Brigham Young University
BYU ScholarsArchive

All Theses and Dissertations

2014-03-18

Multi-Rotor--Aided Three-Dimensional 802.11 Wireless Heat Mapping

Scott James Pack
Brigham Young University - Provo

Follow this and additional works at: https://scholarsarchive.byu.edu/etd

Part of the Construction Engineering and Management Commons

BYU ScholarsArchive Citation

Pack, Scott James, "Multi-Rotor--Aided Three-Dimensional 802.11 Wireless Heat Mapping" (2014). *All Theses and Dissertations*. 4015.
https://scholarsarchive.byu.edu/etd/4015

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.

Multi-Rotor Aided Three Dimensional

802.11 Wireless Heat-Mapping

Scott James Pack

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Richard G. Helps
Joseph J. Ekstrom

School of Technology

Brigham Young University

March 2014

Copyright © 2014 Scott James Pack

All Rights Reserved

ABSTRACT

Multi-Rotor Aided Three Dimensional
802.11 Wireless Heat-Mapping

Scott James Pack
School of Technology, BYU
Master of Science

Traditional wireless site surveys produce a heat-map of link strength or quality over a target area, usually on the ground plane. In recent years research has gone into using aerial drones in network attack and surveillance, making three dimensional awareness of wireless coverage areas of interest. A multi-rotor drone and data collection module were built and tested as part of this research. Site assessments were conducted both in open space and near structures. Collected data was interpolated across the target area, and visualized as points and contours. These visualizations were exported to a Keyhole Markup Language (KML) for visualization in context. Resulting visualizations proved to be beneficial in identifying the coverage area of both authorized and rogue access points.

Keywords: wireless network, coverage, security, heat-map, site survey, quadcopter, multi-rotor

ACKNOWLEDGEMENTS

I would like to express my gratitude to those that assisted and encouraged me in performing this research. In particular, I would like to thank my wife, Drue, for her support and patience through months of having multi-rotor paraphernalia on every conceivable surface. I would like to thank my committee chair, Dr. Dale Rowe, for his assistance as a mentor; his experience and provided direction proved invaluable.

I would also like to thank my parents, Jim & Lynn Pack for their consistent support in my education and encouragement in fervently pursuing my interests and studies. My dad who brought me into the world of RC flight several years ago, and who with Dave Packham introduced me to multi-rotors. Thanks to Lane Broadbent and Byron Doyle, both of whom I relied on for bouncing ideas back and forth, 3D printing bits and pieces, and getting input on issues I ran into through the process.

I appreciate the BYU Information Technology faculty for the coursework and instruction performed through the IT program which prepared me for this research, and will assuredly continue to serve me well through the future. Finally, I appreciate BYU administration for their stewardship of the university, enabling research and providing learning experiences for myself and so many others.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

A background of wireless communications, security, and drone aircraft. The research questions and objective are put forward, as well as terminology, justification of the research and summary of the methodology. The scope and delimitations of the research are also stated.

1.1 Background

As few as fifteen years ago almost all computer networks used some configuration of copper lines, such as coaxial, 10-Base-T, or Category 3-5E twisted pair, to provide access-level connectivity to hosts. This provided hosts with the ability to connect to network resources, and in many cases remains to the present day the connection method of preference for static hosts, due to excellent speed and reliability, as well as inherent confidentiality and privacy. Over the past ten years however an explosion of wireless deployments has taken place, likely as a result of dropping costs in wireless interface production, standardization of wireless protocols, the relative ease of installation, and the ability to provide connectivity to mobile hosts.

The addition of the wireless radio spectrum as an access medium to computer networks greatly increases the convenience of connecting both mobile and static devices to organizations information resources. Form a security perspective however, the addition of wireless access increases the attack surface that a network presents to potential attackers. Initial attempts to provide traffic confidentiality in wireless networks similar to that of wired networks took the form of the Wired Equivalent Privacy, or WEP. WEP uses a stream encryption cipher to increase confidentiality and a checksum for data integrity. Shortly after the WEP debut, several weaknesses were discovered, which compromised the effectiveness of the protocol (Beck and Tews 2008). WEP was followed by encryption protocols Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA-2), available with a configurable suite of encryption protocols, and personal or enterprise authentication types. Even these protocols however are vulnerable to cryptanalysis, and exploitation of related services. Wi-Fi Protected Setup (WPS) for example is a service installed on many Wireless Access Points (WAP) which allows for quick addition of a new host to the network. This setup mechanism was identified as susceptible to brute force attacks, allowing many WPS-enabled networks to be compromised within 8 hours (Aked, Bolan, and Brand 2012).

While methods exist to increase the security of wireless networks, it is worthwhile to take into consideration Law #3 of the Immutable Laws of Security written by Microsoft, "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore" (Microsoft 2000). The same principle can be applied to a wireless network; if a malicious individual is permitted to place a host within the wireless coverage area and given sufficient time, an attacker can perform reconnaissance, scan for vulnerabilities, and otherwise negatively impact the confidentiality and availability of the network infrastructure.

As a result of this increase in attack surface via a wireless network, many organizations have elected to refuse to provide wireless access in their workplace, others find that their business needs demand wireless access, and have made deployments. To counter the ability of an attacker to intrude upon a wireless network, while fulfilling the business needs of an organization, it is important to be aware of the geographic coverage area of a wireless network.

Wireless site surveys are the process of inspecting the geographic area around a wireless access point (WAP) to determine the signal strength of a network at different points, the spectrum used by the network, and the spectrum used by neighboring or overlapping wireless networks. This is a common practice when deploying large wireless solutions and is used to determine optimal WAP placement, and to make channel assignments that will least interfere with other wireless devices. These surveys are presently performed by loading software on a laptop including a map of the area, roaming the area while taking signal-to-noise (SNR) measurements and clicking on the map to associate the reading with the appropriate location partially automating the process of creating a wireless "heat-map." Other software tools use GPS to position the data-point (Kershaw 2012). While this can be effective, it is limited to those areas accessible by an individual with a laptop. In the past this has been sufficient as most attackers were only capable of performing scans from the ground or road outside the facility, a practice known as "war-driving" (Berghel 2004). In recent years however, unmanned aerial vehicles (UAVs) have increased in capability, and research is being performed on using UAVs as a network attack platform, creating a new attack method of "war-flying" (Reed, Geis, and Dietrich 2011). This makes it important to be aware of wireless coverage areas not only on the ground, but in the air and in areas not accessible to human actors, such as balconies, roof tops, etc.

1.2 Problem Statement

Current methods of performing wireless site surveys fail to measure coverage in areas inaccessible to human actors, yet accessible to aerial attackers. These spaces also need to be monitored to obtain a comprehensive understanding the physical attack surface of a wireless network.

1.3 Research Questions, Objectives, and Hypothesis

Research questions are designed to determine the feasibility of using a multi-rotor drone in performing network coverage assessments. Questions and objectives addressed by this research include the following:

Research Question 1 (R1): Is a multi-rotor UAV a suitable platform for collecting geo-located wireless spectrum data?

Research Question 2 (R2): How does performing a 3D site survey using a multi-rotor UAV compare with alternative 3D site survey approaches in regard to speed, accuracy, safety, and cost?

Research Question 3 (R3): Is currently available open-source GPS-assisted waypoint navigation sufficiently accurate to execute a preplanned, autonomous three-dimensional wireless assessment?

Objective 1 (O1): Build a multi-rotor aerial transport platform and data collection module with which to conduct tests answering R1-R3.

Hypothesis 1 (H1): Such a platform can be built without specialist knowledge, using openly available parts and technologies for a low cost (under $1,000).

1.4 Definitions

Access Point – A radio transceiver used as a communications point through which client traffic is routed to the appropriate client. Often connected to a gateway providing connectivity to the internet.

Attacker – An individual or organization with malicious intent.

Autonomous – Capable of executing pre-planned objectives without manual intervention.

Coverage Area – The physical area or footprint within which a client may interact with an access point.

Drone – An unmanned aerial platform, frequently associated with autonomous operations. See UAV.

ESC – Electronic Speed Controller, an electric circuit used to control the speed and direction of an electric motor.

ESSID – Extended Service Set Identifier, a character string associated with one or more access points and used to identify networks.

Heat-Map – A geographic map overlaid with information to communicate density or change of a given metric. Often used to illustrate weather, population, and chemical density in materials. In this study it is used to indicate link quality.

KML - Keyhole Markup Language. An adaptation of the XML standard for use in describing geographic features and overlays.

Link Quality – A metric used to approximate the anticipated reliability and availability of a link, taking into consideration signal strength, interference, and bit error rates.

Rogue Access Point – An unauthorized access point attached to network infrastructure. Such a device introduces security risk in that it does not necessarily fulfill the security requirements of the organization.

Signal Strength – The strength of a signal as perceived by the receiver, typically represented in dBi, but often calculated by the receiver on a scale from 0 to 255.

Site Survey – The process of collecting data from a geographic area on a given parameter.

Telemetry – The wireless transmission of real-time data regarding a remote device.

UAV – Unmanned Aerial Vehicle. An airborne platform capable of flight without a pilot on board.

1.5 Justification

Attacks on wireless networks via wireless drone have been shown to be a real possibility (Tassey and Perkins 2009). War-flying has become an established term and platforms developed for research and field use have succeeded in performing network surveillance, acting as a covert transmission channel, performing wireless network attacks, and performing traffic redirection. Coverage assessment is crucial to determining exposure, and determining appropriate countermeasures.

1.6 Summary of Proposed Methodology

Data will be collected on a given wireless network by performing a manual or automated low-speed fly-by or fly-around of a target wireless network. In the duration of the fly-by, the signal to noise ratio (SNR) of every access point detected will be noted as a data point, as well as the altitude, latitude, and longitude at which the measurement was taken. This data will be filtered to exclude all data except that pertinent to the access point in consideration. Once this data is collected, Matlab will be used to plot the data points for further review.

As a trial run, a linear fly-by of a Wireless Access-Point (WAP) in an open area will be performed, starting at 50m to one side of the access-point and antenna, and will fly through the diameter of the access-point, concluding the flight on the far side. The collected data will be plotted in Matlab, and inspected to ensure that the results align with expected wireless transmission behavior, establishing construct validity. This will be performed several times at different speeds, providing an idea of the accuracy afforded by the hardware configuration and the maximum velocity at which the greatest amount of accuracy can still be obtained.

The platform will then be used to collect data points on single plane, a few feet above the ground. This will be collected by circumnavigating the WAP while in altitude hold. This will be performed several times, and will then be plotted in Matlab for inspection of face and construct validity.

A 3-dimensional heat-map will then be generated by performing the same process as the prior test, but at several altitudes resulting in a set of survey planes. This heat-map will be visualized for face validity. It is suspected that the platform may be incapable of sustaining flight for the required time period due to weight and power limitations. If necessary, several flights may take place and be combined to provide data over the desired target area.

Having determined the accuracy of the platform in generating a three dimensional heat-map, attempts will be made to create a heat-map using a production target, such as an access point inside of a building. A manual assessment will first be performed, followed by potential automated assessments. GPS waypoints will be set in the mission planner to establish the flight path.

1.7 Scope

The scope of this research is limited to determining the suitability of the use of a multi-rotor aerial platform in identifying the physical exterior coverage area of an 802.11 wireless access point to a client using readily available consumer-grade hardware.

1.8 Delimitations

The following topics have been determined to be outside the scope of this project.

1.8.1 Maximum Coverage Area

Radio frequency signal strength is proportional to the inverse square of distance from the emanation source. This means that signal strength decreases exponentially as distance increases, a very sensitive receiver however is still capable in some situations at picking up radio emissions from an 802.11 access point at up to 2 kilometers. The intent of this research is not to identify the distance at which an attacker is no longer capable of interfering with a network, but to determine the suitability of a multi-rotor in collecting information to determine the area in which it can reasonably be said that an attacker *could* interfere with the network.

1.8.2 5GHz, GSM and Other Communications Channels

Some research has gone into using mobile platforms to attack the Global System for Mobile Communications (GSM), a standard for cell-phone infrastructure. Assessing this infrastructure is outside of the scope of this research. 802.11 wireless systems are typically deployed for use of a specific group, such as employees of an organization within defined geographic limitations, such as the exterior walls of an office, and as such cover smaller geographic areas. GSM networks however are designed to provide good service to as large an area as possible, using longer wavelengths in the 380MHz-870MHz range. Additionally, due to hardware restrictions the 5GHz band will be omitted. While some aspects of this research may be useful for assessing the coverage area of a given GSM cell and likely directly applicable to 5 GHz 802.11 networks this particular work will be aligned to performing assessment of 2.4GHz 802.11 networks.

1.8.3 Penetration Testing

Performing a wireless assessment falls into what is referred to in offensive security as reconnaissance and is a preliminary step in a penetration test; this does not imply that the intent of this research is to conduct a penetration test. While the tools do exist, and are in fact present on the assessment platform to attempt the compromise of wireless networks, this research is not designed to go any further into the process of penetration testing than determining the signal strength of a potential “victim” at multiple points, and is intended to be completely passive in respect to the measured infrastructure.

1.8.4 Attacker Detection & Identification

The result of an assessment as described in this research explores the identification of where an attacker may access a wireless network, but it does not involve detection or identification of attack agents.

1.8.5 Countermeasure Evaluation

The result of an assessment as described in this research will reveal some locations in which an attacker could place a host. When such a location is determined, it is likely that an organization would want to evaluate countermeasures to mitigate this risk. This paper does review existing methods to counter such a risk, but performing an evaluation or comparison of these countermeasures is outside the scope of this research.

2. LITERATURE REVIEW

A review of the development of wireless communications and security, UAV development and legality is explored as well as the use of unmanned aircraft in network surveillance and attack.

2.1 Wireless Communications

Wireless communication is the process of establishing communication between a transmitter and receiver without the installation of a conductor between the two. This can be done by using one of several carrier types, such as light or radio waves.

There are several observations of radio characteristics that universally apply to wireless radio communications that can be used to estimate the capacity, range, and efficiency of a given deployment. Two important concepts are the inverse square law and the Shannon-Hartley Theorem. The Inverse Square Law states that the intensity of a radio signal is proportional to the inverse square of the distance from the signal source. This means that increasing the transmission power linearly will result in diminishing returns in signal propagation distance. The Shannon-Hartley Theorem states that the throughput of a channel is related to the bandwidth of the channel and the signal-to-noise ratio between the transmitter and receiver. This theorem can be used to determine the theoretical maximum communication efficiency over a noiseless medium with a given bandwidth (Shannon and Weaver 1948).

All radio-based wireless communications use an antenna to convert electrical power into radio waves. Antennas are commonly a minimum of one half the wavelength of the wave it is being used to transmit. Antennas vary in many respects, including the gain, radiation pattern, efficiency, polarization, and directivity; which characteristics are manipulated in order to achieve to goals of a given wireless communications implementation.

2.2 Wireless Deployments

In the 1968-1971 the University of Hawaii developed one of the first wireless packet-switched computer-to-computer systems. This deployment functioned on two 100KHz channels, each of which operated at 24,000 baud (Abramson 1970). As development continued, the IEEE 802 standards committee established several standards for wireless network deployments under the standards group 802.11 (IEEE 1997), specifying physical requirements of a wireless data interface, such as maximum power and appropriate spectrum use, and had typical speeds of 1-2Mbps. Refinements continue to be made to the 802.11 standard (IEEE 2012), resulting in the release of 802.11 standards a, b, g, n, ac, and ad. All of these standards currently function in the 2.4GHz or 5GHz bands.

Home and office wireless deployments have ballooned since the 1990s, creating a market that produces approximately one billion dollars in revenue per quarter (Machowinski 2013). Most of these deployments are based on the 802.11 b, g, and n families, with the ac standard beginning to make an appearance. The following table illustrates maximum theoretical speeds, although actual speed depends greatly upon host count, antenna type, transmission power, manufacturer, obstructions, weather, and other variables.

Table 1: 802.11 Families

802.11 Family Spec	Frequency	Max Theoretical Speed
802.11a	5GHz	54 Mbps
802.11b	2.4GHz	11 Mbps
802.11g	2.4GHz	54 Mbps
802.11n	2.5GHz/5GHz	150Mbps
802.11ac	5GHz	866.7 Mbps

In 802.11 the central transceiver to which hosts connect is referred to as the wireless access point (WAP) or simply access point (AP). Configuration of the access point determines the particular spectrum range or channel to be used by hosts on the network, the Service Set Identifier (SSID) of the network, the Basic Service Set Identifier (BSSID) which is the MAC address of the AP, the encryption method to be used, as well as higher level parameters such as DHCP and gateway services.

2.3 Wireless Security

Many networks depend on the physical difficulty of accessing the communication medium as a security measure, relying on an air-gap to prevent unwanted access. With the inclusion of wireless access, an individual is permitted to traverse this air-gap. Broadcasting network communications using the electro-magnetic spectrum raises many concerns regarding the confidentiality and integrity of network data. This was recognized quickly, and countermeasures were developed to increase the security of data in transit by using key-based encryption. One of the first encryption methods used to increase the security of wireless traffic was Wired-

Equivalent Privacy (WEP). Integration with existing federated identity management systems such as RADIUS and Kerberos was created to allow for organization-wide unified authentication and authorization. However due to the way that clients generated initialization vectors (IVs) in the WEP protocol an attacker was capable of collecting sufficient traffic to determine the original encryption key, allowing an attacker both to connect to the wireless network with the valid key, as well as decrypt traffic between the AP and other hosts (Stubblefield and Rubin 2001) in minutes. As a result of this vulnerability the vast majority of deployments have moved away from WEP as a wireless security protocol.

In the space vacated by WEP, Wi-Fi Protected Access (WPA) version 1 and WPA version 2 were created as modular security methods. These have the ability to use Temporal Key Integrity Protocol (TKIP) and CCMP, a security protocol based upon the industry standard encryption algorithm AES. The core components of WPA had been established to be relatively secure, suffering from only a few cryptanalysis weaknesses. These weakness open the possibility that an attacker could conceivably recover unknown message segments in a message containing a majority of known text (Beck and Tews 2008). Additionally, many home deployments were using insufficiently complicated and predictable pre-shared keys. To provide an alternative to customer-assigned keys a protocol known as Wireless Protected Setup (WPS) was created and deployed in many networks. The WPA2 protocol allows for easier authentication to an access point by making use of a 7-digit PIN. A method was created to brute-force this PIN, granting access and revealing the AP pre-shared key within in an average of 4 hours (Aked, Bolan, and Brand 2012). Many access point manufacturers prevented disabling WPS, resulting in a large family of wireless devices that are impossible to bring within an acceptable level of risk.

In addition to breaches in confidentiality, there exist many methods for an attacker to render the access point unavailable to one or multiple hosts. The design of many encryption systems used for wireless communications allow the transmission of certain control requests to be made outside of the encrypted tunnel typically used for data transmission (IEEE 1997). One of these control requests is the de-authentication request, a request sent by a client to an access point to signal the clients desire to end encrypted communication. As no authentication is required for a de-authentication request, an attacker impersonating the MAC address of a victim is capable of sending a de-authentication request, dropping the victim from the access point; this is known as a "de-auth" attack. When spoofed de-authentication requests are sent in quick succession it can result a denial of service condition, preventing the victim from gaining access to the wireless network.

A similar method is the disassociation attack in which an attacker impersonates a victim in sending a request to stop communications with the access point altogether. Another clever attack includes impersonating a power-saving mode request from the client. This directs the access point to buffer messages intended for the victim, and spoofing the notice of packets in the buffer from the access point to the client. This attack has the effect of both preventing the client from receiving data intended for it, as well as consuming memory resources on the access point (Bellardo and Savage 2003).

Given that there exist such a range of tools and techniques to breach both the confidentiality, integrity and availability of wireless network communications, it is unsurprising to see many organizations hesitant to deploy wireless access in the workplace. In order to provide the ease of access afforded by wireless connectivity while mitigating risk, many organizations segregate wireless traffic from sensitive traffic and services. Even if implemented to best practices access to a wireless network still provides an attacker with a foothold which may be able to be leveraged into further access.

2.4 Site Surveys

Site surveys are carried out for a variety of reasons. When initially deploying a wireless network a site survey is often performed to determine channel usage over an area in an effort to decrease the amount of overlap. Site surveys are also performed to identify unauthorized, or rogue access points. Rogue access points present a risk to security in that by connecting an improperly hardened and configured access point to a network it expands the attack surface available to a would-be wrongdoer. Data collected by a site survey typically includes information such as ESSID, BSSID, relative signal strength, link quality, and location. One such method involves providing a heat-mapping software on a mobile computer with a map of the area, moving the computer around the area on a cart, and collecting data from a wireless interface (Hills 2004). The physical location of the data-point is given by a human actor indicating the appropriate spot on the area map. Once sufficient data has been collected, a heat-map is generated showing the coverage area of each ESSID. One drawback with this approach is the difficulty and time required for an individual to perform this task. Additionally, in many instances several mobile computers would be used to perform this survey, injecting possible unknown variables such as antenna configuration and alignment, which would reduce the consistency of the results (Zvanovec, Pechac, and Klepal 2003).

Site surveys are also done for other reasons, such as providing low granularity positioning. By referencing nearby BSSIDs to an existing map, it is possible for an internet-connected device to determine the approximate location of the device. In order to make this possible, large-scale war-driving was done by Google and others resulting in lawsuits across the United States and the United Kingdom (Leiteritz 2010). Individuals known as "wardrivers" also collect similar information, which may be used for legitimate research information, or may be used for piggybacking, or using wireless access points to get internet access without permission (Berghel 2004).

2.5 UAV Deployment

Unmanned Aerial Vehicles (UAVs) also known as "drones" have recently come into the public eye in a large way. Typically modeled after fixed-wing aircraft, their use in military operations to perform reconnaissance or eliminate a target without endangering personnel has sparked much debate on the status of drone use in warfare (Sharkey 2011). UAVs have been used by researchers and rescue personnel to inspect the landscape in hazardous areas, such as post-disaster zone inspection (Ahmed 2008).

The availability of light-weight and high-accuracy sensors such as accelerometers, magnetometers, gyroscopes, GPS, and sonar or laser range-finders have made it possible to create multi-rotor platforms, commonly known as quadcopters or quadrocopters[1] that can function as a reliable aerial platform for a wide range of purposes. Previous uses include everything from landscape mapping to light-weight construction. The dynamics of a rotor UAV as opposed to a fixed-wing aircraft allows several advantages to a multi-rotor. (1) To execute maneuvering with sub-meter accuracy. (2) Vertical take-off and landing (VTOL) enables a multi-rotor to access areas restricted by the forward-only flight mechanics of fixed-wing aircraft, and (3) maintain an in-place hover. This makes multi-rotor platforms appropriate for

[1] Note* The term "multi-rotor" will be used to describe the platform used in this research.

applications requiring access in areas with restricted space, such as between buildings. There are also some disadvantages including limited flight time, noise generated by the motors, and the inability to remain airborne without applied throttle.

Multi-rotor development has progressed quickly in both the open source sector (predominantly from hobbyist groups such as Aeroquad[2] and Arducopter[3]) and the consumer market, such as the Parrot AR Drone (Visser and Dijkshoorn 2011). Products from both of these domains are undergoing continual refinement, many of which are now capable of performing advanced maneuvering, capturing and transmitting video feeds, following pre-planned GPS waypoint paths, and a degree of collision avoidance.

A typical consumer-grade multi-rotor UAV consists of the following components:

- Frame – Typically built of a lightweight material such as aluminum or carbon fiber.
- Flight Controller – Microcontroller responsible for integration sensory and receiver output. Scales these inputs to effect a change in duty cycle on each of the motors to achieve a desired position or angle of attack.
- Sensors – Varied between deployments, typically includes an accelerometer, magnetometer, gyroscope, and barometer, may include GPS, sonar range-finder, optical flow sensor, and others.
- Receiver – Used for radio control of the UAV, typically 6-8 channel receivers functioning in the 27MHz, 50MHz, 72MHz, 75MHz, or 2.4GHz spectrum ranges.
- Electric Speed Controllers – Used to manage the speed of each individual motor.

[2] "Aeroquad: Open-Source Quadcopter/Multicopter." http://aeroquad.com/content.php.
[3] "The Arducopter Project." *Google Code Repository*. https://code.google.com/p/arducopter/.

- Motors – Brushless electric motors, configurable in a Tri, Quad X, Quad +, or several other flight configurations.
- Battery – Typically a Lithium Polymer battery, as this family or cells permits the high discharge rates required by running several brushless motors simultaneously.
- Telemetry – Used to communicate with a ground-station to report flight status and to receive ground station commands. 802.15 radios are commonly used, but many alternatives exist.

2.6 UAV Legality and Public Reception

The phrase "drone" came into the vernacular with the United States military drone program, used to conduct surveillance operations and kinetic strikes on military targets. On account of several incidents leading to civilian deaths and domestic surveillance the term "drone," although synonymous with "UAV," has acquired a stigma. The use of these military drones is tightly regulated, regarding both the type of equipment used and the area in which they are flown. (Krishnan 2009).

Increasing numbers of manufacturers have begun producing and selling small personal UAVs for personal recreation. This type of RC flight also known as "Small Unmanned Aircraft" (SUA) flight, is permitted under a Federal Aviation Administration advisory which also applies to fixed-wing RC flight. The advisory specifically permits the non-commercial operation of model aircraft with certain restrictions. These restrictions include flight less than 400 feet from the ground, a "sufficient distance from populated areas," and not in the presence of spectators until the aircraft is successfully flight tested (Federal Aviation Administration 1981). This advisory was later modified to include a requirement for line-of-sight piloting and a manual over-ride in the case of aircraft with automated navigation capabilities.

The addition of GPS and cameras or other surveillance equipment to UAVs in accordance with the previously mentioned advisory is permitted, but this is subject to change. As of the time of this writing, a bill is in consideration which would seriously limit the use of UAV-mounted cameras in civilian use (Committee of Criminal Justice and Public Safety 2013).[4]

2.7 UAV in Wireless and as a Network Attack Platform

As UAVs are starting to become more commonplace, research is being conducted in using aerial platforms as a mobile network attack agent. A few examples include WASP, a retired fixed-wing drone refitted with equipment to intercept 802.11 and GSM data transmissions (Perkins et al, 2011). Another source has performed research in using a multi-rotor UAV as a covert channel for data exfiltration (Reed, Geis, and Dietrich 2011). As a UAV may be used to provide network connectivity external to an organizations own infrastructure, traffic using this type of alternate data channel circumvents protective network measures such as firewalls and intrusion detection systems, and has been found to be useful as a communication channel for remote command and control (C2) of infected hosts known as “bots” or “zombies.” Research into using UAVs as a temporary network bridge between hosts has also been successful (Alvissalim et al. 2012).

[4] Disclaimer: This is *not* a thorough legal study of the use of UAV use in commercial, amateur, military, or other types of use. Any individual intending to use a UAV must research legal restrictions with the particular implications of their use.

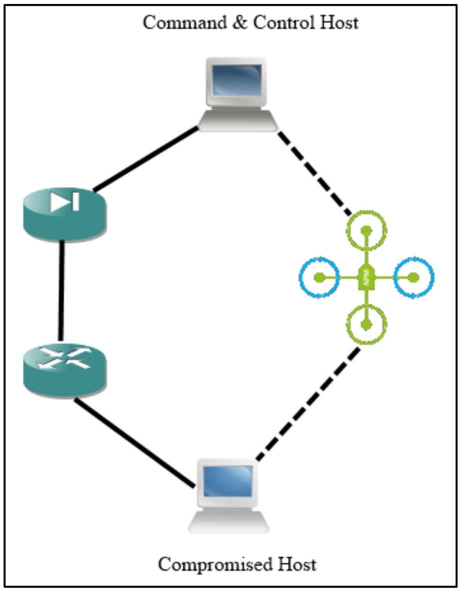


Figure 2-1: Command and Control via UAV

Shortly following and riding on the curtails of the announcement of an online retailer's research into using multi-rotors in parcel delivery[5] extensive work was done on exploiting the telemetry communications[6] of the popular commercial multi-rotor, the Parrot AR. Software was written or repurposed to de-authenticate the telemetry connection to the pilot, and assume the connection, putting an attacker in control of the on-board access point. This attack suite was also placed on-board a drone of the same model, creating an airborne attacker capable of compromising access points and other drones (Kamkar 2013).

In 2013, documents attributed to the United States National Security Agency (NSA) revealed a lightweight embedded computer running a version of Linux named the "SPARROW II." (Appelbaum, Horchert, and Stöcker 2013). This embedded system was categorized as a tool for "Wireless Survey – Airborne Operations – UAV" and described as a "fully functional WLAN

[5] "Amazon Prime Air." http://www.amazon.com/b?node=8037720011
[6] "Skyjack." http://samy.pl/skyjack/.

collection system” capable of supporting GPS functionality. While the exact usage of such a module is unclear, such a module may be capable of carrying out airborne network surveillance and intrusion. Additionally, research has been carried out in the use of a variety of airborne platforms, including UAVs, to deploy a mesh network consisting of infrared (IR), Ultra Wide-Band (UWB) and acoustic sensors in a military application, in an effort to detect explosives, firearms and other objects of military importance (Diamond and Ceruti 2007).

In brief, a network intruder may be capable of positioning a UAV in locations which have access to a wireless network but were previously not considered a physical attack vector. This allows an attacker to establish a presence in areas with obstructions such as height, cliffs, fences, or posted guards. Wireless coverage area awareness in a two-dimensional context may now be insufficient for organizations with high confidentiality requirements.

By using a UAV platform to assess a wireless network, it is possible to collect reliable data necessary to create a three dimensional heat map of the wireless network. Once aware, organizations can take action to reduce their exposure by relocating WAPs, shielding buildings, reducing antenna transmission power, or however they see fit.

3. METHODOLOGY

The equipment preparation, instrumentation, and flight assessment plans are laid out. Flight plans are established in order of increasing difficulty.

3.1 Equipment Preparation

To collect the necessary materials to pursue the aforementioned research object, open-source multi-rotor flight-controllers will be assessed on the criteria of flexibility, reported stability, compatible telemetry options, reported waypoint functionality, loiter functionality, and resilience. A frame will be constructed of lightweight materials as determined by weight, size, and availability. A flight controller integrating barometer, accelerometer, gyroscope, and magnetometer will be utilized, as such an integrated board adds less weight and size than flight controllers requiring numerous external sensors and breakout boards.

Collecting wireless data using the flight controller would require modification of the flight controller and may impact the ability of the flight controller to respond to flight sensor data, resulting in a less stable platform. This being the case, a separate data collection module will function as a removable module, with independent processing, storage, and wireless connectivity. This independent architecture allows the multi-rotor to act purely as a delivery device and provides a modular, scalable design that can easily be repurposed for other RF surveillance tasks.

Tuning will be performed to obtain the highest performance attainable on the given platform. The ability of the data collection module to collect and log geo-located signal quality data on a WAP will be assessed. This data will be saved in a simple ASCII CSV format for analysis and converted to the KML format for visualization, which is an XML format developed for use with Google Earth and other Earth viewers. Conversion will also take place to import data into Matlab for additional analysis and visualization.

3.2 Instrumentation Interference Test

To determine the extent to which the multi-rotor and data collection module interfere with each other, measurements will be taken to determine the accuracy of each module individually. The two will then be combined to determine any interference effect. This in part will determine the suitability of the multi-rotor platform as a delivery system for the data collection module.

3.2.1 Multi-Rotor: GPS Baseline

To approximate running conditions of the multirotor as closely as possible without introducing errors inherent in flight, the multi-rotor will be kept in a static position for the duration of the test. Propellers will be removed, the multirotor will be powered on and given 2 minutes to acquire a GPS lock. This is considered sufficient, as most GPS receivers acquire a satellite lock within 45 seconds. The throttle will be set at to a hover and data will be collected over the course of 3 minutes while the multirotor is armed and with motors running. Measurements will be taken at the maximum available frequency supported by the GPS receiver.

3.2.2 Data Collection Module: GPS Baseline

The Data Collection module will be placed in a well-known location for a five-minute period, during which it will collect GPS data at the maximum available frequency supported by the GPS receiver. The GPS data from these trials will be used to create a baseline for data collection module GPS accuracy. These datasets will be used to determine the mean squared error of the recorded GPS coordinates in latitude and longitude. The combined standard deviation will be considered the GPS baseline figure.

3.2.3 Multi-Rotor & Data Collection Module: Interaction Testing

The data collection module will then be mounted on the Multi-Rotor and, as performed previously, a five-minute trial will take place during which both the Multi-rotor and Data Collection module GPS will be sampling at the maximum supported frequency.

3.3 Flight Time Test

One constraint faced by a rotor-based aerial platform is flight-time, which is determined by fuel or battery capacity and discharge rate. Discharge rate in turn is affected by several variables, including weight, flight pattern, motor efficiency, and weather. All multi-rotor platforms in consideration use a Lithium Polymer battery pack and support fail-safe landing. All batteries will be charged to 4.2V per cell. As Lithium Polymer batteries can become damaged if drained to full capacity, flight will be deemed at a close when the flight controller initiates fail-safe landing at 80% remaining capacity and flight-time will be recorded. This will be repeated three times.

3.4 Manual Site Assessment Testing

Assessments will be performed in order of increasing difficulty. For each assessment, a WAP will be placed in a location central to the flight pattern. In order to obtain information while at first minimizing risk of collisions, assessments will be performed by manually piloting the multi-rotor.

3.4.1 Structure-Free Manual Assessment

A manual assessment will be performed to inspect the data collection method in the absence of preset navigation. To perform the manual assessment, the multi-rotor will be placed in an open area without obstructions such as trees and buildings. The multi-rotor will be flown about the area while collecting RSSI data on nearby WAPs. This will be used to ensure that the multi-rotor is working and data is being collected, as well as to provide data for developing visualization approaches. This will be repeated 3 times.

3.4.2 Linear Manual Assessment

The WAP will be placed in the center of an open area. The multi-rotor will be placed at a point 50 meters form the WAP, and piloted directly over the WAP, completing the flight 50 meters beyond the AP.

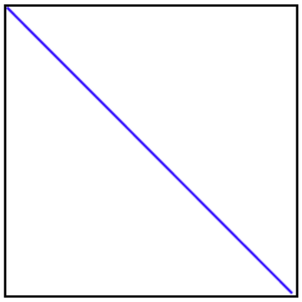


Figure 3-1: Linear Flight Path

3.4.3 Planar Manual Assessment

The WAP will be placed in an open area. The multirotor will be manually piloted around the perimeter of the area. This assessment will be performed 3 times. The flight path is in blue in the following illustration.

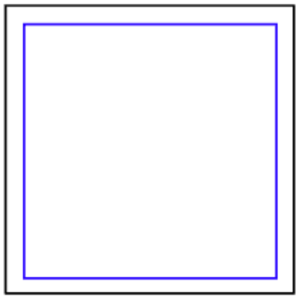


Figure 3-2: Perimeter Flight Path

3.4.4 Volumetric Manual Assessment

The WAP will be placed near the center of an open area. The multirotor will be manually piloted in a about the perimeter at several altitudes between 3m and 25m. This assessment will be performed 3 times. The different altitudes of the flight path are shown in the following illustration in green, red, and blue. It should be noted that while attempts will be made to achieve as close to the planned path as possible, flight and environmental characteristics are likely to cause deviations.

3.5 Structure Volumetric Manual Assessment

The multirotor will be manually piloted around a selection of the perimeter of the building at an approximate altitude of 2 meters, and done at several altitudes between 3m and 25m. This assessment will be performed 3 times.

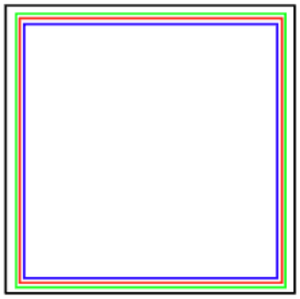


Figure 3-3: Volumetric Flight Path

3.6 Automated Site Assessment

Assuming successful completion of the previous, manual assessments and automated flight proves stable enough for automated assessments, flights will continue into the following plans.

3.6.1 Linear Automated Assessment

10 waypoints will be set along a 100 meter linear path at a fixed altitude of 3 meters. This assessment will be performed 3 times.

3.6.2 Planar Automated Assessment

Waypoints will be set in a perimeter around the target area at a fixed altitude of 3 meters. This assessment will be performed 3 times.

3.6.3 Volumetric Automated Assessment

Waypoints will be set in perimeter the target area at varied altitudes of 5, 15, and 25 meters. This will be plotted for face validity, and compared against the antenna specifications of the WAP manufacturer for construct validity. This assessment will be performed 3 times.

3.6.4 Structure Volumetric Automated Assessment

Waypoints will be set in perimeter around the building at increasing altitude of 5, 15, and 25 meters.

3.7 Analysis Methodology

The following sections describe the methodology used for data analysis.

3.7.1 GPS Analysis

As determined previously, GPS data points for the Multi-Rotor baseline will be taken at the maximum rate supported by the GPS receiver over the course several minutes and stored. The combined standard deviation in latitude and longitude determined in meters and recorded.

3.7.2 2D Visualization

Link quality data collected in two dimensions will be rendered in a scatter-plot as well as interpolated across the assessed area and displayed as a geographical contour heat-map.

3.7.3 3D Visualization

Data collected in three dimensions will be rendered in a 3D scatter-plot. An interpolation will also be made and used to generate “slices” of the heat-map, which will be rendered in the horizontal plane.

3.7.4 Additional 3D Visualization

Interpolated 3D data will be exported into KML format for first-person view inspection, both as points and contour slices. This allows the collected data to be put in context with the surrounding environment. Snapshots will be taken from each of these visualizations and included in later chapters. Due to the amount of data generated by each of the logs it is unfeasible to fully include them. Full 3D visualizations and data are available on DVD.

4. IMPLEMENTATION

Exploration of the multi-rotor built and data interpretation systems is established. Pertinent sections of the build process is explained, and a flight checklist is provided. Descriptions of the scripts used to generate visualizations are set forth.

4.1 Multi-Rotor Equipment Selection

The following equipment was used for the assembled multi-rotor.

Table 2: Multi-Rotor Equipment

Equipment Type	Model
Flight Controller	Arducopter APM 2.5, Code 2.8.1
Telemetry	RCTimer 433MHz Unit
GPS	uBlox NEO-6M GPS
Frame	Glass Fiber “Firefly” 450mm
Power Module	3DR C/I Power Monitor
Motors	Turnigy 2826 Brushless DC
Electronic Speed Controllers	Turnigy 30A Plush ESC
Battery	Zippy 4000mAh 4 cell Lithium Polymer

The Arducopter APM was selected as a result of the low price point, familiarity with the platform, ongoing development, and flexibility to be tuned to accommodate a variety of frames, motors, and payloads. Motors and ESC specifications were increased slightly from the default suggested build as the overall weight of the platform and payload were anticipated to be heavier than the frame and electronics alone. A modular approach was taken in the build, making for simpler modifications and repairs. A build of this type is often used as a camera-ship and used in performing aerial photography. A 3D-printed boom was built to separate the GPS from the ESCs and motors, intending to reduce interference with normal GPS functionality.

4.2 Data Collection Module

The data collection module consists of a Raspberry Pi Model B running Raspbian Wheezy, a Pi-optimized version of the Debian operating system. The Alfa Networks AWUS036NHA, a common war-driving USB interface, and a standard 5-Dbi omnidirectional antenna were used for collecting wireless measurements. The uBlox CN-06 GPS receiver is used to determine the platforms position and was connected to the 3.3V, ground, and serial in/out pins included in the Raspberry Pi general purpose input/output (GPIO) pin bank. As initial testing showed the altitude determined by GPS to be wildly inaccurate, an Adafruit BMP085 barometer was installed, using the I2C interface, also available on the GPIO pins. The Raspberry Pi and attached peripherals were powered using a 12.6 volt to 5 volt regulator connecting the lithium polymer battery being used to power the multi-rotor and the USB micro power interface on the Raspberry Pi.

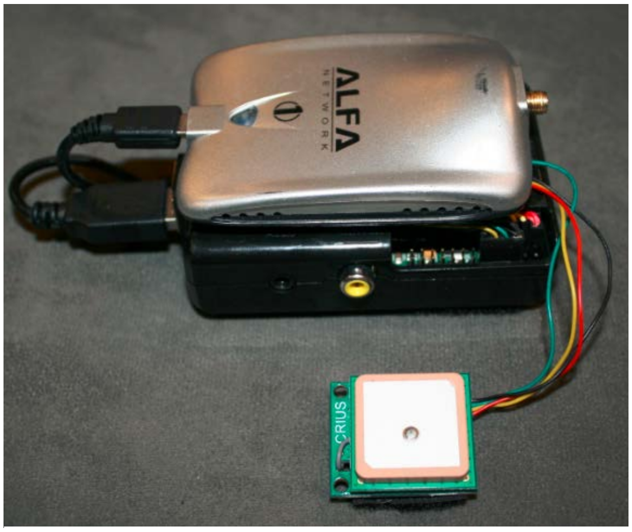


Figure 4-1: Data Collection Module

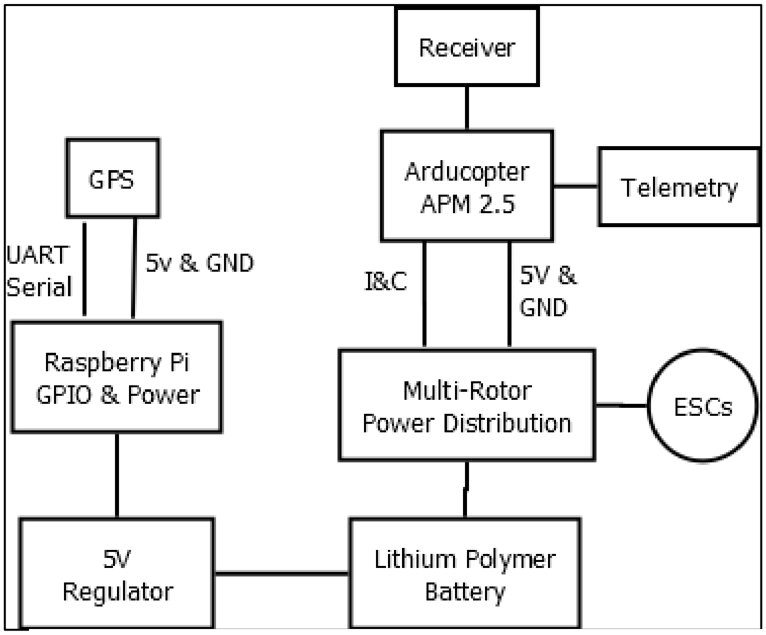


Figure 4-2: High Level Connection Diagram

4.3 Flight Procedures

The patterns of the individual flights varied, but the process of starting a flight was maintained across each flight. Prior to initiating a flight, the battery was confirmed to be fully charged to 12.6V. The battery was strapped to the bottom of the ground plate. The flight controller, GPS, and data collection module were visually inspected to ensure that they were properly mounted on the frame. The SD card used as the boot image and log storage medium was inserted into the data collection unit. The data collection module antenna was checked to ensure vertical alignment. At this point the transmitter was turned on and the throttle was set to zero. The area was inspected to ensure that no bystanders were in the flight area. The battery was connected to the power module, which caused the flight controller to power up and provide a series of three beeps to confirm successful power-on, and a timer was started for two minutes. The Raspberry Pi power and storage access LEDs were inspected to ensure that the data collection module was successfully started. After the two minute timer expired, providing sufficient time for a GPS satellite lock, the Python script collecting data automatically started and the scheduled flight commenced.

Upon finishing the flight and returning the multi-rotor to the ground the power was removed, and the battery was removed and set aside to be charged at a later point. In case of a rough landing or crash the entire multi-rotor was inspected for cracks and other signs of breakage. Repairs were made if necessary. The SD card was ejected for retrieval, backup and inspection of the collected data.

4.4 Flight Checklist

1. Ensure battery is fully charged.
2. Check for inclement weather.
3. Ensure data collection module, GPS, and other peripherals are well attached.
4. Ensure SD card is fully inserted.

5. Ensure that no bystanders are near the flight area.

6. Ensure the transmitter throttle is set to zero.

7. Connect battery to multi-rotor.

8. Check power LED on the Raspberry Pi & Wireless Adapter

9. Wait two minutes for GPS lock.

10. Conduct flight pattern as described in the methodology.

4.5 Data Collection Script

A Python script was written to perform the following:

1. Wait 2 minutes to acquire a GPS position lock.

2. Initiate a serial connection to the GPS

3. Create a log file in `/var/log/geolocate/` on the SD card for output

4. Perform the following items repeatedly

    a. Scan for nearby APs

    b. Parse AP information

    c. Acquire a GPS coordinate

    d. Acquire barometer altitude

    e. Write results to the log file in CSV format

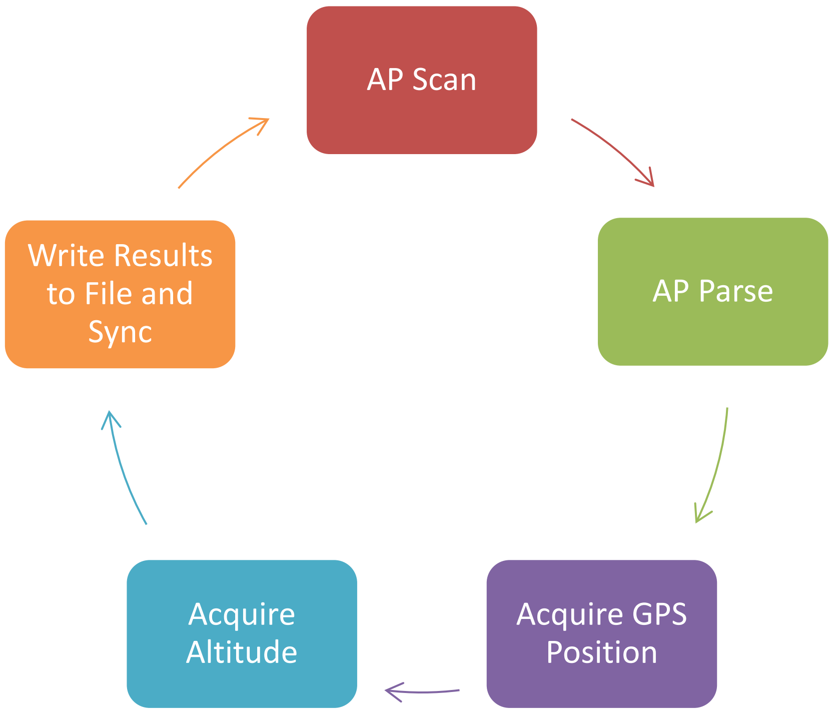


Figure 4-3: Data Collection Cycle

Since the entire purpose of the module was to perform data collection, this script was called at boot-time using an entry in `/etc/rc.local`. By removing and re-applying power to the data collection module a new log would be created every time. This made it possible to separate distinct flights into distinct files. Data collection results were written to the file after every sampling.

One problem that was identified early and remedied was caused by the way Python file operations are buffered by the operating system. Raspbian uses the journaled ext3 filesystem which stores changes in a disk transaction journal and later makes the actual change in the correct place on the storage medium. When Python attempts to write changes to a file, the modifications would be written in the journal but not written to disk until the operating system performed a file-system synchronization upon recovery. If a file-system synchronization did not occur before the power was removed the file contents would remain in the journal without being written into the file. To ensure that data was not omitted from the end of the flight a flush disk transactions request was included in the data collection loop to write the pending changes from the journal.

4.6 Analysis and Visualization Script Description

Several toolkits exist that provide the tools for visualizing this type of data. The Google Earth Toolbox for Matlab and Python[7] (Davis 2011) and the KML Toolbox[8] (Oliveira) provided useful functions and objects. Several Matlab and Python scripts were written using these libraries to assist in interpreting and visualizing data and are included in the appendices.

4.6.1 GPS Precision Script

A Matlab script was written to determine a precision figure for a GPS log, assuming that the GPS was given sufficient time to obtain a lock, and was not moved for the duration of the data collection.

1. Import data in Excel format
2. Convert latitude & longitude to meters
3. Calculate the standard deviation for combined latitude and longitude in meter units.

[7] "Google Earth Toolbox." http://www.mathworks.com/matlabcentral/fileexchange/12954-google-earth-toolbox.
[8] "KML Toolbox." http://www.mathworks.com/matlabcentral/fileexchange/34694-kml-toolbox-v2-7.

4.6.2 2-D KML Visualization

A Python script was written to convert the log files generated by the Data Collection script and create a Google-Earth Compatible KML file for visualization of the individual data points collected.

4.6.3 2-D Data Interpolation and Visualization

A Matlab script was written to import and visualize filtered interpolated data on a given access point in two-dimensional space.

1. Import the data in Excel format.
2. Create the 2-d interpolated grid.
3. Color the points according to signal strength.
4. Render the visualization.

4.6.4 3-D Data Interpolation Slice Visualization

A Matlab script was written to import and visualize data on a given access point in three-dimensional space by interpolating known points across a three-dimensional grid. These points are exported to a KML file.

1. Import the data in Excel format.
2. Create a 3 dimensional matrix of query points for interpolation.
3. Use known points to interpolate query points across the matrix volume.
4. Render a slice at the altitude mean.

5. Attach a function to the scroll-wheel to move the slice on the horizontal plane.
6. Re-render horizontal slice upon scroll movement.

4.6.5 3-D Data Interpolation Point KML Visualization

A Matlab script was written to import and visualize data on a given access point in three dimensional space by interpolating known points across a volume, and generating points reflecting the signal quality at the location.

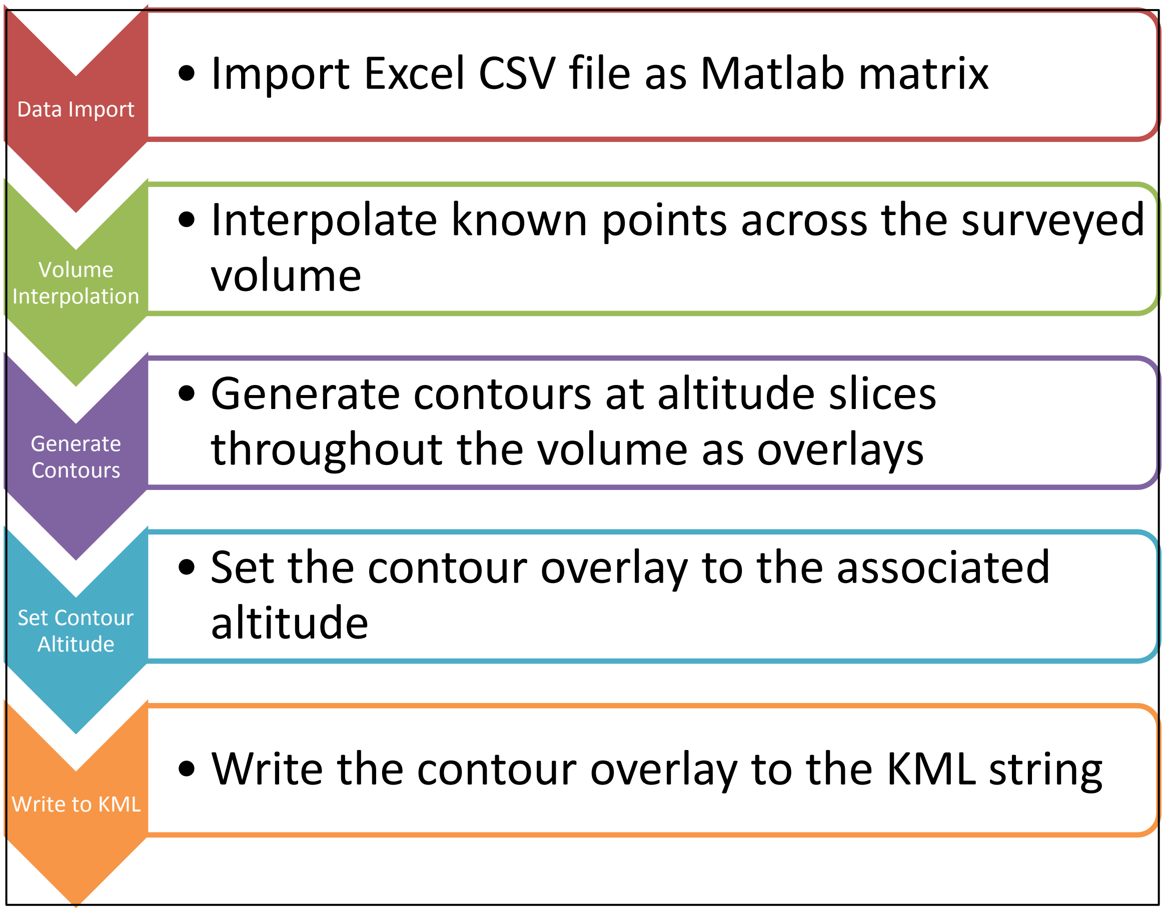
1. Import the data in Excel format.
2. Create a 3 dimensional matrix of query points for interpolation.
3. Use known points to interpolate query points across the query matrix volume.
4. Set the point icon according to signal quality associated with the point.
5. Generate a KML point for each point in the volume.
6. Write the KML string to a file.

4.6.6 3-D Data Interpolation Contour KML Visualization

A Matlab script was written to import and visualize data on a given access point in three dimensional space by interpolating known points across a volume, and generating contours at several slices. This was a manipulation of the topographical map generating function, which is typically used to create contours at increasing altitudes. By specifying that all contours for a given slice were to be placed on the same plane, and manually setting the altitude of the contour object to the desired altitude it was possible to generate the desired visualization. These contour sets are exported to a KML file.

The KML Toolbox was intended to show a finite number of levels in a given dataset. The distinct levels were determined by the data provided to the contour function. This caused each contour slice with local maximum and minimum values to be assigned the color of the maximum or minimum respectively. As the KML Toolbox didn't maintain value consistency across contours, the toolbox was modified to allow for value consistency across multiple contours. Feedback was given to the toolbox author requesting manual selection of maximum and minimum values to be included in future releases.

1. Import the data in Excel format.
2. Create a 3 dimensional matrix of query points for interpolation.
3. Use known points to interpolate query points across the matrix volume using a linear interpolation algorithm.
4. Iterate through the volume by altitude.
    a. Generate a contour set on link quality.
    b. Set the altitude of the contour set.
    c. Add the contour set to the KML string.



- Import Excel CSV file as Matlab matrix
- Interpolate known points across the surveyed volume
- Generate contours at altitude slices throughout the volume as overlays
- Set the contour overlay to the associated altitude
- Write the contour overlay to the KML string

Figure 4-4: KML Generation Process

5. RESULTS AND ANALYSIS

Results of the data collection and visualizations are provided. Problems and limitations discovered in the data collection process are identified.

5.1 Multi-Rotor Results

The following sections describe the results of the multi-rotor build process and flight performance.

5.1.1 Multi-Rotor Build Issues

Initial testing showed the configuration to be slightly more powerful than the flight controllers anticipated build. This was made manifest in 6-10Hz oscillations of approximately five degrees off normal in pitch and roll axes, which would increase if unchecked to the point that the platform would crash. As a result, an amount of tuning was required in the proportional figure of the rate control loop to reduce these oscillations. The initial rate proportional value, used to determine the amount to change the duty cycle of a motor to effect a change in attitude, was .175 which was slowly reduced to .08. Once this tuning was completed the pitch and yaw oscillations disappeared, leaving a stable and responsive platform.

During the period of testing, there were several crashes, typically resulting in the glass fiber motor booms snapping near the motor mount. This break point on the motor boom acted in the same way a as a vehicular crumple zone, expending the energy of the crash in a break in the inexpensive and modular frame component, rather than causing more expensive and difficult to repair damage to the motors or electronics.

Double-sided mounting adhesive was used at first to mount the telemetry unit. This provided a very firm connection between the telemetry unit and the frame. In several instances a hard landing, while not causing any structural damage, would cause the telemetry unit antenna to bounce. This bounce placed additional strain on the SMA antenna connector, snapping the solder mounts which were responsible for both conductivity and mechanical connection to the antenna. Replacement of the mounting adhesive with Velcro permitted the telemetry unit to move slightly, distributing the impact and preventing damage to the antenna connector.

5.1.2 Multi-Rotor Performance

With competent piloting skills, it was possible for the multi-rotor to perform vertical takeoff, maintain a loose hands-off loiter, be flown within a given area, and be flown in the vicinity of buildings. In the absence of winds over 10 mph an experienced pilot can maneuver the multi-rotor safely within 2-3 meters of walls, trees, and other obstacles.

5.1.3 Flight Time Test

With the 4000Mah battery and attached data collection module, the multi-rotor was capable of maintaining a hover for an average of eight minutes and forty-four seconds prior to initiating the fail-safe descent at 80% of battery capacity. Continuing to discharge the battery past this point can cause damage to the battery and runs the risk of sudden power loss. It was determined that to prevent loss of power while airborne, flights would be limited to a six minute maximum.

5.2 Data Collection Module Results

The following sections describe the data collection module performance results.

5.2.1 Data Collection Module Build Issues

The assembled data collection module was built and tested independently from the multi-rotor. Initially, stability issues were present with the USB wireless network card, the cause of which was traced to insufficient current being provided through the USB interface. A modification was done to bypass the poly-fuse restricting current supply to the USB interfaces which permitted an increased current draw and has not as yet shown any negative results.

Standalone data collection module testing took place by allowing two minutes to acquire satellites, and walking the module around a perimeter block with some known access points, and inspecting the results. Initial testing showed the altitude as determined by the GPS receiver to have wildly erroneous altitude changes, showing a range of over 30 meters while in a static location. As a result a barometer was included to determine altitude. This decreased the altitude range to a much more acceptable 2.26 meters and a standard deviation of 0.52 meters.

Table 3: Altitude Accuracy

Barometer Range	GPS Range
2.26m	>30m

Some refinements to the script were made over time to correct for errors. The libraries used to interface with the barometer were capable of determining altitude from the pressure reading provided by the barometer, but as barometric pressure at a given altitude can vary significantly with weather the ground altitude provided was often incorrect by 30-65 meters. By taking an initial reading at ground level and subtracting this number from all future readings a relative altitude was obtained.

The combined standard deviation of the latitude and longitude provided by the GPS receiver on the data collection module at a static location over a five minute period came to 0.24 meters. When mounted to the multi-rotor and in close proximity to noise generated by the radio equipment, ESCs and motors at hover throttle, the standard deviation increased to 0.63 meters, maintaining sub-meter precision. It is worth noting that again in these tests, two minutes elapsed between powering on the GPS receiver and taking readings to allow for satellite acquisition.

5.3 Flights and Visualization Results

Several different approaches were made at visualizing the data.

1. Logs were parsed directly into a KML format, using coordinate information to place a point and link quality to determine the color of the point. Points were broken into folders, allowing a given SSID name to be enabled or disabled in a KML viewer such as Google Earth.

This allowed for quick confirmation that the entirety of the flight had been recorded and was used to identify and filter out data for the desired access point.

2. Recorded points were interpolated across the surveyed grid and selected slices rendered. This provided utility in obtaining an illustration of coverage within a single horizontal plane.

3. Recorded points for three dimensional flights were interpolated across the surveyed grid and exported as coordinates to a KML.

4. Recorded points for three dimensional flights were interpolated across the surveyed grid and exported as contour slices to a KML. This type of illustration is subject to obscuring some areas depending on the camera positioning, but allows for an all-in-one visualization of multiple planes at once.

5.3.1 Linear Flight Visualization

An access point was placed centrally in this area, and the multi-rotor was flown at an altitude of approximately two meters and a velocity of 2-3 m/s. The low precision of these figures are a result of wind, momentum, piloting error, and other factors inherent in outdoor flight. Figure 5-1: Linear KML shows the locations and link quality of individual data points collected over the course of one of the linear flights. The results show that, as could be expected, link quality was higher at positions closer to the AP[9].

[9] This and all following satellite imagery are obtained from Google Earth and are used in accordance to the Google Earth acceptable use policy.

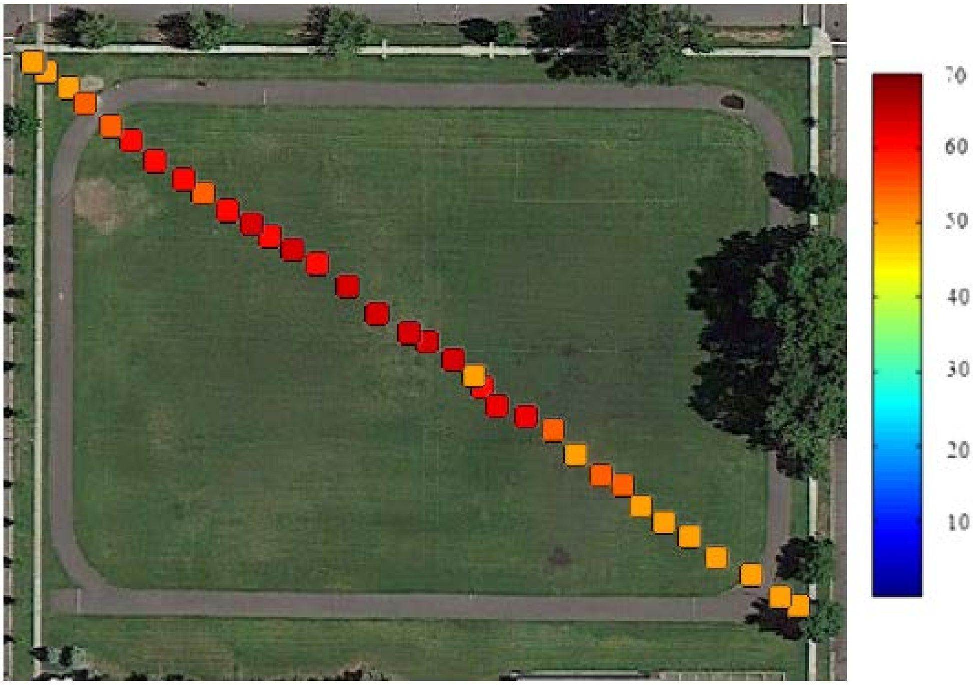


Figure 5-1: Linear Point KML

KML Interpolation Contour script was used to convert this data into a contour. In contrast to the point KML, this contour illustrates smaller differences in link quality, and determines the distances at which signal strength appears to have greater drop-off.

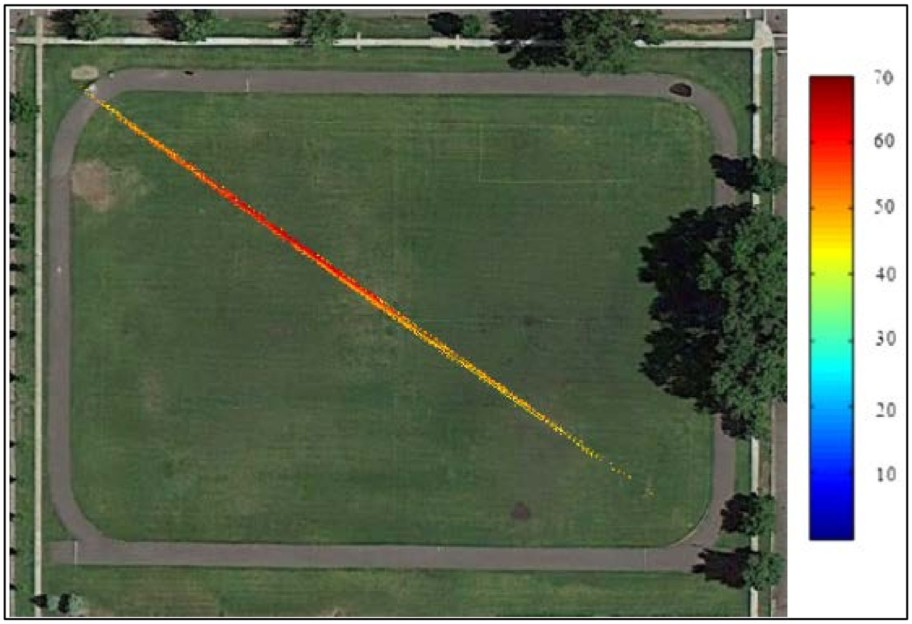


Figure 5-2: Linear Contour

5.4 Planar Flight Visualization

The multi-rotor was flown around the perimeter of the area, with a central access point. As seen in Figure 5-3: Planar KML, the corners of the flight have a lower signal quality, as they are at a greater distance from the centrally located AP. Greater signal strength in one area near the north (top) of the figure suggests that the antenna may be directionally focused.

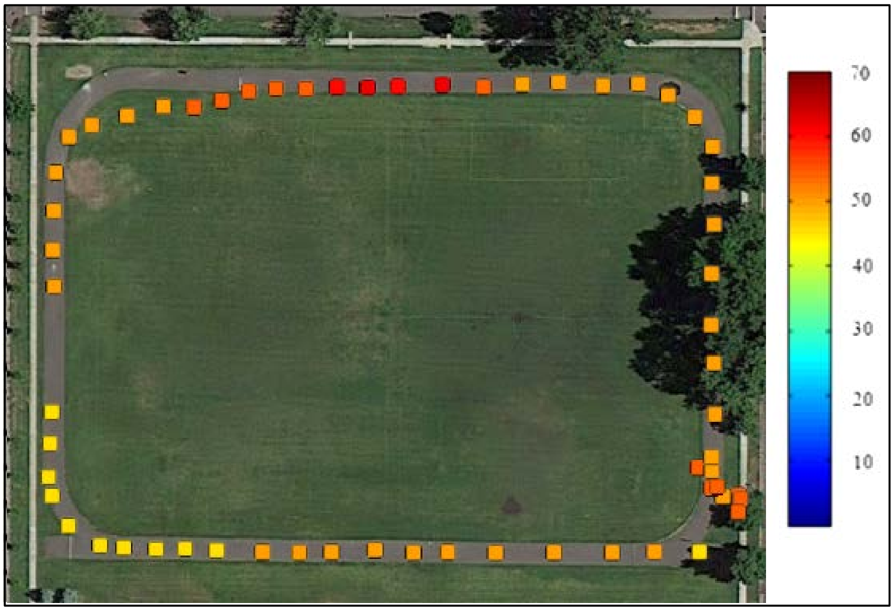


Figure 5-3: Planar KML

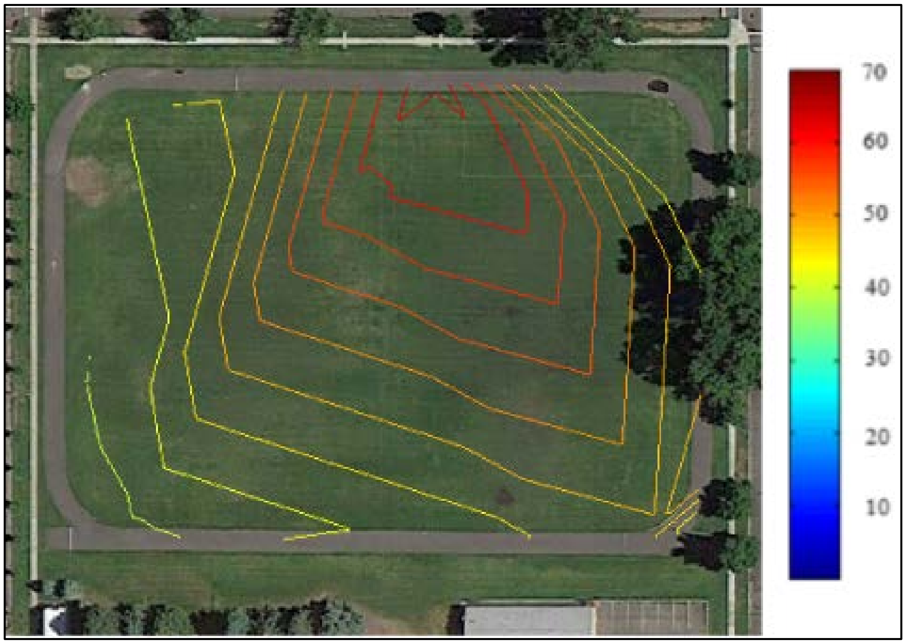


Figure 5-4: Planar Contour

The contour visualization in Figure 5-4: Planar Contour, shows the same information in a contour slice. Due to the fact that data from the center of the area was not collected, the interpolation suggests that the strongest link quality would be had on the top of the perimeter. This suggests that the perimeter flights reveal some amount of useful data, but combining the perimeter flight with a diagonal flight would increase data value and accuracy.

5.4.1 Multi-Plane Flight Visualization

A multi-planar flight was done over a quarter of the anticipated coverage area of the placed access point. During the flight altitude was changed to collect readings from multiple heights. The interpolated results suggest that at a given distance from the access point, a better connection may be had at 10 meters above ground compared to five meters above ground. Figure 5-5: Volumetric Interpolated KML displays the collected data and Figure 5-6: Volumetric KML displays a selection of the linearly interpolated values.

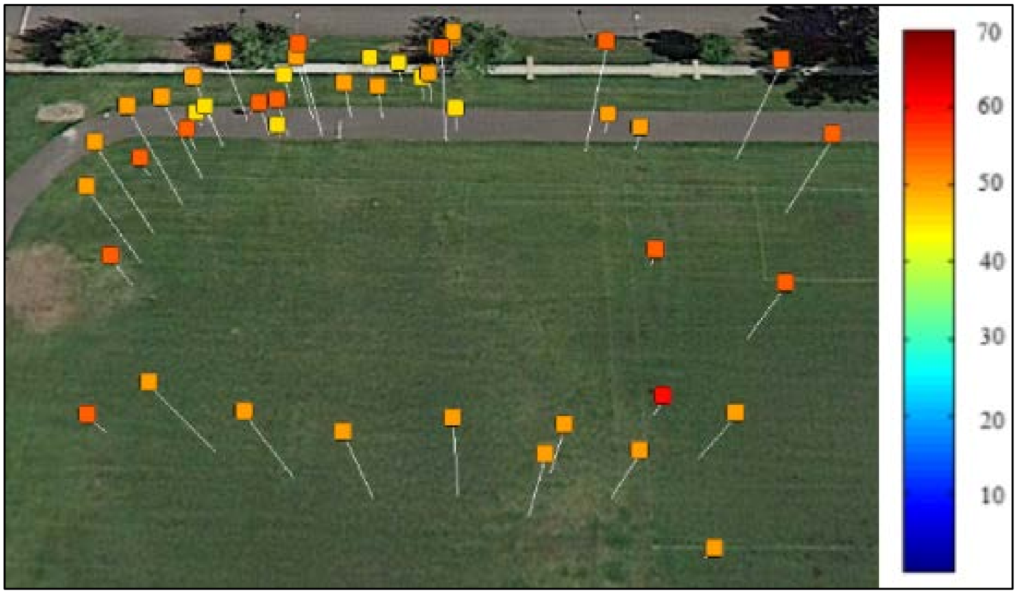


Figure 5-5: Volumetric KML

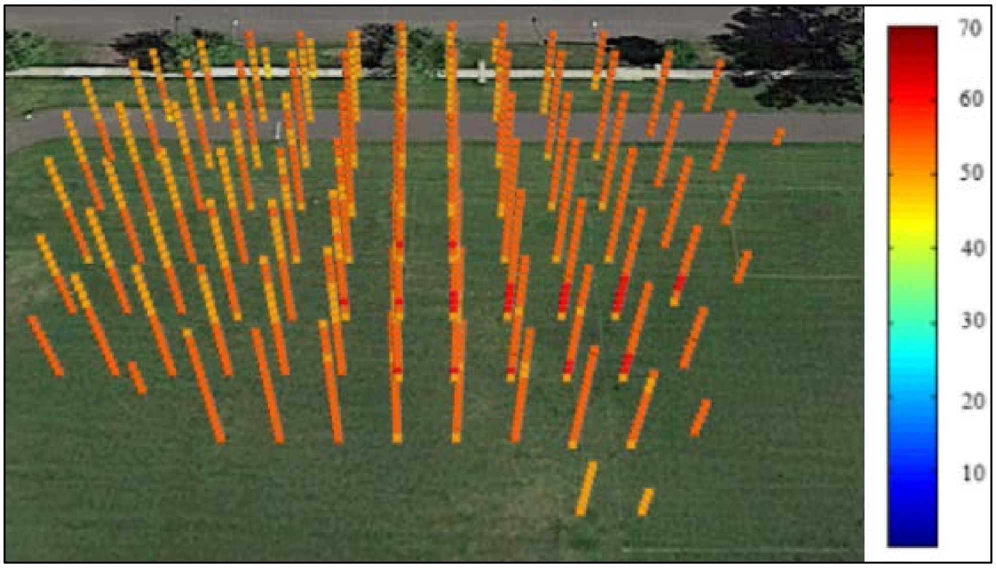


Figure 5-6: Volumetric Interpolated KML

Planes from the interpolated data were selected at five and ten meters, and used to generate contour maps. This illustrates one method of visualizing the data layer by layer.

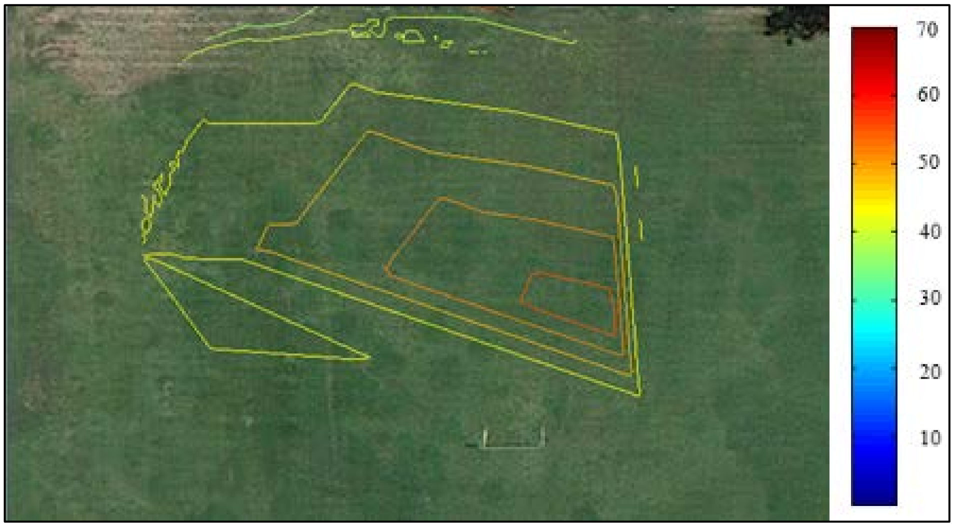


Figure 5-5: Contour at 5m

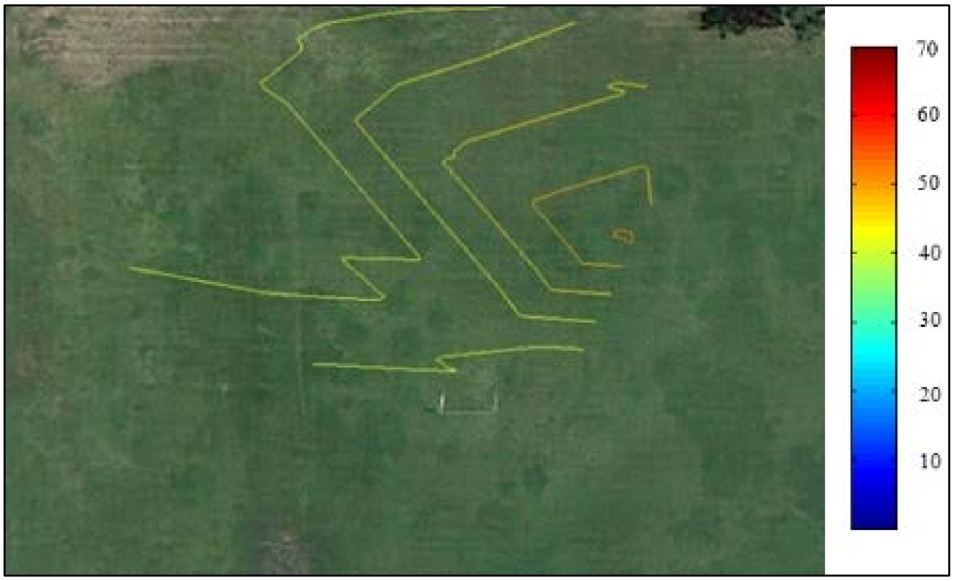


Figure 5-6: Contour at 10m

5.4.2 Structure Flight Visualization

Having established a reasonably stable flight platform and a functional data collection unit, structure assessments were started. Two flights were made on the south and west sides of an eight story building and their logs combined. Almost 300 access points were detected and mapped, but the following figures illustrate a single AP located within the building on the south-east side, appearing closest the camera. This access point was placed by campus technology and was intended to provide connectivity to those on the east side of the ground floor.

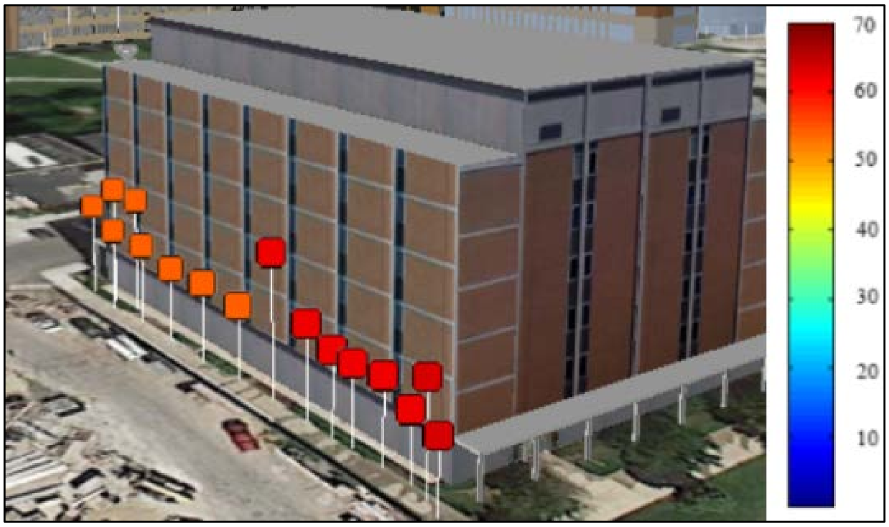


Figure 5-7: Structure KML

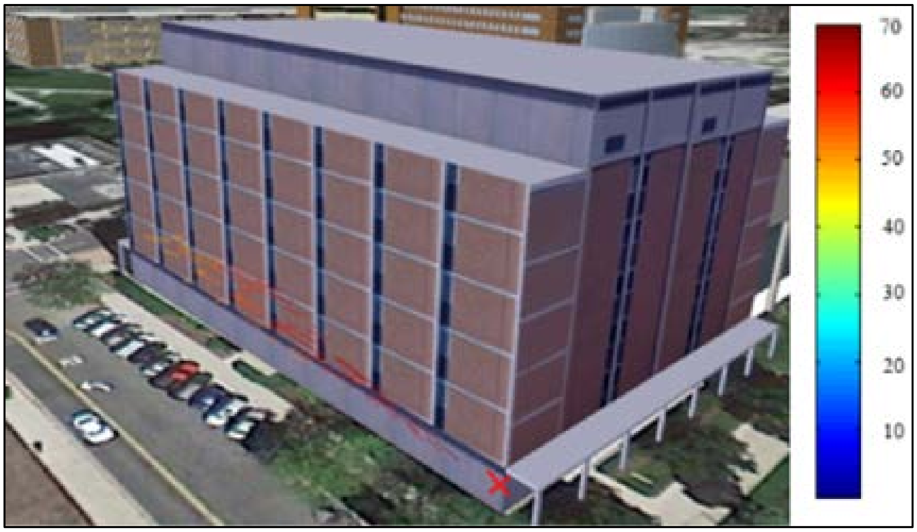


Figure 5-8: Structure Contour

The following image depicting the south and east sides of the building was generated by interpolating the data across the area, and drawing contours at .5m intervals. To provide context, the building is nineteen meters high, and a red "X" has been drawn at the point of the access point. The previous figure as well as the following illustrate that an attacker outside of the building is still within the coverage area of the access point.

Figure 5-10: Structure Contour also illustrates that the coverage area of the access point widens vertically as the distance from the access point increases. This is congruous with the doughnut-shaped coverage area typical of such an access point.

In the duration of the structure flight, several access points were identified which were not placed by campus technology.

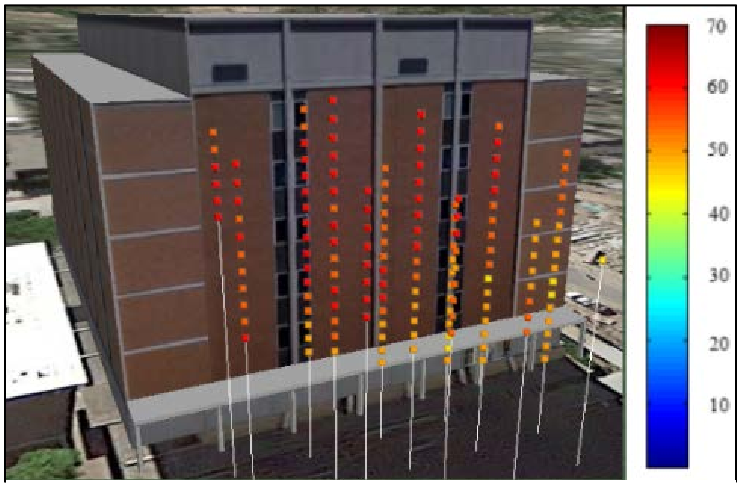


Figure 5-9: Interpolated Rogue AP

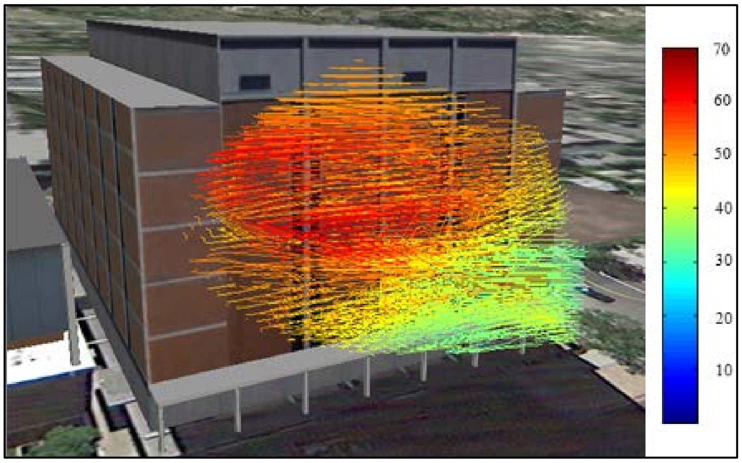


Figure 5-10: Rogue AP Contour

Figures 5-11 and 5-12 illustrate the west side of the building and was filtered on a rogue access point, not authorized for placement, also representing a potential security risk to the campus network. The interpolated contour plot suggests that link quality is strongest near the north-west corner of the building on the fourth and fifth floors.

5.5 R1 Analysis

R1: Is a multi-rotor UAV a suitable platform for collecting geo-located wireless spectrum data?

In respect to the first research question, the results suggest that a multirotor is suitable in collecting geo-located wireless spectrum data. The tested multirotor was capable of sustaining stable flight with the added weight of the data collection module. Noise associated with the multi-rotor does increase GPS receiver standard deviation by a factor of two, however the resulting precision was still within a meter. This level of precision is still capable of providing useful data and would be considered tolerable in most applications. Results of the data provided by the multi-rotor were deemed useful in identifying areas within which an attacker could receive data from or interfere with the access point, as well as establish the highest link quality area, from which access point location can be approximated.

5.6 R2 Analysis

R2: How does performing a 3D site survey using a multi-rotor UAV compare with alternative 3D site survey approaches in regard to speed, accuracy, safety, and cost?

In respect to the second research question, a multi-rotor provides several benefits when compared to other site surveillance methods, while lacking in others.

Speed: In performing the multi-rotor tests speed appeared to be a primary benefit, even in two-dimensional site surveys. While slower than most fixed-wing aircraft of similar size, the multi-rotor is capable of moving as quickly as 20m/s. The benefit of this speed however is tempered by the sampling rate of the data collection module. This results in a speed and accuracy tradeoff. Regarding three dimensional assessments, there exists no close comparison, but the multi-rotor can be considered substantially faster than other imaginable alternatives, such as dangling the data collection module off the roof or climbing up and down a ladder.

Accuracy: The standard deviation of horizontal precision was found to be .63 meters, and the standard deviation of altitude precision was found to be .52 meters. This is substantially less accurate than a static receiver or collection of receivers, such as an anechoic chamber, but is certainly comparable to assessments performed in production deployments. The geo-location range remains accurate enough to provide actionable intelligence. A multirotor has several benefits over other potential airborne transportation platforms, notably fixed-wing aircraft, in that it has no requirement for constant forward motion. This allows the multirotor to navigate in areas that would be inaccessible to other unmanned aircraft. In comparison to a manual three dimensional test, the equipment used to collect GPS and Link Quality information would likely be comparable.

Cost: In a two-dimensional site survey, the entire cost of the multi-rotor, an approximate $700, could in many situations be considered superfluous, as the data collection module could be carried by hand. In regards to three dimensional assessments, it is also initially more expensive, albeit more efficient, than manual methods of accessing the same areas such as using a ladder or rope suspension. The increase in time required to perform the assessment also leads to an increase in cost, as wages must be paid to have personnel conduct the assessment.

Safety: A multi-rotor is certainly not without risks. Pilot error aside, the high maneuverability, speed, and dependence upon physical sensors make it possible for an improperly tuned multi-rotor to behave erratically. Considering the high speed at which the propellers are rotated, contact with buildings or people will always end badly. While a thorough investigation has not been done, many anecdotal incidents provide legitimacy to the risks of multirotor flight (Mortimer 2013). These same issues are present with fixed-wing aircraft, and compounded by higher speed flights. Performing manual assessments presents a different type of risk in that an assessor may need to either climb a ladder, or perform the assessment from the top of the building.

Table 4: 3D Assessment Method Comparison

	Multi-Rotor UAV	**Fixed-Wing UAV**	**Manual**
Speed	High	High	Low
Cost	Moderate initial cost Low operations cost	Moderate initial cost Low operations cost	Moderate initial cost Moderate operation cost
Accuracy	High	Low, due to inaccessible areas	High (Where feasible)
Safety	Moderate Risk	High Risk	Low/Moderate Risk

5.7 R3 Analysis

R3: Is currently available open-source GPS-assisted waypoint navigation sufficiently accurate to execute a preplanned, autonomous three-dimensional wireless assessment?

Prior to attempting autonomous flight the navigation GPS was inspected for reliability. Unfortunately occasional GPS glitches would occur, as illustrated in the following figure. This figure illustrates the GPS readings in latitude over the course of a single flight. The X-axis portrays the reading number, *not* the time at which the reading occurred. Erroneous readings occurred near GPS readings 800 and 1200, causing a significant rise and fall in the latitude reading, in these cases equal to approximately 15 meters. This type of behavior was consistent across several flights.

In spite of this, several flights took place in an attempt to perform autonomous surveys. These commenced with determining the ability of the multi-rotor to utilize the "loiter" mode with a tight, one meter radius which is a prerequisite to fully autonomous flight. GPS glitches occurred at several times causing erratic movement and forcing the pilot to switch back to manual control.

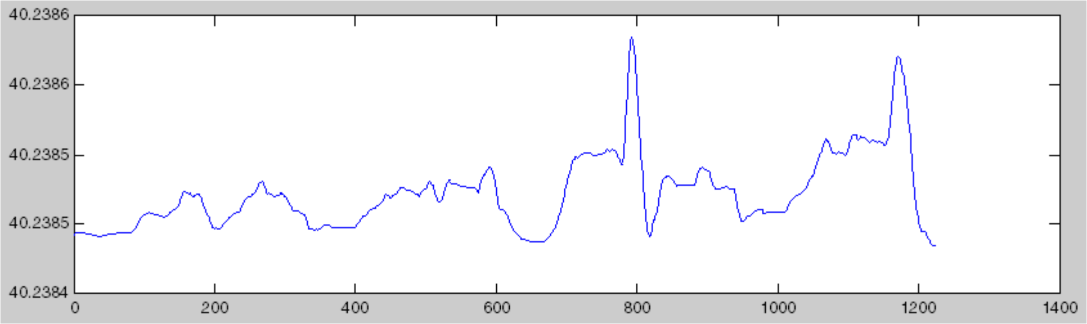


Figure 5-9: GPS Latitude Glitch

The data-collection module suffered occasional GPS glitches as well, but as it was not responsible for navigation there was a much smaller impact. GPS glitches also appeared less frequently, which is likely a result of the significantly lower sampling rate. The multi-rotor was sampling the GPS at the maximum rate, which made it react to all GPS data glitches. The GPS glitch issue may be correctable by using other sensors to mitigate the effects of wildly inaccurate data, and some flight controllers have recently started to use such a technique.

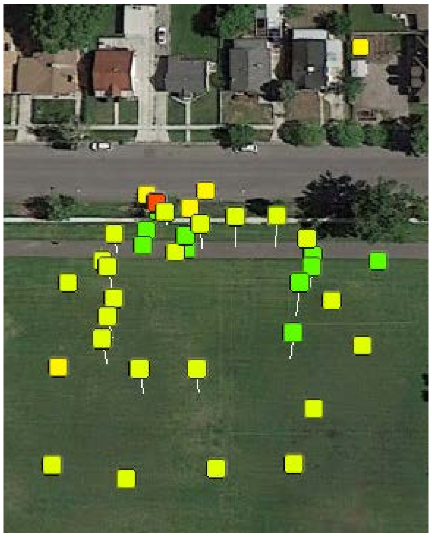


Figure 5-10: Data Collection GPS Glitch

Additionally, metallic objects such as buildings had an accumulative effect on the magnetometer. The flight controller primarily uses the gyroscope to determine changes in heading, and uses the magnetometer to correct gyroscope drift. Buildings in the proximity introduce changes to natural magnetic fields, which causes a magnetometer to provide bad results. This prevents magnetometer readings from being sufficiently accurate to prevent gyroscope drift. The flight controller limited magnetometer correction over time which prevented violent yaw “corrections” but the issue was made manifest in gyroscope drift which was visible in manual flight near buildings. As the effect was very slow, approximately one degree every 15 seconds, it was a simple matter to counter this while in manual flight; automated flight however relies heavily upon heading determination. This makes for a very unsafe automated flight situation in which attempts to correct positioning as determined by GPS coordinates are applied in the incorrect direction, which places the multi-rotor further from the intended location. As the GPS readings provide information to the multi-rotor that it is getting increasingly off-course, more aggressive acceleration is made in pitch and roll until either manual control is assumed or a crash occurs. The inability to correct for gyroscope drift presents a difficult problem for autonomous heat-mapping in the proximity of buildings with ferrous construction materials. Due to the instability and lack of reliability in auto flight mode, autonomous tests were suspended to prevent damage to persons or property.

6. CONCLUSIONS AND FURTHER WORK

6.1 Conclusion

A multi-rotor appears to be a capable platform for conducting three dimensional wireless site surveys. The maneuverability and low groundspeed allowed by the platform makes it possible to collect data in areas that would otherwise be very difficult to obtain. Drawbacks to use of a multi-rotor in such an application are limitations in flight time as a result of battery-life, and limitations in autonomous flight. Issues presented by GPS glitches and magnetometer drift make autonomous flights in close proximity to buildings unsafe. Data collected by performing manual flights is sufficiently accurate to provide actionable information on the three-dimensional coverage area of a wireless network. Further work has been identified to further explore the capabilities and security of a UAV in three dimensional wireless assessment.

6.2 Future Work

Suggested further work to follow this research includes the following items.

Data Collection Module Survey: Additional work could be done to identify and compare alternative data collection modules on the basis of weight, power consumption, antenna characteristics, and sampling frequency. The Raspberry Pi was selected for this research on the basis of its weight, price, and availability. Possible alternatives that may have a power, weight, or processing advantage to the Raspberry Pi may include the BeagleBone[10], one of the Arduino boards with appropriate shields (Al-Kadi, Al-Tuwaijri, and Al-Omran 2013), or a custom-built solution.

Increase Surveyed Spectrum: This research limited itself to performing assessments on 802.11 wireless access points. Future research may include the use of a different receiver or a software defined radio (SDR) to collect link quality or signal strength data in different spectra. Example ranges include ZigBee in 512MHz, BlueTooth in 2.4GHz, Cell Phone Technologies, and Radio Frequency Identification (RFID) systems which span a range of frequencies.

Flight Controller Survey: This research chose the APM 2.5 Arducopter based on price, availability, and ability to be tuned to different payloads and motor weights. A further analysis of flight controllers, including prebuilt platforms, may be pursued in an effort to identify a multi-rotor capable of more reliable autonomous flight. Potential alternatives include the DJI Wukong and Naza[11]. These flight controllers are notably more expensive than the APM 2.5 used in this research.

3D Assessments over Time: This research was intended only to identify the coverage area of an AP at a given point in time. Further research may include performing multiple site surveys over a time period to determine the effect of any temporal variables in coverage area.

Transmitter Security Assessment: The multi-rotor used in this research used a 2.4GHz transmitter. A binding process is performed to use a given receiver with a given transmitter. An analysis of the security of this binding process would be useful in determining the possibility of an attacker hijacking a similar platform. This is conceptually close to the “skyjack” project.

[10] “BeagleBone.” http://beagleboard.org/Products/BeagleBone
[11] DJI Official Site. http://www.dji.com/

Swarm Assessment: Research is being conducted in swarm dynamics using multi-rotors and other aerial platforms. Significant challenges exist in moving this practice into an uncontrolled environment with obstacles, but the use of two or more platforms would likely significantly decrease the amount of time it takes to perform an assessment.

Directional Antenna: By using a directional antenna mounted on a rotating gimbal it may be possible to achieve additional information regarding the placement of an access point within a building or elsewhere.

REFERENCES

3DRobotics. 2012. “Arducopter Motor Setup.” http://copter.ardupilot.com/wiki/motor-setup/.

Abramson, N. 1970. “THE ALOHA SYSTEM: Another Alternative for Computer Communications.” *AFIPS Joint Computer Conference*: 281–285. http://dl.acm.org/citation.cfm?id=1478502.

Ahmed, A. 2008. “UAV BASED MONITORING SYSTEM AND OBJECT DETECTION TECHNIQUE.” *Archives* XXXVII (Commission 8): 373–378.

Aked, S., C. Bolan, and M. Brand. 2012. “An Investigation into the Wi-Fi Protected Setup PIN of the Linksys WRT160n V2”: 28–35.

Al-Kadi, T., Z. Al-Tuwaijri, and A. Al-Omran. 2013. “Arduino Wi-Fi Network Analyzer.” *Procedia Computer Science* 21 (January): 522–529. doi:10.1016/j.procs.2013.09.073.

Alvissalim, M. S., B. Zaman, A. Hafizh, Z. M. Ma, J. Wisnu, and J. P. Mursanto. 2012. “Swarm Quadrotor Robots for Telecommunication Network Coverage Area Expansion in Disaster Area”: 2256–2261.

Appelbaum, J., J. Horchert, and C. Stöcker. 2013. “Shopping for Spy Gear.” *Der Spiegel*. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Beck, M., and E. Tews. 2008. “Practical Attacks Against WEP and WPA”: 1–12.

Bellardo, J., and S. Savage. 2003. “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions.” In *USENIX Security Symposium*.

Berghel, H. 2004. “Wireless Infidelity I: War Driving.” *Communications of the ACM* 47 (9): 21–26.

Committee of Criminal Justice and Public Safety. 2013. *Prohibiting Images of a Person’s Residence to Be Taken from the Air.* New Hampshire Liberty Alliance.

Davis, S. 2011. “Google Earth Toolbox.” http://www.mathworks.com/matlabcentral/fileexchange/12954-google-earth-toolbox.

Diamond, S. M., and M. G. Ceruti. 2007. “Application of Wireless Sensor Network to Military Information Integration.” *IEEE* (1-4244-0865-2): 317–322.

Federal Aviation Administration. 1981. *Model Aircraft Operating Standards*. Department of Transportation.

Hills, A. 2004. “Rollabout : A Wireless Design Tool.” *IEEE Communications Magazine* 42 (February): 132–138.

IEEE. 1997. *Telecommunications and Information Exchange Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

———. 2012. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. *IEEE-SA Standards Board*. Vol. 2012.

Kamkar, S. 2013. “Skyjack.” http://samy.pl/skyjack/.

Kershaw, M. 2012. “Kismet.” http://www.kismetwireless.net/.

Krishnan, A. 2009. *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Burlington, VT: Ashgate Publishing Limited.

Leiteritz, R. 2010. *Google Statement on WIFI Collection*. Vol. 4. http://www.google.com/googleblogs/pdfs/google_submission_dpas_wifi_collection.pdf.

Machowinski, M. 2013. *Wireless LAN Market up 12% in 2Q13*. Boston, MASSACHUSETTS. http://www.infonetics.com/pr/2013/2Q13-Wireless-LAN-Market-Highlights.asp.

Microsoft. 2000. “Ten Immutable Laws of Security (Version 2.0).” *Technet*. http://technet.microsoft.com/en-us/library/hh278941.aspx.

Mortimer, G. 2013. *Multirotor Crashes into Crowd*. Spain. http://www.suasnews.com/2013/09/25136/multirotor-crashes-into-crowd-spain/.

Oliveira, R. “KML Toolbox.” http://www.mathworks.com/matlabcentral/fileexchange/34694-kml-toolbox-v2-7.

Reed, T., J. Geis, and S. Dietrich. 2011. “SkyNET : a 3G-enabled Mobile Attack Drone and Stealth Botmaster Approach Attack Framework.” *Framework*: 4–4. https://db.usenix.org/events/woot11/tech/final_files/Reed.pdf.

Shannon, C., and W. Weaver. 1948. “A Mathematical Theory of Communication.” *The Bell System Technical Journal* 27 (July): 379–423, 623–656. http://circuit.ucsd.edu/~yhk/ece287a-win08/shannon1948.pdf.

Sharkey, N. 2011. “The Automation and Proliferation of Military Drones and the Protection of Civilians.” *Law, Innovation, and Technology* 3 (2): 229–240.

Stubblefield, A, and A D Rubin. 2001. “Using the Fluhrer , Mantin , and Shamir Attack Using the Fluhrer , Mantin , and Shamir Attack to Break WEP.”

Tassey, M., and R. Perkins. 2009. “WASP: Wireless Aerial Surveillance Platform.” In *DEFCON 19*. http://www.defcon.org/images/defcon-19/dc-19-presentations/Tassey-Perkins/DEFCON-19-Tassey-Perkins-Wireless-Aerial-Surveillance-Platform.pdf.

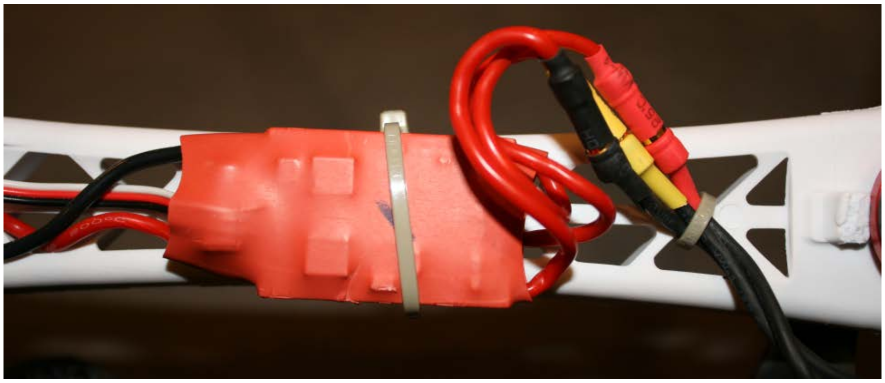
Visser, A., and N. Dijkshoorn. 2011. “Closing the Gap Between Simulation and Reality in the Sensor and Motion Models of an Autonomous AR. Drone.” *Proceedings of the …*. http://www.science.uva.nl/~arnoud/publications/DesignDecisions.pdf.

Zvanovec, S., P. Pechac, and M. Klepal. 2003. “Wireless LAN Networks Design: Site Survey or Propagation Modeling?” *Radioengineering*: 42–49. http://www.urel.feec.vutbr.cz/RADIOENG/fulltexts/2003/03_04_42_49.pdf.

APPENDICES

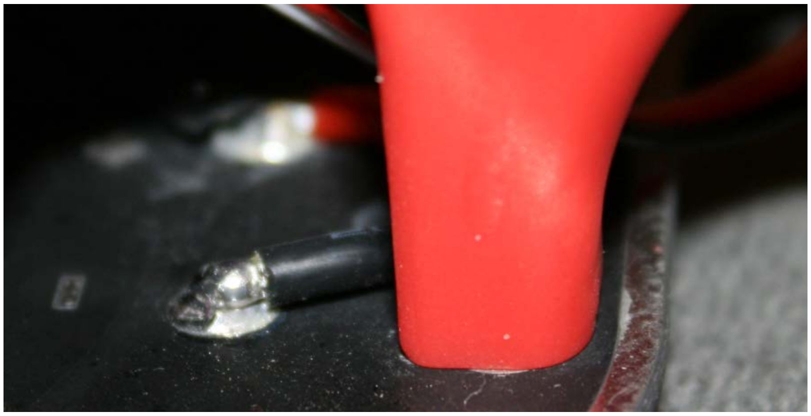
APPENDIX A: Multi-Rotor Build Process

The first part of the build process was to prepare the individual components. Female bullet connectors were soldered to the three leads on each ESC to be connected to the brushless motors, and male connectors were soldered to the motor leads. Shrink wrap was used to ensure that the connector was insulated as much as possible to prevent accidentally shorting between the leads, which were also color-coded to ensure that the appropriate leads could be switched to reverse motor direction as needed. The ESCs were labeled according to their place in the flight configuration, and mounted to the appropriate boom. Each ESC was attached using a small amount of double-sided mounting tape to prevent it from sliding lengthwise along the boom and connected to the boom with a small zip tie, making for a lightweight, easily replaceable, solid, and inexpensive placement.



Mounted ESC

The bottom plate of the frame to which the motor booms would later attach was a printed circuit board (PCB) and provided power distribution to the ESCs by means of exposed solder pads. A small amount of solder was applied to each of these pads and used to connect the leads to the ESCs 12V and ground leads. Once these connections were made, the bottom frame plate was screwed into the booms. The ESC control power, ground, and signal wires for all four ESCs were run down the boom towards the central platforms.

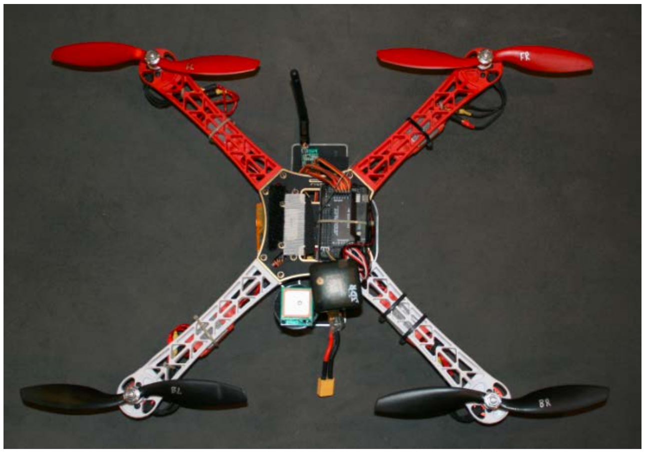


ESC to Frame Connections

The motors were then mounted. Due to the shape of the motor booms and the mounting surface of the brushless motors, a small part of the frame had to be cut away. This allowed the motors to be mounted solidly on the bottom of the motor booms with the shaft protruding up through the mounting holes. Propeller collets were attached to each of the motor shafts.

Modified Motor Boom Mount

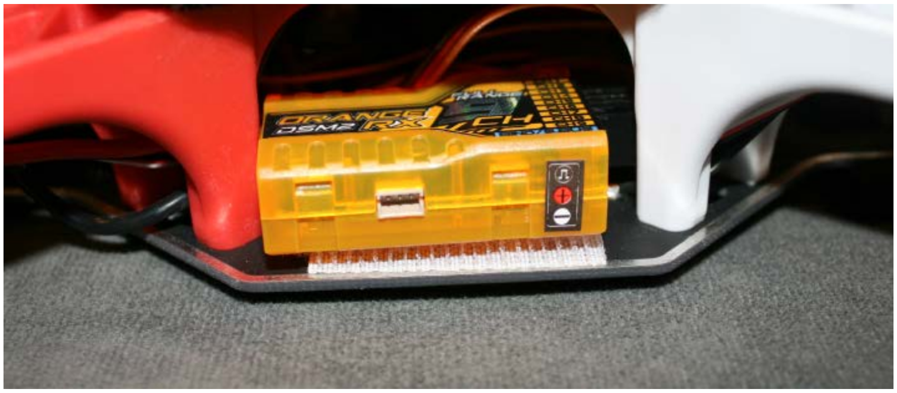
Counter-rotating propellers were attached to the collets, with clockwise-rotating pairs and counter-clockwise rotating pairs across from each other, as specified in the flight configuration documentation (3DRobotics 2012). Propellers were color-coordinated to provide heading orientation while in flight.



Assembled Multi-Rotor with Flight Controller

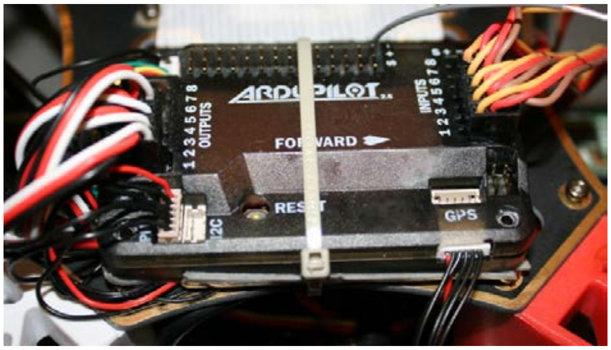
The 12V to 5V regulator and current/voltage monitor was soldered to the appropriate XT60 connectors for battery connection, and soldered to the pads on the side of the power distribution plate. The top plate was then screwed into the tops of the motor booms, providing both cover for the wiring and frame rigidity. The flight controller was mounted on the top plate using mounting adhesive and a zip-tie, and was placed on one half of the plate to leave space for the data collection module. Each of the ESC control lines, the ground and 5V lines from the power module, and the battery monitor lines were run through the top plate.

After initially using double-sided tape which later caused problems (see section 5.1.1), Velcro pads were adhered to the mounting surfaces on the bottom plate, to which was attached the telemetry and receiver units.



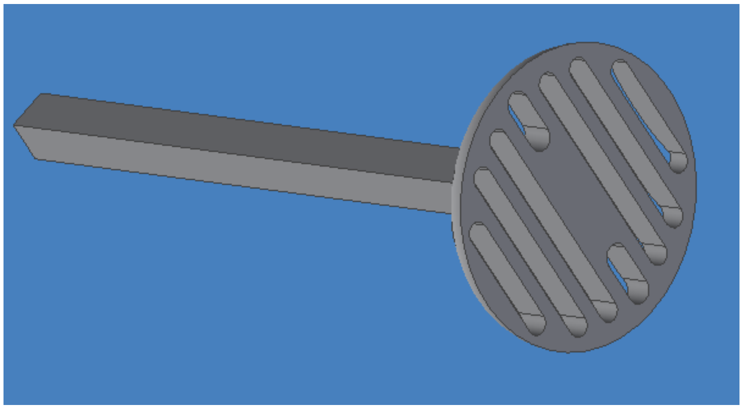
Mounted Receiver

After all of the components were mounted to the multi-rotor, each of the signal lines were connected to the flight controller including the power module, the ESC control lines, the receiver outputs, the GPS and telemetry.



Flight Controller

Using a 3D printer and CAD software, a pair of small vertical booms were created out of ABS plastic to provide a platform for the GPS. The use of a GPS boom is standard practice in most multi-rotor builds and is done to increase the surface area available for mounting hardware, as well as physically separate the GPS receivers from other components on the multi-rotor which are sources of noise and affect radio equipment.



GPS Boom CAD Drawing

APPENDIX B: Data Collection Python Script

```
import serial
import re
import subprocess
import time
from decimal import *
from pynmea import nmea
from Adafruit_BMP085 import BMP085
import os.path
import os

bmp = BMP085(0x77)
#Identify the next unused log file.
filenum = 0
fileset = False
while not fileset:
      filenum = filenum + 1
      filename = str(filenum) + ".log"
      if not os.path.isfile("/var/log/geolocate/" + filename):
            fileset = True

f = open("/var/log/geolocate/" + filename,'w')
f.write("\n")
f.flush()
os.fsync(f)
start_alt = bmp.readAltitude()
time.sleep(120)

#Set up the output lists

addresses = []
channels = []
qualities = []
signal_levels = []
essids = []
getcontext().prec = 10
getcontext().rounding = ROUND_FLOOR

#Set up the GPS object
```

```
gps = serial.Serial('/dev/ttyAMA0',9600,timeout=1)
gpgga = nmea.GPGGA()


#Start data collection
while 1:
    location = ""

    del addresses[:]
    del channels[:]
    del qualities[:]
    del signal_levels[:]
    del essids[:]

    gotAPs = False
    while not gotAPs:
        try:
            output =
subprocess.check_output(['iwlist','wlan0','scan'])
            output = output.splitlines()
            gotAPs = True
        except:
            #Sometimes the wireless doesn't work for a sec, just
keep trying.
            continue

    gotAP = False
    for line in output:
        try:
            address = re.search('Address:
(..:..:..:..:..:..)',line)
            if address is not None:
                addresses.append(address.group(1))
                gotAP = True

            channel = re.search('Channel:(.*)',line)
            if channel is not None:
                channels.append(channel.group(1))

            quality = re.search('Quality=(.*?)\/70',line)
            if quality is not None:
                qualities.append(quality.group(1))

            signal_level = re.search('Signal level=(.*?)
dBm',line)
            if signal_level is not None:
                signal_levels.append(signal_level.group(1))

            essid = re.search('ESSID:\"(.*?)\"',line)
            if essid is not None:
                essids.append(essid.group(1))
        except:
```

```
                  continue

      located = False
      gps.flushInput()
      gps.flushOutput()
      if gotAP:
            while (not located):
                  try:
                        data = gps.readline()
                        if 'GPGGA' in data:
                              #parse into a GPGGA object
                              gpgga.parse(data)
                              lat = Decimal(gpgga.latitude)
                              long = Decimal(gpgga.longitude)
                              #shift the decimal point and convert long &
lat into decimal degrees
                              lat = ((lat-(lat%100))/100)+(lat%100)/60
                              long = ((long-
(long%100))/100)+(long%100)/60
                              if gpgga.lon_direction == 'W':
                                    long*=-1;
                              if gpgga.lat_direction == 'S':
                                    lat*=-1
                              #Grab the barometer altitude, subtract the
starting altitude to get relative to ground
                              altitude = bmp.readAltitude()-start_alt

                              location = str(lat) + "," + str(long) + ","
+ str(altitude)
                              located = True
                  except:
                        #No GPS attached or no signal or some such
problem.
                        continue
            for idx, val in enumerate(addresses):
                  try:
                        f.write(essids[idx] + "," + addresses[idx] + ","
+ channels[idx] + "," + qualities[idx] + "," + signal_levels[idx] +
"," + location)
                        f.write('\n')
                        f.flush()
                        os.fsync(f)
                  except:
                        continue
            f.flush()
```

APPENDIX C: Analysis Scripts

GPS Precision Matlab Script

```
DATA = xlsread('figure.xlsx');
qual = DATA(:,2);
lat = DATA(:,4);
long = DATA(:,5);
 lat = lat *  111131.75;
 long = long * 85000;
lat = lat - min(lat);
long = long - min(long);
gps_fig = sqrt(var(lat) + var(long));
gps_fig

figure
scatter(lat,long);
```

2D KML Visualization Matlab Script

```
  function single_plane
      DATA = xlsread('Quad_11.xlsx');

      I = DATA(:,2);  % RSSI
      X = DATA(:,5);  % LAT
      Y = DATA(:,4);  % LONG

      % Create an empty grid of query points.
      [Xq,Yq] = meshgrid(max(X):-.000001:min(X), min(Y):.000001:max(Y));
      % Interpolate the known points across the query points to get a
  plane
     P = griddata(X,Y,I,Xq,Yq);
% Remove the black cell edges.

      pcolor(Xq,Yq,P);
```

```
    cm=flipud(jet);
    colormap(cm);
    colorbar;
    set(findobj(gca,'Type','Surface'),'EdgeColor','none')
end
```

3D Slice Visualization Matlab Script

```
function scroll_wheel2

   figure('WindowScrollWheelFcn',@figScroll);
   I=imread('selected_image.jpg');
   imshow(I)
   hold all
   [x,y] = ginput(1);
   x=round(x);
   y=round(y);
   plot(x,y,'r+');
   a=250;
   r1=x-a;
   r2=y-a;
   l=2*a;
   h=drawrectangle(r1,r2,l);
   set(h,'EraseMode', 'normal', 'LineStyle', ':')

   step=20;

   function figScroll(src,evnt)

        if evnt.VerticalScrollCount < 0

         r1i=r1-step;
         r2i=r2-step;
         li=l+2*step;

         drawnow
         set(h,'Position',[r1i,r2i,li,li])

         r1=r1i;
         r2=r2i;
         l=li;

      elseif evnt.VerticalScrollCount > 0

         r1i=r1+step;
         r2i=r2+step;
         li=l-2*step;
         if li>20
```

```
            drawnow
            set(h,'Position',[r1i,r2i,li,li])

             r1=r1i;
             r2=r2i;
             l=li;

      end
   end %figScroll

end % scroll_wheel
```

KML Point Visualization Python Script

```
import sys
import simplekml
import time
kml = simplekml.Kml()
filename = sys.argv[1]
f = ""
for arg in sys.argv:
      print arg

try:
      print "Opening " + filename + " for map data"
      f = open(sys.argv[1])
except:
      print "Unable to open map data"
      time.sleep(60)
      exit()
input = f.readlines()
documents = {}
print "Parsing GPS & Wireless Data"
count = 0;
for i, point in enumerate(input):
      try:
            if i%100 == 0:
                  print i
            count = i
            point = point.replace("\n","")
            parameters = point.split(",")
            if parameters[0] not in documents.keys():
                  newdoc = kml.newdocument(name=parameters[0])
                  documents[parameters[0]] = newdoc
            #print parameters
            pnt = documents[parameters[0]].newpoint(name="")
            #pnt =
documents[parameters[0]].newpoint(name=parameters[0])
            alt = parameters[7]
            alt = float(parameters[7])
            pnt.coords = [(parameters[6],parameters[5],alt)]
            pnt.altitudemode =
simplekml.AltitudeMode.relativetoground
            description = "ESSID = " + parameters[0] + "\n" +
"Quality = " + parameters[3] + "\nSNR = " + parameters[4]
            pnt.extrude=1
            pnt.description = description
            pnt.style.iconstyle.scale=.5
            #The link "quality" will be between 0 and 70
            quality = int(parameters[3])
            pnt.style.iconstyle.icon.href = '.\wp_images\img-
35.png'
            if quality > 40:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
40.png'
            if quality > 45:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
45.png'
            if quality > 50:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
50.png'
            if quality > 55:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
55.png'
            if quality > 60:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
60.png'
            if quality > 65:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
65.png'
            if quality == 70:
                  pnt.style.iconstyle.icon.href = '.\wp_images\img-
70.png'

      except:
            continue
print "Finished Parsing " + str(i) + " records."
print "Writing KML"
kml.save(filename + ".kml")
print "Map Creation Complete"
```

*Note: In KML point visualization, points color was determined by splitting link quality into groups of 5, ie 30-34, 35-39, 40-44, etc. This was done to reduce the number of icons required to produce the visualization. This technique was used for all KML point visualizations.

3D Point Interpolation Matlab Script

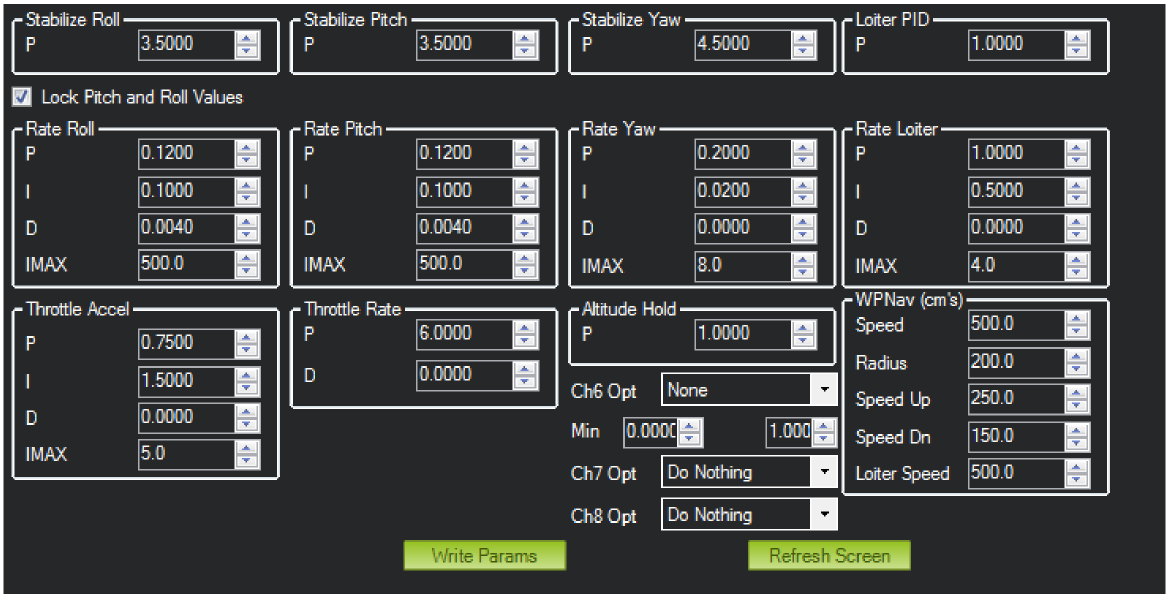
```
function ge_plot_volume
    xlsxdoc = 'input.xlsx';
    addpath('\MATLAB\googleearth')
    DATA = xlsread(xlsxdoc);

    I = DATA(:,2);  % RSSI
    X = DATA(:,4);  % LAT
    Y = DATA(:,5);  % LONG
    Z = DATA(:,6);  % ALT

    % Create an empty grid of query points.
    [Xq,Yq,Zq] = meshgrid(max(X):-.00005:min(X), min(Y):.00005:max(Y),
min(Z):1:max(Z));
    % Interpolate the known points across the query points to get a volume.
    V = griddata(X,Y,Z,I,Xq,Yq,Zq);

    %Iterate over the matrices and create points.
    kmlStr = [];
    skip = 0;
    for idx = 1:numel(V)
        icon_location = ' ';
        % Set the icon according to the RSSI
        % Omit NaN RSSI
        if V(idx) >= 70
           icon_location = '.\wp_images\img-70.png';
        elseif V(idx) < 70 && V(idx) >= 65
            icon_location = '.\wp_images\img-65.png';
        elseif V(idx) < 65 && V(idx) >= 60
            icon_location = '.\wp_images\img-60.png';
        elseif V(idx) < 60 && V(idx) >= 55
            icon_location = '.\wp_images\img-55.png';
        elseif V(idx) < 55 && V(idx) >= 50
            icon_location = '.\wp_images\img-50.png';
        elseif V(idx) < 50 && V(idx) >= 45
            icon_location = '.\wp_images\img-45.png';
        elseif V(idx) < 45
            icon_location = '.\wp_images\img-40.png';
        %else
        %    icon_location = '.\wp_images\img-35.png';
        %end
        else
            icon_location = ' ';
        end
        if icon_location ~= ' '
            kmlStr{idx-skip} =
(ge_point(Yq(idx),Xq(idx),Zq(idx),'iconScale',.5,'iconURL',icon_location,'alt
itudeMode','relativeToGround'));
        else
            skip = skip + 1;
        end
    end

    %Output the doument.
    ge_output(strcat(xlsxdoc,'.kml'),[kmlStr{:}]);
end
```

KML 3D Contour Slices Matlab Script

```
      function contour_slices
          DATA = xlsread('filtered.xlsx');

          I = DATA(:,2);  % RSSI
          X = DATA(:,5);  % LAT
          Y = DATA(:,4);  % LONG
          Z = DATA(:,6);  % ALT

           [Xq,Yq,Zq] = meshgrid(max(X):-
      .000005:min(X),min(Y):.000005:max(Y), min(Z):.5:max(Z));
           V = griddata(X,Y,Z,I,Xq,Yq,Zq);
           k = kml('KML File');

           [d1,d2,d3] = size(Xq);

            for idx = 1:d3
              try
                  Yqi = Yq(:,:,idx);
                  Xqi = Xq(:,:,idx);
                  Zqi = Zq(:,:,idx);
                  Vi = V(:,:,idx);
                  name = strcat(num2str(idx),'m above bround');

      k.contour(Xqi,Yqi,Vi,'altitudeMode','relativeToGround','altitude',Zqi(1
      ,1),'name',name);
              end
            end
           k.save('sample.xml');

      end
```

APPENDIX D: Tuning Parameters and Flight Results

Basic Tuning Parameters



Stabilize Roll
P 3.5000

Stabilize Pitch
P 3.5000

Stabilize Yaw
P 4.5000

Loiter PID
P 1.0000

☑ Lock Pitch and Roll Values

Rate Roll
P 0.1200
I 0.1000
D 0.0040
IMAX 500.0

Rate Pitch
P 0.1200
I 0.1000
D 0.0040
IMAX 500.0

Rate Yaw
P 0.2000
I 0.0200
D 0.0000
IMAX 8.0

Rate Loiter
P 1.0000
I 0.5000
D 0.0000
IMAX 4.0

Throttle Accel
P 0.7500
I 1.5000
D 0.0000
IMAX 5.0

Throttle Rate
P 6.0000
D 0.0000

Altitude Hold
P 1.0000

Ch6 Opt None
Min 0.0000 1.000
Ch7 Opt Do Nothing
Ch8 Opt Do Nothing

WPNav (cm's)
Speed 500.0
Radius 200.0
Speed Up 250.0
Speed Dn 150.0
Loiter Speed 500.0

Flight Times

Flight #	Time
1	09:32
2	08:08
3	08:33
AVG	**08:44**

Data Collection Log Index

Log #	Flight Purpose
1	Testing Equipment
2	Testing Equipment
3	Testing Equipment
4	Data Collection GPS
5	Data Collection SNR
6	Interaction SNR & GPS
7	Structure-Free Linear
8	Structure-Free Linear
9	Structure-Free Linear
10	Structure-Free Planar
11	Structure-Free Planar
12	Discard (Struct-Free Planar, Antenna Positioning Issue)
13	Discard (Struct-Free Planar, GPS Lock Failure)
14	Structure-Free Planar
15	Structure-Free General Area (Unused)
16	Discard (Struct-Free Volume, AP Failure)
17	Struct-Free Volumetric
18	Struct-Free Volumetric
19	Struct-Free Volumetric
20	Vertical Spike Above AP
21	Struct-Free Volumetric (AF)
22	Data Collection GPS
23	Interaction GPS
24	Widstoe South Wall
25	Widstoe West Wall