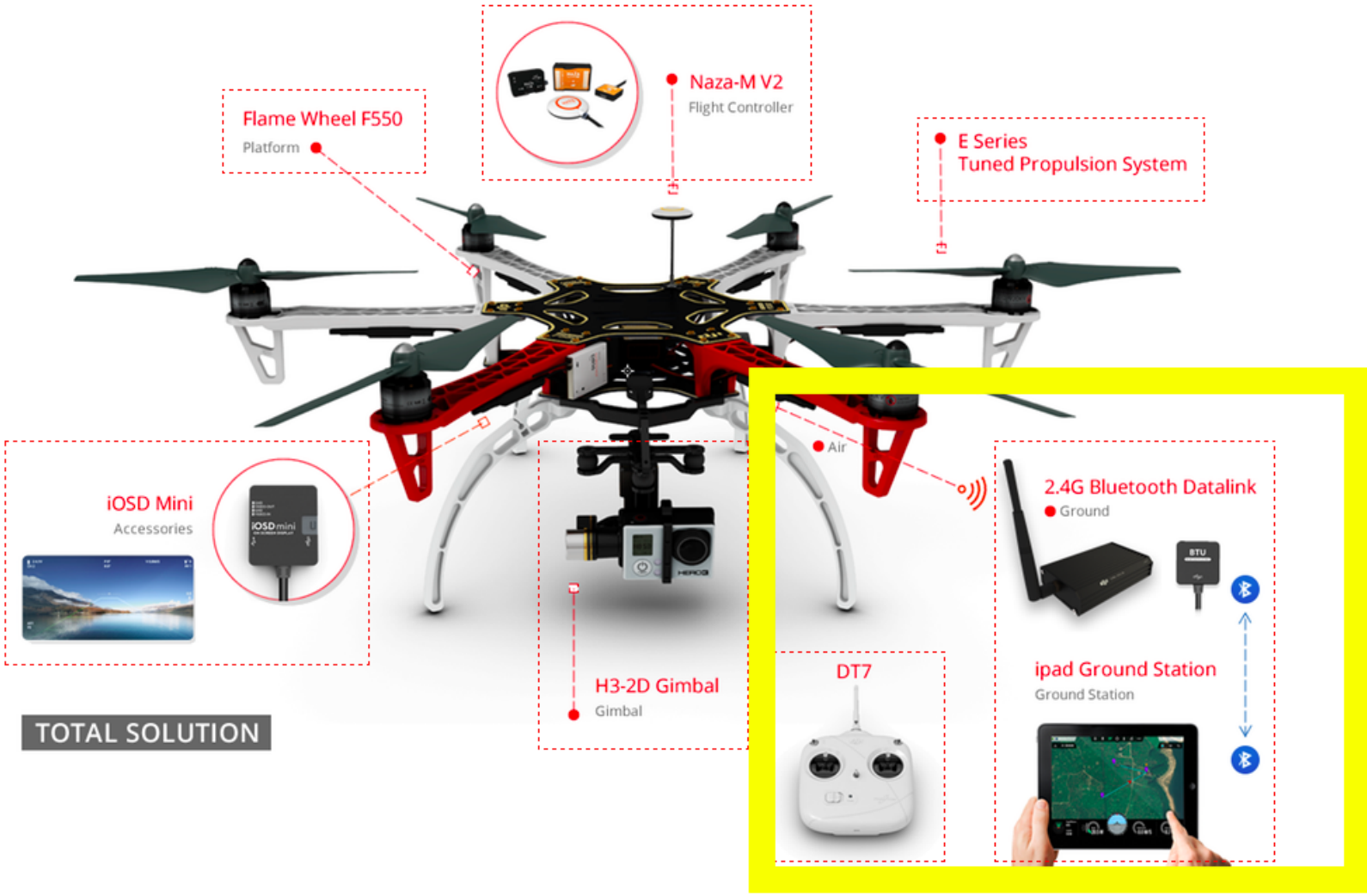


Figure 1: Flame Wheel ARF F550 Datalink Diagram

The 2.4Ghz frequency is commonly used by most Wireless Access Points, following the IEEE 802.11a/b/g standard. Bluetooth is another protocol that operates within the 2.4Ghz RF (radio frequency) spectrum[2]. This means that communication packets for the drone are being sent and received out in the open, which can be can be intercepted and analyzed with the right tools.

Each drone will be using a BeagleBone Black with a PixHawk Fire v1.6 Cape, making our drones Linux powered, running Ubuntu ARM, enabling us to use ROS[3]. The PixHawk is a flight control system, similar to the Naza-M2, which comes standard on the Flame Wheel ARF F550. It handles the drone's flight system, and includes a cluster of sensors (GPS, Gyroscope, etc) to keep track of vital information in order to maintain control over the drone while in flight. The PixHawk also handles telementry communication between the drone and the ground-station. As stated before, 2.4Ghz is the operating frequency between the drone and the ground-station, though

the PixHawk also supports a RFD900 900Mhz Telemetry Radio, for longer telemetry reporting distances[4]. This opens up an additional communication channel that could be targeted. In order to intercept and analyze 900Mhz RF communications, we would need additional tools, seperate from what would be needed to intercept and analyze communications on the 2.4Ghz frequency[5].

What should now be clear is that there is a lot of data transmitted in the open air in order to have a successful drone system. This means that there are a lot of different ways that communications can be intercepted and even altered, in an attempt to gain control over a drone's flight plan. Knowing which communication channels to target is only a small part of getting to the ultimate goal of intercepting drone data; consider that the Research and Development phase. The next step is to explore how exactly to capture that data.

## Methods of Data Capture

Capturing communication data between the user flying the drone, and the drone itself, will allow us to reverse engineer the communication protocols being used. Being able to capture that data also presents the possibility of doing a Man-In-The-Middle (MITM) like attack, enabling an attacker to intercept and spoof commands being sent to the drone in real time.

In order to capture this data, we need hardware that can recieve RF on the 2.4Ghz and 900Mhz band. There are many, many options out there, some of which can be quite costly. Since the primary method of communication is through the 2.4 Ghz band, we can use a standard wireless radio that can run in permiscuous mode[6]. Permiscuous Mode enables us to capture wireless packets without associating with an access point. This is how a lot of wireless attacks are performed[6]. With this, we can use the Aircrack-NG suite of wireless auditing tools to attack the wireless communication channel that the drone uses[7].

While running in permiscuous mode a popular packet capturing tool known as Wireshark will also be helpful. Wireshark is a very powerful application that will allow deep packet inspection, which will aid in reverse engineering the communication channel[6].

With these tools we will be able to capture communication between the drone and the drone ground control station, allowing us to leverage that data to develop drone attack methods, relating to our communications threat model.

It is also important to note that we need to get written approval from Oregon State University to intercept wireless traffic. During the time we intercept traffic, we will also capture legitmate traffic in the area that we are operating. We have spoken with OSU's Cheif Information Security Officer, Dave Nevin, regarding this approval.

## Leveraging Captured Data to Develop Attack Methods

Wireshark will also assist with analyzing the unknown communication protocol that the drone uses. Following the packet streams, and looking at the raw packet data, will allow us to form a concrete understanding of how the drone and ground control system associate with each other, and how commands are sent to the drone[8].

If reverse engineering proves to be unsuccessful, or difficult, we will still be in a poisiton to attack the drone communications, using MITM style attacks, and possibly some fuzzing related attacks[9].

# References

[1] DJI. Naza-m2 flight control system. [Online]. Available: https://www.dji.com/naza-m-v2

[2] B. Barnett. Hacking at the 2.4ghz spectrum. [Online]. Available: http://www.grymoire.com/Security/Hardware.html#TOC

[3] BeagleBoard. Pixhawk fire cape: Linux drones with the beaglebone black. [Online]. Available: http://beagleboard.org/project/pxf/

[4] A. Project. Pixhawk overview. [Online]. Available: http://ardupilot.org/copter/docs/common-pixhawk-overview.html

[5] B. Barnett. Hacking the 900mhz spectrum. [Online]. Available: http://www.grymoire.com/Security/Hardware.html#Hacking_the_.3C1Ghz_Range_.28900Mhz_.29_Spectrum

[6] Wireshark. Wlan ieee 802.11 capture setup. [Online]. Available: https://wiki.wireshark.org/CaptureSetup/WLAN

[7] A. NG. Getting started with aircrack-ng. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=getting_started

[8] Polynomial. How do you analyze an unknown network protocol. [Online]. Available: https://security.stackexchange.com/questions/17344/how-do-you-analyze-an-unknown-network-protocol

[9] H. Bck. Network fuzzing with american fuzzy lop. [Online]. Available: https://blog.fuzzing-project.org/27-Network-fuzzing-with-american-fuzzy-lop.html