Fall 2019

Involuntary Signal-Based Grounding of Civilian Unmanned Aerial Systems (UAS) in Civilian Airspace

Keith Conley
University of Southern Mississippi

INVOLUNTARY SIGNAL-BASED GROUNDING OF CIVILIAN UNMANNED AERIAL SYSTEMS (UAS) IN CIVILIAN AIRSPACE

by

Keith Conley

A Thesis
Submitted to the Graduate School,
the College of Arts and Sciences
and the School of Computing Sciences and Computer Engineering
at The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Master of Science

Approved by:

Janet Donaldson, Committee Chair
Anna Wan
Bikramjit Banerjee
Tom Rishel

Dr. Janet Donaldson Committee Chair	Dr. Andrew Sung Director of School	Dr. Karen S. Coats Dean of the Graduate School

December 2019

ABSTRACT

This thesis investigates the involuntary signal-based grounding of civilian unmanned aerial systems (UAS) in unauthorized air spaces. The technique proposed here will forcibly land unauthorized UAS in a given area in such a way that the UAS will not be harmed, and the pilot cannot stop the landing. The technique will not involuntarily ground authorized drones which will be determined prior to the landing. Unauthorized airspaces include military bases, university campuses, areas affected by a natural disaster, and stadiums for public events. This thesis proposes an early prototype of a hardware-based signal based involuntary grounding technique to handle the problem by immediately grounding unauthorized drones. Research in the development of UAS is in the direction of airspace integration. For the potential of airspace integration three communication protocols were evaluated: LoRa WAN, Bluetooth 5, and Frequency Shift Keying (FSK) for their long range capabilities. Of the three technologies, LoRa WAN transmitted the farthest, however the FSK module transmitted a comparable distance at a lower power. The power measurements were taken using existing modules, however, due to LoRa using a higher frequency than the FSK module this outcome was expected.

ACKNOWLEDGMENTS

I would like to thank my lovely wife Crystal, and my loving parents for supporting me at all points in my education. I would also like to thank my committee members: Dr. Wan, Dr. Donaldson, Mr. Rishel, and Dr. Banerjee for their tremendous efforts in helping edit this work together. I would not have finished without them. I would also like to thank Dr. Amer Dawoud for his support in writing the DoD proposal that funded part of this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

ARM	Advanced RISC Microcomputers
AACS	Advanced Access Content System
BPSK	Binary Phase Shift Key Modulation
CRC	Cyclic Redundancy Check
CRUD&N	Create, Reuse, Update, Delete, and Notify
CSS	Chirp Spread Spectrum
D2I	Drone-2-Infrastructure
DOLSR	Directional Optimized Link State Routing Protocol
DSSS	Direct Spread Sequence Spectrum
ESC	Electronic Speed Controller
eNodeB	Evolved Node B Antennae
FAA	Federal Aviation Administration
FANET	Flying Ad Hoc Network
FD-MIMO	Full Dimensional Multiple Input Multiple Output Receive Antennae
FEMA	Federal Emergency Management Agency
FSK	Frequency Shift Keying
IOT	Internet of Things
IPE	Interworking Proximity Entity
LTE	Long Term Evolution
MANETS	Mobile Ad Hoc Networks

MDR	Message Delivery Ratio
MIMO	Multiple Input Multiple Output
NCMD	Number of Consecutive Message Drops
OLSR	Optimized Link State Routing Protocol
PN	Pseudo Random Noise
PSA	Platform Security Architecture
QPSK	Quadrature Phase Shift Keying
RSRP	Received Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RSSNR	Reference Signal to Noise Ratio
SINR	Signal-to-Interference-Plus-Noise Ratio
TCP	Transmission Control Protocol
TFR	Temporary Flight Restriction
UAV	Unmanned Aerial Vehicle
UD	Update Delay
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
UTM	Unmanned Traffic Manager
VANET	Vehicle Ad Hoc Network

CHAPTER I - Introduction

There is a definite need to involuntarily ground Unmanned Aerial System (UAS) in multiple areas such as military bases, university campuses, stadiums. and after a natural disaster. In this thesis UAS refers to common systems that are available commercially such as quadcopters although there are many different types of UAS such as military UAS and civilian UAS. Typically, military UAS are large and are used by the military to carry out missions. Military bases are strictly defined as no-fly zones and the involuntary grounding of the UAS will be handled with a physical based attack. UAS taking pictures of military bases are a clear and self-evident threat to security. Involuntarily grounding civilian UAS with physical attacks is not an option outside of military bases. Civilian UAS is the focus of this thesis.

University security have concerns about UAS being used to survey security patrols and exit routes. University security can be routinely understaffed which allows for areas of the campus to be unpatrolled during various times in the day. These gaps are a perfect time for a criminal to strike, and as such UAS are banned. UAS are naturally banned at stadiums for the same reasons as they are banned at university campuses. Stadium security is a field that is taken very seriously, and information can cause serious threats. The airspace after a natural disaster becomes a restricted flight area. If an aerial vehicle such as a helicopter cannot communicate with the UAS occupying the same airspace, the the helicopter will have to land for safe operation of the helicopter. During a disaster, not all UAS are a problem. There are commercial UAS pilots that are contracted by disaster relief organizations to gather information and assess the overall damage.

Communication amongst these organizations may be hindered due to lack of macro coordination between authorized UAS pilots.

1.1 Disaster Relief Challenges

The main challenge for disaster relief efforts is obtaining information to make intelligent decisions for matters such as logistics. For example, determining which shelters need water and how much water is needed can be a difficult decision if communication isn't established with that shelter. Furthermore, common communication methods go down during natural disasters. This is a well-documented occurrence with 364 cell towers, 16 emergency 911 call centers going down, and 180,000 homes losing all phone and internet access during 2017 hurricane Harvey. [1] As such, FEMA has determined that communication resiliency and capabilities is a key challenge for the future.[2]

1.2 UAS for Disaster Relief

UAS are helpful for gathering information during natural disasters because they are small, very mobile, can move quickly, are easily deployable, and are relatively inexpensive. They can also broadcast video during their patrols. As such, drones can provide critical data very quickly to emergency management personnel after disasters. The FAA currently allows disaster management authorities to take advantage of drones by offering a pilot license course which enables an individual to fly for commercial purposes. FEMA hires these licensed individuals to obtain and provide information to disaster relief efforts.

1.3 Challenges UAS Pose

The greatest challenge comes from unauthorized UAS pilots. Many of the drones in unauthorized airspace after a disaster are rogue drones operated by ordinary citizens. This has been recognized as a problem by the FAA which has issued the statement, “Flying a drone without authorization in or near the disaster area may violate federal, state, or local laws and ordinances, even if a Temporary Flight Restriction (TFR) is not in place. Allow first responders to save lives and property without interference.” [3]

The problem is that emergency aircraft are flying at low altitudes during emergencies and if a pilot detects an aircraft, which is what a drone is classified as, in their airspace, and the emergency aircraft cannot communicate with the rogue aircraft then the emergency aircraft will have to land. This reduces the effectiveness of rescue operations.

1.4 Communicating with Civilian UAS in Restricted Airspaces

In summary, UAS are vital for hurricane relief efforts, but they also present the problem of enabling civilians to unknowingly disrupt relief efforts. The problem can be alleviated with a better communication technology. Better communication technology will also make drones more effective for emergency management officials because better quality video can be transmitted back. This communication technology must be localized and cannot rely on cellular networks in order to be usable during emergencies.

While it is desireable to be able to ground UAS in many different situations, there is an immediate need to be able to ground UAS during natural disasters. Although, it is true that UAS are vital for hurricane relief efforts, unauthorized UAS also pose a great threat to aircrafts during the relief efforts. Unauthorized UAS also directly interfere with

relief efforts and in turn put lives in danger. This threat can be mitigated with the ability to involuntarily ground UAS using a signal based wireless technique.

1.5 Thesis Organization

The thesis is laid out in the following manner. Chapter one discuses the need to be able to ground UAS during disaster situations. Chapter 2 provides background in the form of an overview of current UAS communication research. Chapter 3 describes the system operation and the communication protocols. Chapter 4 describes the experiments undertaken and provides data. Chapter 5 provides a discussion of the experiment results, and chapter 6 is the conclusion and future work that can add to this research.

CHAPTER II - Background

This section provides an overview of ongoing research in the field of UAS communication. The search contained the following keywords “drone communication”, “drone defeat”, “drone jamming”, “drone barrier”, “unauthorized drones”, “drone denial”, “drone landing module”, “drone emergency stop”, “drone e stop”, “drone public safety”, and “drone privacy”. The “drone communication” keyword brings up papers on using cell phone communication protocols and cell phone networks such as Schalk and Herrmann. [4] “Drone defeat” and “drone jamming” bring up papers of using actively adversarial methods such as jamming to defeat UAS. Although the phrase barrier is a common term used to define a restricted area drone barrier brings up papers of using UAS to inspect the Great Barrier Reef and physical barriers such as roadside barriers. Unauthorized drones uncover papers on detecting the physical presence of drones. This thesis refers to known unauthorized drones that need to be grounded in restricted airspace. “Drone denial” brings up work on DDOS attacks, and general drone hacking. “Drone landing module” uncovered work on helping drones to land better. “Drone emergency stop” brings up a paper on public safety drones. “Drone e stop” which is a common phrase for emergency stop but didn’t return search results on IEEE Xplore. “Drone public safety” brings up papers on monitoring cities with drones. “Drone privacy” brings up a paper by Blank and Kirrane on restricting areas by creating no fly zones in way point navigation software. [5] However way point navigation software has no effect on civilians flying unauthorized drones. What proceeds is a summary of research in UAS communication.

Section 1 discusses research in communication methods, and different types of communication networks including cellular networks, Military networks, and civil networks. Section 2 discuses research in evaluating networks. Section 3 discuses research in improve network routing. Section 4 discuses research in drone security. Finally section 5 discuses research in designing a traffic manager for autonomous UAS.

2.1 Communication Methods

This section provides an overview of research trends focusing on using cellular communication to improve the control of drones. The overarching idea is that 4G Long Term Evolution (LTE) is good enough to maintain a connection for everyone in cities. In this context the phrase good enough refers to the ability of 4G LTE to maintain a connection for large cities with dense populations. Therefore, 4G LTE should power our drones, but the research, by Schalk and Herrmann demonstrates that even if the cell towers are up cellular communication is not ideal due to the differences between the use cases of a smartphone against a UAS.[4]

2.1.1 Cellular Networks

Schalk and Herrmann assessed the suitability of current LTE networks for a drone Unmanned Traffic Manager (UTM) and for Drone 2 Infrastructure (D2I) communication. [4] Metropolitan areas are likely to have a drone density of over 200 drones per square kilometer. [6] Current LTE networks can maintain such a high connection density in principle. Schalk evaluated his model by using a Message Delivery Ratio (MDR) and Number of Consecutive message drops (NCMD). MDR is like an Update Delay (UD) that was used in Kloibers study while NCMD is represented as a cumulative distribution function of the probability of a message being received against the total number of

messages. [7] The results showed a message delivery rate of 95% with a payload size of 300 bytes per message at a rate of 10hz. This payload size is pitiful compared to the streaming video that emergency management personnel require for the job and demonstrates again that current LTE technology cannot handle drone communication.

Schalk and Herrmann's study presented the problem of inter cell interference. Inter cell interference is a kind of interference caused by a device that uses the resources of multiple access points at once. These findings were echoed by Van Der Bergh. [8] However, Xingqin Lin presented a counter study with findings that claim that LTE is sufficient for the initial drone roll out. [9] Xingqin Lin presented findings from field trials involving low altitude drones on commercial LTE networks. The field trials were implemented using a DJI drone equipped with a smart phone for data collection. The key measured parameter was Received Signal Received Power (RSRP). The power measured when the drone was at a height of 50m was 2.8dB lower than the power received at ground level. When the drone was at 150m, it received 4.8dB less power. Additionally, the maximum throughput that the drone was able to receive was roughly 18 Mbps downlink, which is less than half of what other studies have stated as the minimum data throughput for drone applications.

Amorim and Nguyen attempted to improve the current understanding of LTE by modeling radio channel path loss. [10] The results showed that path loss decreased as the altitude of the drone increased. The results also showed that a free space model of propagation could be used after the drone achieved an altitude of 100 meters above ground. These efforts were furthered by Zhao and Luo who analyzed the problem of transmitting media from drones to base stations. [11] They also proposed a minimum data

rate of 50Mbps, which cannot be handled by single channel communication, nor currently used drones. The other challenge is to maintain the data rate for long durations and over great distances to facilitate normal drone operations.

Amorim and Nguyen found that the air-to-ground link is susceptible to Rician fading, which is a stochastic model for radio propagation. Rician fading can normally be observed when there is a line-of-sight between the transmitter and receiver. It describes the physical anomaly of the radio signal being partially cancelled. This causes the signal to arrive by various paths, adding to multipath interference. In contrast, the conventional ground-to-drone link is susceptible to Rayleigh fading. Rayleigh fading is another radio signal propagation model that can be observed when there is no dominant line-of-sight between the transmitter and receiver pair, which can happen in urban environments for instance. The proposed solution is to focus beams to produce higher throughput and longer transmission distances. However, the focused beams must reach their target. To this end, Luo proposed an algorithm based on the direction of arrival (DoA) to predict where the beam should be pointing. [11] The algorithm takes LTE channel state information and velocity vectors based on inertial measurements as algorithm inputs. It then predicts the direction where the transmission beam needs to be focused and alters its path accordingly. The algorithm was able to predict direction with an error of 0.258 degrees at 500 meters. Unfortunately, directional antennas are currently expensive and large so beam forming has been ignored in the involuntary grounding technique research.

Muruganathan, Siva, and Lin also sought to control drone communication better. [12] They reported on the 3rd Generation Partnership Project (3GPP) Release 15 which is an organization that resides over telecommunication standards. The report stated that the

intercell interference for drones is particularly bad because the drones are flying above the evolved node B (eNodeB) antennae that are used to deliver data to cellular devices. This position would give the drone line-of-sight connection to multiple eNodeB stations. In addition to affecting the throughput of the drones, this interference will also affect groud users. Thus, drone communication would have to be controlled, and the first step to controlling drone communication is to identify it.

There are two main types of data that must be classified. The first is application data while the second is command and control data. Current technology classifies all data coming from drones as application data, and, as such, adding command and control data will go a long way in preventing interference. Muruganathan, Siva, and Lin looked at three scenarios that involved the antennas being above roofs, antennas being below roof, and rural scenarios with antennas being spread far apart. Drones were determined to cause more interference than grounded equipment with drones causing 6.2db of interference despite an aerial coverage of only 7.1%.

Several solutions were proposed, such as user-equipment delivering noise measurements to the eNodeB antennae. Another solution is to measure interference using node cross-talk. The final proposed solution is to measure the interference from the node pinging the user-equipment. Ultimately, the network would respond using this data alongside full dimensional multiple input multiple output receive antennae (FD-MIMO) on the node stations and directional antennae on the drones to mitigate interference. The nodes would then send command and control messages to the drone on where to aim the directional antennae to lessen the line-of-sight interference.

2.1.2 Military Networks

Jun Li published a study of four communication and networking architectures for drones, as well as several standard protocols that would handle many devices. [13] The four architectures displayed in Figure 2.1 are: Centralized Unmanned Aerial Vehicle (UAV) Network (a), UAV Ad Hoc Network (b), Multi-Group UAV Network (c), and Multi-Layer UAV Ad Hoc Network (d). Centralized UAV Networks are defined by all UAVs communicating back to a ground station. This is the network type that is closest to the LTE Networks above. UAV Ad-Hoc Networks have a backbone UAV that communicates with the ground station. All the node UAVs communicate to the backbone. This type of network would allow a longer range because the backbone can extend the range of the ground station and that attribute would be good in a disaster situation, but the nodes are still communicating with the same node and this can cause signal collisions. Multi-Group UAV Networks use multiple UAV backbones. This network setup allows the UAVs to spread out more in order to cover more ground, but it still has the issue that the backbones have to send data back to the ground station directly. The main trait of the Multi-Layer UAV Ad-Hoc Network is that the multiple backbones can use other UAVs as relays. This is the most flexible type of network, and it is the best sort of network for disaster relief drones.

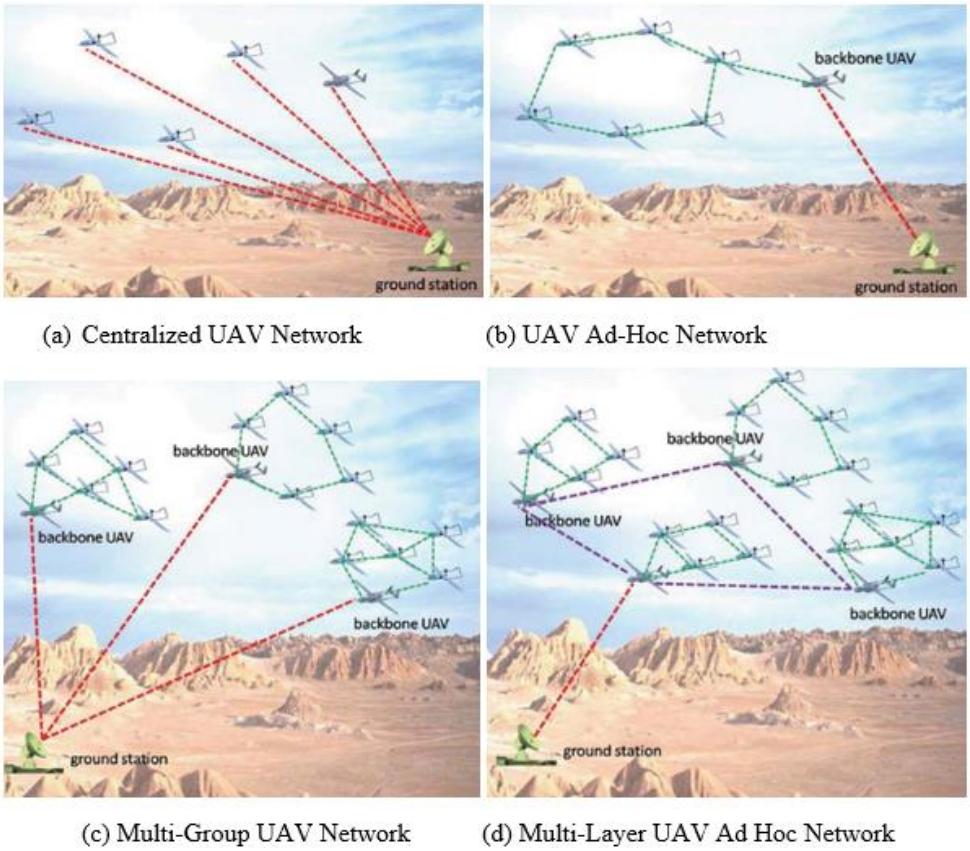

Figure 2.1 *A visual network topology of the Military Networks studied in [13]*

(a) Centralized UAV Network (b) UAV Ad-Hoc Network (c) Multi-Group UAV Network (d) Multi-Layer UAV Ad Hoc Network

The communication protocols reported on in the study were designed to work with the above network topologies, and they are divided into two groups: current data links and next generation data links. The current data links consist of Common Data Link, Tactical Common Data Link, link-11, link-14, link-16, and link-22. Common Data Link was developed in 1991 by the U.S. Military; it allows full duplex transmission of images and signal data and specifies wide band line-of-sight radios using a 200 Kbps uplink. [13] Common Data Link uses binary phase shift key modulation (BPSK), Viterbi convolution encoding, interleaving, and pseudo noise spreading for its uplink. The down

link uses quadrature phase shift key (QPSK) modulation, Viterbi convolution encoding, and interleaving at a data rate of 10.7 Mbps.

Tactical Common Data Link was developed by the U.S. Military to send multimedia securely from drones to ground stations. It uses a Ku narrow band uplink at a data rate of 200 Kbps while the down link is 10.71 Mbps. Link-11 is the NATO version of Tactical Data Link that operates in the High Frequency Band. [12] Link-14 is a system for broadcasting maritime data between ships. Link-16 uses the L-band and is a tactical data link designed by NATO to be jam resistant. Typically, Link-16 is used for air-to-air and ground-to-air applications. Link-22 is a secure radio system designed by NATO. It was designed to improve on Link-11 and use the same applications as Link-16. Link-22 can also use relay nodes to extend its range. Unfortunately, none of the current data links have the bandwidth required for current drone networks, but the next generation data links are much closer.

The next generation data links consist of Tactical Targeting Network Technology and Wideband Networking Waveform. Tactical Targeting Network Technology was developed by DARPA to support line-of-sight ad hoc IP networks. The network is IP based and has an uplink of 2 Mbps. [13] The network can support up to 200 nodes and can accept up to four data streams at once. The network transmits secure jam resistant communications at internet speeds. Similarly, Wideband Networking Waveform provides tactical wireless networking for users and backbone infrastructures. The technology can dynamically configure transmission parameters such as transmissions power, transmission protocol, etc. It also uses a distributed resource management scheme to improve packet delivery, and the technology can even operate in ad hoc mode with a

neighbor discovery function. In summary, the next generation data links work closer to the modern networking equipment that is available to consumers.

2.1.3 Civil Networks

Mahdi and Domenico studied the challenges of wireless communication for drones using the802.11 and 802.15 communication protocol for search and rescue. [14] Mahdi and Domenico put forth that the core challenge of drones for search and rescue is to obtain and maintain a reliable high data rate. They further echoed the concerns of using cellular networks due to reliability concerns. The study instead presented a hybrid architecture of Wi-Fi 802.11n and XBee-PRO 802.15.4 for bulk data transfers.

The experiments showed that Wi-Fi drone-to-drone relay throughput falls far below the theoretical maximum. In fact Wi-Fi throughput barely reaches the throughput of older 802.11a/g technology. Mahdi and Domenico hypothesized that the throughput drop is due to the 802.11n rate adaptation being unable to cope with channels that are moving fast in three dimensions. The measured throughput at 340 meters was 3 Mbps, at 120 meters the throughput was 44 Mbps, and at 20 meters away the throughput was 46 Mbps with large variances. These measurements were using the UDP protocol with MIMO features enabled. The 3Mbps data rate is enough for the involuntary grounding technique research, but the 802.11 protocol was ignored in this research due to insufficient propagation range.

2.2 Evaluating Networks

Raffelsberger presented a performance evaluation tool for drone communication. [15] The evaluation tool measures signal strength and several communication protocols such as Transmission Control Protocol (TCP), UDP, the downlink throughput, and the

uplink throughput. The parameters presented for signal strength evaluation are reference signal RSRP, reference signal received quality (RSRQ), and reference signal to noise ratio (RSSNR). It was found that the downlink performance is higher on the ground, but the uplink performance is higher in the air, however UDP performance remained relatively stable up to 150M in the air.

While Raffelsberger created a tool, other researchers evaluated network models through implementation such as Merwaday who further investigated using drone based heterogeneous networks for public safety communications. [16] Merwaday's findings showed that broadband communication can enhance public safety operations. Merwaday also put forth the idea that drones can be used to deploy broadband networks during disaster situations. This idea was followed up by Chandrasekharan who presented a study on using aerial vehicles to deploy wireless networks. [17] The project was called the ABSOLUTE project and was designed to implement LTE-A aerial base stations using low altitude platforms to provide wireless coverage for public safety purposes. The study evaluated several types of aircraft which included drones, aircraft, airships, and tethered helikites.

The ABSOLUTE project specified the aerial base stations to operate at 150 meters altitude with five hours of autonomy. The base stations provide LTE network connectivity based on the alternative architecture, whereby most of the base station equipment operate in the base band and the radio frequency equipment operates in a Remote Radio Head that is connected via a fiber optic antenna. This allows the base station to separate into a terrestrial component and an aerial component. Altogether, this implementation allowed a smartphone to ping the network up to 300 meters away. The

conclusion of the report was that regulations and mechanical limitations are the largest hurdle in implementing aerial networks, but progress was nevertheless made towards that goal.

Leszek and Lotfi presented a study of an ad hoc networking simulation. [18] This study stated that effective resource utilization was essential for UAV ad hoc networks. The paper presented Opportunistic Resource Utilization Networks called Oppnets. The principle behind the Oppnet was to start the network by sending out a seed Oppnet. The seed network would then begin discovering foreign nodes or application networks, after which it would invite or force the nodes to join the mission as helper nodes. The action of gathering helper nodes extended the seed into an Extended Oppnet. This network topology was different from traditional networks in which all the nodes deploy together. Oppnets are of interest regarding drones as this mechanism is similar to how emergency response teams operate in the real world. It is also a point of interest since there are a broad set of potential helpers for the Oppnet.

Tareque published a paper on how to classify drone networks. [19] Drone networks are very economical with many small drones costing less and requiring less maintenance than a large drone. Multi UAV networks can maintain continuity if one or more drones fail during the mission. Missions can be completed faster with many small drones. Using multiple drones can offer higher accuracy by providing a larger radar cross section. However, multi UAV networks also have several issues, such as each drone requiring special hardware to transmit. Transmission reliability can decrease as distance between drones increase or as line-of-sight issues arrive. The network architecture specified for drones will have to be able to handle these problems. Tareque proposes

Flying Ad Hoc Network (FANET) as the network class for drones. FANET is a special form of Mobile Ad Hoc Networks (MANETS).

FANET will face the following open problems: P2P UAV communication, regulations for civilian UAVs, robust FANET algorithms, UAV placement, FANET standardization, and coordination of UAVs with manned aircraft. Of these problems, UAV regulation is the biggest obstacle to drone development in civilian areas. Outside of regulatory concerns, drone-to-drone communication will be a key concern for facilitating the ability to use FANETs and robust algorithms to allow drones to be added or deleted from the network. Suescun and Cardei presented results that further echoed the sentiments of Tareque and added to the efforts by proposing that delay tolerant networks be investigated as there may be inevitable delays in drone networks. [20]

2.3 Network Routing

Hayat and Yanmaz presented a survey on drone networks that envisioned a future with teams of small-scale drones in air traffic. [21] These teams of drones can be used for all sorts of applications including surveying infrastructure after natural disasters, but reliable communication and networking will be essential to achieving that future and one of the big routing challenges is in reducing network latency. Alshabtat tackled routing latency problems in ad hoc networks. [22] The nature of ad hoc networking allows the physical locations of the nodes in the network to be random which means that the default packets routing path may not be the most efficient path. This problem becomes even worse in mobile ad hoc networks because the nodes are constantly moving and changing configuration. Mobile ad hoc networks are an emerging type of network that involves drones autonomously forming multi hop relay networks without a centralized station and

as such, current routing protocols run into implementation problems on proposed networking transmission solutions such as directional antennae.

Routing protocols are divided into two categories: reactive routing protocols and proactive routing protocols. Alshabtat discusses two proactive routing protocols: Optimized Link State Routing Protocol (OLSR) and Directional Optimized Link State Routing Protocol (DOLSR). OLSR is a table-driven proactive routing protocol that is an enhancement of the pure link state protocols because OLSR does not retransmit every message as soon as the first copy is received, thereby reducing overall transmission overhead. The main feature of OLSR is the multi-point relay. OLSR transmits over multiple paths at the same time so that one transmission may reach the destination faster, as can be seen in Figure 2.2.

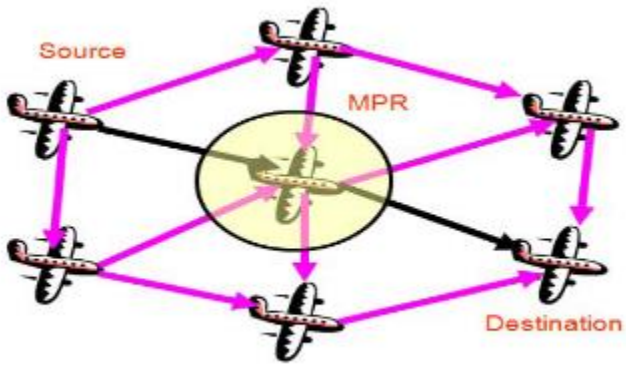

Figure 2.2 *Diagram of OLSR Algorithm with a Multi-Point Relay (MPR) [22]*

DOLSR takes inspiration from OLSR, but it considers the selection of the multi-point relay, but it selects the MPR in a better way which shrinks latency by reducing the number of hops needed. The algorithm was tested in a simulation and it was found that DOLSR was consistently able to reduce the number of node hops needed by two when

compared against OLSR. The DOLSR algorithm could be interesting in the future to extend the range of the involuntary grounding technique through using other drones as a relay.

Hayat and Samira presented a system of multiple drones where the drones and ground clients can join the network in an ad hoc manner called a multi-device, multi-sender network. [23] The network communicated using 802.11n and the study reports both indoor and outdoor experiments. The experiments extended the range of the network by using a novel antennae setup.

Kopeikin studied task allocation routing. [24] Mozaffari offered up a proposal for optimal transport theory. [25] Zeng and Zhang presented an article on the opportunities and challenges of drone communication. [26] The easiest way to guarantee that a drone network fail would be to improperly route control messages. Poor routing decisions on control messages can lead to drone crashes, drones flying out of network range, or improper network configurations. Kopeikin proposed a novel solution to use task allocation to control the network topology; this involved the network emitting a discovery transmission that logged the time cost to hop to each node. This determines the latency that will be introduced by the nodes. This transmission would then allow the network to create and maintain a minimum spanning tree. The drones would then classify the data to be transmitted as sensor data or state data. The difference was that state data did not have high bandwidth requirements but needed to be transmitted with minimal latency, while the sensor data possibility had higher bandwidth requirements such as transmitting video feeds. The path to transmit the data would be determined by the type of data sent and would follow a prediction of how the network topology may change.

2.4 Drone Security

Bunse and Plotz wrote a chapter in the book Engineering Secure Software and Systems that analyzes the security of drone protocols [27]. They report that drones are based on inherently insecure computing architectures. That, however, is an overarching problem for all computers. The most common computing architectures such as ARM and x86 were not originally designed to be secure. Current secure architectures such as the ARM architecture's Platform Security Architecture (PSA) is just the same old ARM architecture with added memory tampering mitigations. These hardware level vulnerabilities allow drones to be easily halted by interfering with their control signals.

The drone vendors currently secure their communication methods by declaring the implementation as a trade secret and by keeping the design details private. Drone data is usually stored locally in plaintext. Furthermore, drones transmit telemetry data in a way that is easily understood by third party tools. At a high level, drone manufacturers rely on frequency hopping, spread spectrum, and key sharing as their main security features, but the manufacturers focus on the 2.4GHz band. The manufacturers also focus on using packet-based transmission. Unfortunately, these decisions mean that the drone in-house communication protocols of the drone vendors behave similarly to IPv4 and other internet protocols. Common internet-based attacks that are effective against devices also work on drones.

There are three types of attacks that can be made against drones: hardware attacks, wireless attacks, and sensor spoofing. Hardware attacks involve physical attacks such as shooting the drone or infecting a drone by replacing a circuit board. Wireless attacks can include hijacking the wireless signal being transmitted to the drone as can be

seen in Figure 2.3 or breaking the communication protocol through brute force attacks. Sensor spoofing involves sending fake sensor data or interfering with sensors during operation.

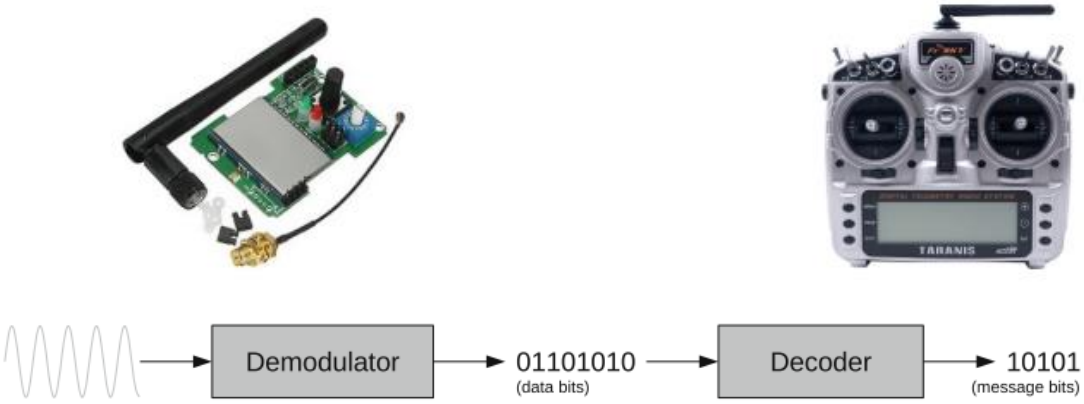

Figure 2.3 *Wireless Attack Hardware [27]*

The wireless attack involves five steps: get documentation, capture data packet, reverse DSSS, identify hopping sequence, and attack [27]. Getting documentation involves analyzing the communication protocol to the drone. There are four common rf transceiver chips that are used for drones: A7105, CC2500, NRF24L01, and CYRF6936. All four chips are readily available from electronics vendors, and the documentation is easily accessible. Capturing the data packet can be achieved by using an off-the-shelf software defined radio with supported software. This step can also be obtained by using a serial communication protocol identifier on the on-board communication line if physical access is available. Reversing the Direct Spread Sequence Spectrum (DSSS) requires obtaining the pseudo random noise (PN) code. The PN code can be obtained by snooping the serial communication line. Identifying the hopping sequence can be achieved by

serial communication identifiers or software defined radio identifying. In practice, this attack can be launched using off-the-shelf equipment that is easily obtainable.

2.5 UTM – Future Airspace Integration

The future of drone networking is to integrate drones into the airspace. This will mostly remove the need for the drone emergency communication, as all aerial vehicles will be able to communicate with each other. In addition to the communication this would also enable novel applications such as a drone crop monitoring system, wildlife tracking, mobile sensor networks, and mobile power delivery. [28][29][30][31]

There have been plenty of strides in this space such as Sung-Chan Choi's drone management system using oneM2M communication. [32] OneM2M is a global initiative created to standardize communication between machines in the IoT space. The goal of the initiative was to make a standard that allowed all IoT and M2M communication to be interoperable. The oneM2M platform offered several common functionalities that could be applied to drone management such as device registration, data management, location, subscription and notification, group management, and Interworking Proximity Entity (IPE). OneM2M was also good for networking drones as the interfaces were simple.

OneM2M adopted the resource-oriented architecture model, and, as such, information and services are exposed as a resource information model. Resources are labeled with a Uniform Resource Identifier (URI), and interactions with the resources were supported by the CRUD&N (Create, Reuse, Update, Delete, and Notify) operations. Thus, oneM2M is analogous to a web application and the oneM2M API similar to web-based APIs. The IPE provides an interface for non oneM2M devices to interface with oneM2M. [32] In this case, the management system is a oneM2M application, and the

drones are interfaced with as IPE systems. First a drone is registered as an IPE device and receives a device ID, then the drone data is sent into the oneM2M system and interpreted as oneM2M services.

Seyit Alperen presented a network topology for a UTM that accounts for current drone technology limitations. [33] The study presents is a search and rescue scenario. The drone limitations that are outlined are as follows: drones have a flight time of fifteen minutes, drone communication uses Wi-Fi or Bluetooth, and the control center needs to quickly adapt to changes in distance between drones.

In acknowledgement of these limitations, a Wireless Drone Network is presented using a hierarchical tree topology where the drones communicate to a backbone drone, which relays back to a ground station. In the proposed topology, the user is acting as the control center. The main drone (MD) is acting as a data path to the control center, and the sub drones (SD) report data to the control center through the MD which is displayed in Figure 2.4.

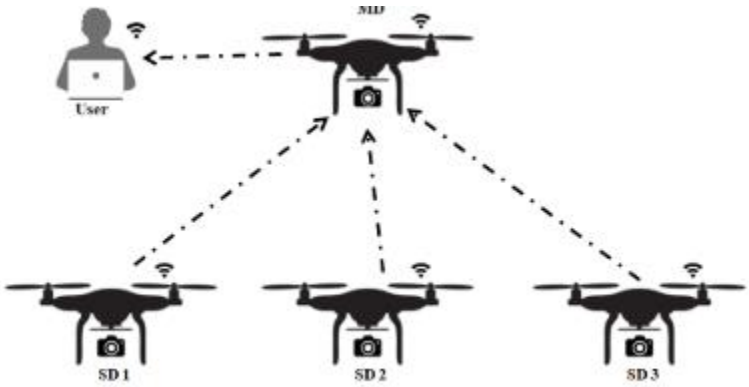

Figure 2.4 *Wireless Drone Network [33]*

Mirmojtaba presented an architecture for a drone management system title the "Internet of Drones." [34] The internet of drones is an architecture for providing coordinated access to controlled airspaces for drones. This system was modelled to be close to air traffic control command centers. In this system, the airspace of the United States will be divided into twenty-four areas. Each of the twenty-four areas will then be subdivided into twenty to eighty different sectors. Each sector will then be managed by a controller. The aircraft are tracked by GPS, and an air traffic controller is to interfere only when necessary. The ideal scenario is to handle the flight paths in a manner like current commercial aircraft, whereby most delays happen before the plane takes off.

The network implementation divides the implementation details into layers. The layers are as follows: application layer, service layer, end-to-end layer, node-to-node layer, and airspace layer. Dividing the network into layers allows the problems involved to be subdivided as well to allow the network to be more modular. The airspace layer implements the map, which contains the geometric representation of the elements in the node graph. The airspace layer also has a broadcast and track protocol which will allow the drones to periodically broadcast their location. The planned trajectory, precise control, collision avoidance, and the weather conditions will also be contained within the airspace layer. Altogether, the internet of drones is a very good model for a management system in the future, and it even includes a layer to implement emergency transmissions which would allow the integration of the involuntary grounding technique.

CHAPTER III - Technology

This chapter describes the operation of the involuntary grounding technique and provides context on radio communication techniques and the UAS ecosystem. This chapter is organized in the following way. Section 1 provides the theory of operation. This provides an overview of how the system operates starting with the basic question of how does a UAS receive authorization to how are authorized UAS differentiated from unauthorized UAS. Section 2 provides an overview of UAS parts and how they interconnect. Section 3 Discusses the radio communication protocols that were used in this thesis.

3.1 Theory of Operation

When a commercial UAS pilot is contacted, they must be brought into a secure area in order for their UAS to receive authorization which adds the security of face to face authentication. Physical communication with the UAS will be obfuscated by using a nonstandard multi-wire communication protocol. The nonstandard multi wire communication protocol will make generic off the shelf tools such as a bus pirate ineffective at determining the protocol as most hacking tools are expecting single wire communication protocols such as I2C, UART, or SPI. The driver to facilitate the communication protocol would be distributed as a shared object file on an encrypted physical storage media that can only be obtained by authorities requesting the driver from the developer of the system. The shared object will be encrypted and stored in a nonstandard file format that the authorization program will access by itself. The storage media will be signed and dated when it leaves the facility. When the program accesses the storage media, if the media is dated 90 days before the current date, the key will be

rejected. This will remove the ability of users to make copies of the storage medium, and it will require users to consistently request new shared object keys. After communication is established the authorization software will pull a unique hardware key from the drone.

The unique key will be generated by SRAM PUF (Physically Unclonable Functions) [35] circuits inside of the microcontroller. SRAM PUFs are generated by using analog thermal noise introduced by the SRAM circuit during manufacturing. This method exploits the manufacturing defects to create unique keys. These keys are only present when the system has power as they are stored in SRAM therefore physical access to the system when the system is unpowered will not allow access to the keys. The hardware key will then be used to generate a public and private key based on a symmetric key, K, using the Advanced Access Content System (AACS) broadcast encryption algorithm. [36] The drone will be given the public key.

Broadcast encryption is a problem space that was labeled by TV broadcasters, and AACS was developed for Blu-Ray Discs. The problem of broadcast encryption is that content will be broadcast out, but the content provider wants to limit access to authorized viewers. This problem mimics our concern of allow authorized drones to continue flying. In AACS, each member of the group has a public and private key pair. There is also a symmetric key K. K is known to every member of the group, because the authorization token is generated by encrypting K with the public key. New members can be added to the group by giving the new member K. The challenge lies in removing members from the group.

Forgetfulness can be coded into standard operating procedure by requiring a new symmetric key for each emergency scenario. This will be enforced by having the drone

authorization program generate a new symmetric key at runtime. This symmetric key is then required to be distributed via physical means. Physical distribution is the most secure way of managing keys, but it relies on keeping the number of authorized drones small enough that physical distribution can be managed. Key collision is mitigated both by basing the keys on SRAM PUFs, and by AACS itself. AACS was developed for handling millions of Blu-Ray players, therefore key collision isn't a concern for a few hundred drones in the air. There is also the challenge of rogue members sharing their keys. This challenge is mitigated by the physical communication protocol which prevents users from having access to the keys themselves.

When a UAS is detected by a radar, the transmitter will broadcast out a signal. If the drone is authorized, then the drone can successfully decrypt the transmission, and continue flying. The UAS will then log the event into an onboard log and send a signal back to identify itself. The transmitter can then display which authorized drone is present. The logs can also be pulled during the after-action report phase in order to verify the event.

The next concern is with physically tampering with the module. The module should ultimately be put on the same pcb as the flight controller. Being on the same board as the flight controller will reduce the system footprint and ensure that the gate has easy access to the signal lines. The gate is an active allow system which means that the module must maintain a logic high on the gate to allow the system to pass. In the event of a pin being burned out on the module the signal will not be able to pass. This would ensure that if the module is tampered with to burn the pins out then the drone will no longer be able to operate. The module and gate can be desoldered from the flight

controller and replaced with a jumper wire to allow the signal to pass, but desoldering surface mount parts without damaging the rest of the board can be difficult for inexperienced users.

A software-based solution would prevent all physical tampering; however UAS hobbyists enjoy tinkering with UAS configuration files. The software solution would also remove the ability to use a proprietary protocol which would reduce the system security overall.

3.2 Drone Overview

A UAS is made up of several subsystems which consist of: the flight controller, the electronic speed controller, the receiver, and the radio controller. The subsystem division allows for problems to be isolated.

3.2.1 Flight Controller

The flight controller is the device that controls the subsystems. A radio receiver will receive controller input. The flight controller will then translate the controller input into usable information for the Electronic Speed Controllers (ESC). The flight controller that was used for the drone is the Copter Controller 3D (CC3D).

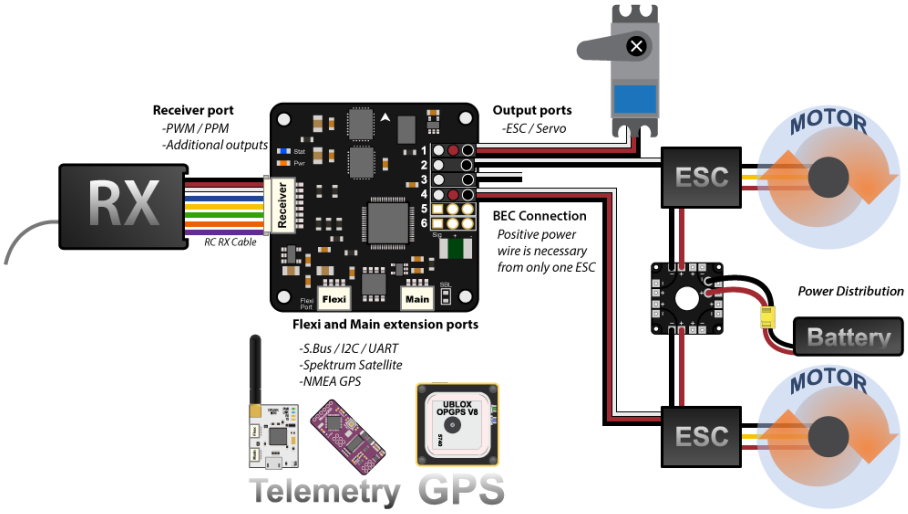

Figure 3.1 *CC3D Diagram – The diagram shows the interfaces to the CC3D [37]*

The receiver port supports both PWM, PPM and SBus protocol inputs. The outputs to the ESCs use PWM as the standard. The rest of the ports are called Flexi ports and they are programmable to support GPS or other telemetry modules using either the UART or SBus protocol. The obvious places to put the communication module are: between the ESC and the Motor, between the flight controller and the ESC, and between the receiver and the flight controller. The first placement, between the ESC and the motor, is a good place because the motors can be shut off immediately. The second placement, between the flight controller and the ESC, is a good placement because the signal is a digital signal and it still controls the motors although less directly. The final placement, between the receiver and the flight controller, is a good place between it can eliminate the controller input and still control the motors.

3.2.2 Electronic Speed Controller

The ESC controls a three-phase brushless DC outrunner motor. This type of motor requires pulses on all three terminals in a certain sequence in order to function properly. The timing needs to stay tight in order to get optimum performance from the motors. These constraints require that the ESC be a separate module from the flight controller. In addition, the ESC actually has its own control system that the flight controller communicates to using PWM. PWM is demonstrated in Figure 3.2.

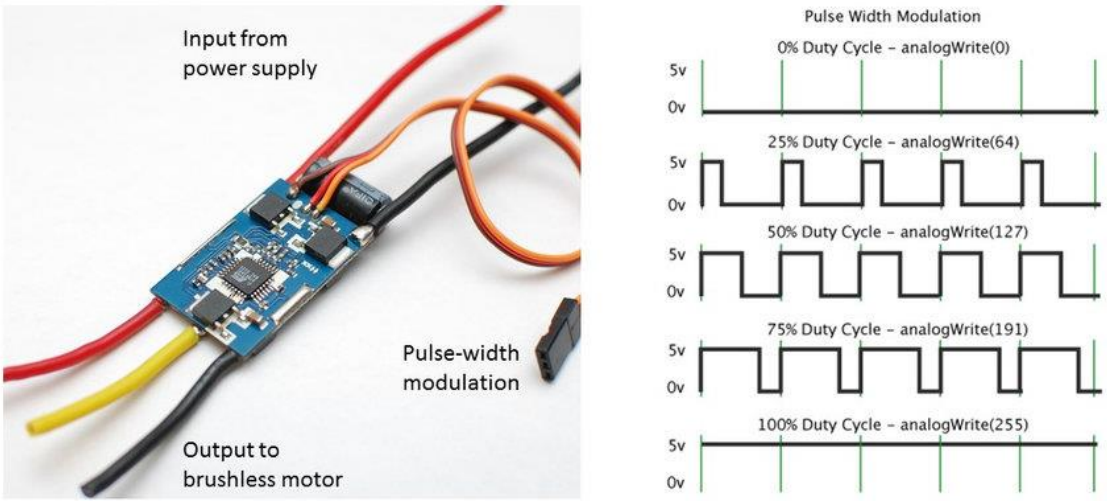

Figure 3.2 *Example PWM Signal from Flight Controller to ESC [38]*

The stop module can't be placed the ESC and the motor because signal integrity is crucial. In addition, the motor can draw up to and over 30A of current, which would require more expensive parts to handle the kickback from shutting the motors off suddenly.

3.2.3 RF Receivers

In a UAS, a controller has a transmitter. The transmitter is bound to a receiver. The receiver will then output a signal to the flight controller. The signal will either be a

PWM signal as in Figure 3.3 or a SBus protocol signal. The PWM signal is only a 55 Hz signal and there are 4 signals one for Throttle, Roll, Pitch, and Yaw.

Figure 3.3 *RF Receiver Output Signal*

The current best place for the communication stop module is between the RF Receiver and the flight controller. The 55 Hz signal is slow enough that the signal can pass through any piece of hardware without being a problem, and the flight controller default response to being cutoff is to stop the motors.

3.3 Radio Communication

Ensuring that the system works is always the main priority. With that in mind the following focuses on how to estimate system range, and possible causes of not reaching the full range. The most common way of estimating rf range is with the Friis Transmission Equation [39] which is shown in equation 1.

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi d})^2$$

Equation 1: Friis Transmission Equation

P_r	Receive Antennae Power (dBm)
P_t	Transmiting Antenna Power (dBm)
G_t	Transmitting Antenna Gain (dBi)
G_r	Receiving Antennae Gain (dBi)
λ	Wavelength (m)
d	Distance between Antennas (m)

Table 3.1 *Variable Definitions for Equation 1*

The Friis Transmission Equation relates the received signal power to distance, frequency, and antennae gain. The equation relies on the following assumptions: the receiving and transmitting antennas are directed towards each other, the antenna are correctly aligned and have the same polarization, and the antennas are unobstructed with no multipath noise. In general, the Friis Transmission Equation states that more power is lost at higher frequencies than would be lost at lower frequencies. RSSI is a power measurement of the received signal in decibels, and the further away from 0 that the RSSI value is, the weaker the signal is.

The communication protocols chosen were based on the above principles as well as with consideration for problems such as rain fading etc. In general, lower frequencies travel farther with a lower data rate while higher frequencies travel a shorter distance but allow a higher data rate. Also, frequencies below 11GHz tend to be affected less by environmental changes such as rain. Bluetooth 5 was chosen as a communication protocol because it is rolled into everyday phones and it supports a high data rate. LoRa was chosen because LoRa was designed for long distance sensor applications. LoRa is also a much lower frequency than Bluetooth so it should travel much farther. In addition,

the FSK module was tuned for 433MHz which is about half the frequency of LoRa, but it uses a simpler transmission protocol so it will be affected more by multipath problems.

Wireless communication protocols are a result of general digital communication systems. Figure 3.4 shows a block diagram of a general digital communication system. The digital send transmits a message in individual bytes. A byte, called a frame, is sent to the encoder block. The encoder transforms the frame into a transmission protocol, which are discussed below, by combining the message signal with a carrier signal. The frame is then sent to the carrier circuits which contain the antennae and the supporting circuits for transmission. The signal is then picked up by the carrier circuits on the receiving end. The received signal is then sent to the decoder where the signal is decoded into a frame and the frame of data is received by the digital receiver.

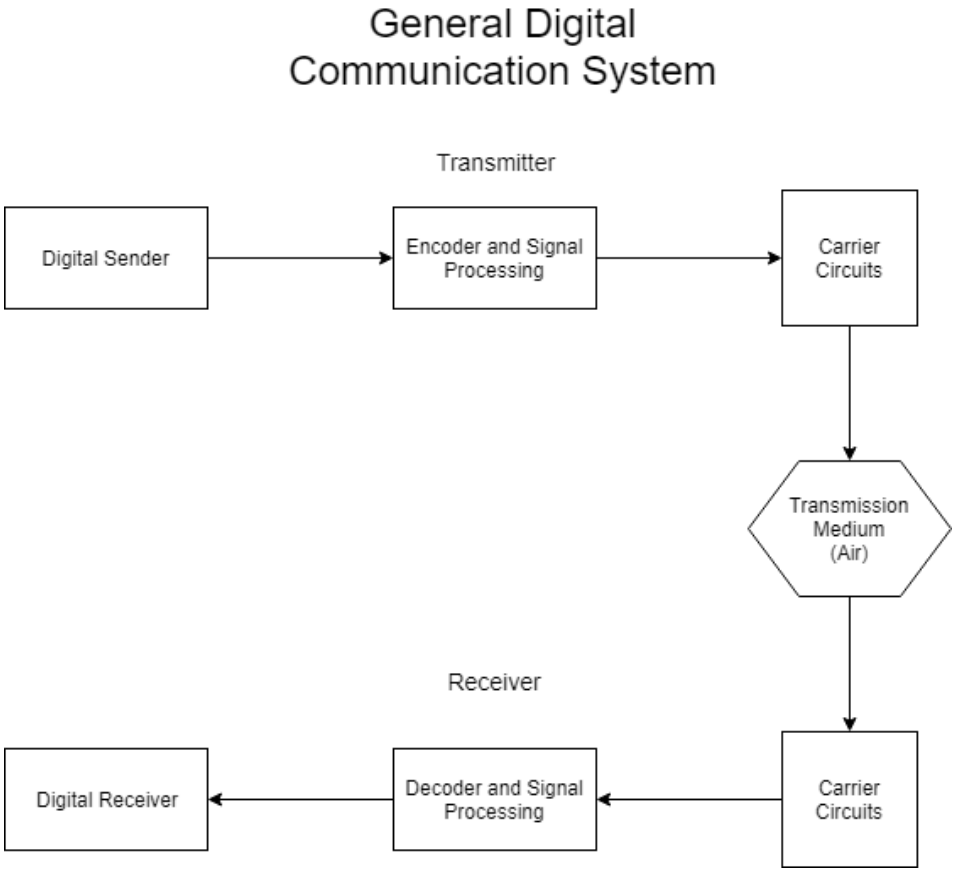

Figure 3.4 *General Digital Communication System*

3.3.1 LoRa

LoRa is a spread spectrum modulation technique that was developed from chirp spread spectrum (CSS) technology. CSS is a form of Direct-Sequence Spread Spectrum (DSSS). DSSS is a spread spectrum modulation technique. Spread spectrum means that the message being sent is spread out in the frequency domain. This technique is very important to handle the multipath problem in RF communications. The multipath problem is a type of interference caused by the transmission medium which is electromagnetic radiation. This radiation propagates throughout the environment in a difficult to model way, although advances have been made in modeling radio signal propagation such as the Rayleigh fading and Rician fading models. The electromagnetic

propagation causes the same bits to appear multiple times to the receiver. This is typically handled on the signal processing side of the receiver with forward error correction (FEC), but it can also be combatted through spread spectrum techniques.

DSSS divides information into bits and each bit has its own frequency channel. This process is achieved by multiplying the carrier frequency with a pseudo noise signal. The pseudo noise signal is a pulse with a shorter duration. The result spreads the data into a bandwidth size equal to the pseudo noise signal, and the final sign is much more resistant to interference. In CSS, each bit is spread by a chirping factor. The spread factor is the number of chirps per bit. As the chirping factor increases, the data rate slows down.

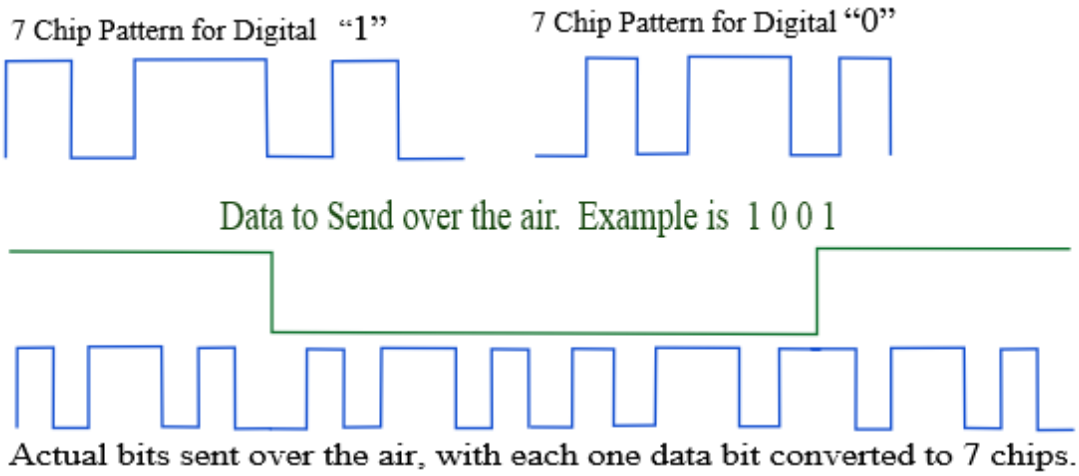

Figure 3.5 *LoRa Modulation Pattern. Spread Factor of 7 [40]*

LoRa is the first low cost implementation of CSS that is available for public and commercial use. LoRa is a long-range low-cost protocol that is targeted for internet of things (IoT) use. LoRa implementations aim for a 10-year life span on a common watch battery. The range that LoRa aims for is a 15 km transmission distance. Because of this long range a single node can collect data from thousands of sensor nodes that is deployed

kilometers away. The data rate of LoRa is 27 kbps normally [41] or 50 kbps when the LoRa chipset is using Frequency Shift Keying (FSK).

The main issues of LoRa is latency as 27 kbps is a very slow transmission rate. The total data transmitted per day has been measured to be as low as 1.5MB per day. This transmission rate is acceptable for delay tolerant applications such as data collection from nodes. Some of the proposed applications that LoRa is useful for is the real time monitoring of agricultural operations.

The LoRa board that was investigated is the B-L072Z-LRWAN1 which is a low power discovery kit made by ST Microelectronics. The board boasts a 20dBm transmitter, and a Murata Sigfox Module. [42] The board was mainly chosen for its community support and documentation. LoRa operates at 868MHz, and the antenna provides a 3dBi gain. Wavelength is related to frequency by the speed of light as demonstrated in Equation 2. This means that the Received Power can be calculated as shown in Table 3.1.

$$\lambda = \frac{C}{f}$$

Equation 2: Wavelength to Frequency

Distance Between Antennas (m)	Power (dBm)
10	-25.21377314
100	-45.21377314
1000	-65.21377314

Table 3.2 *Estimated Received Power by Distance for 868 LoRa*

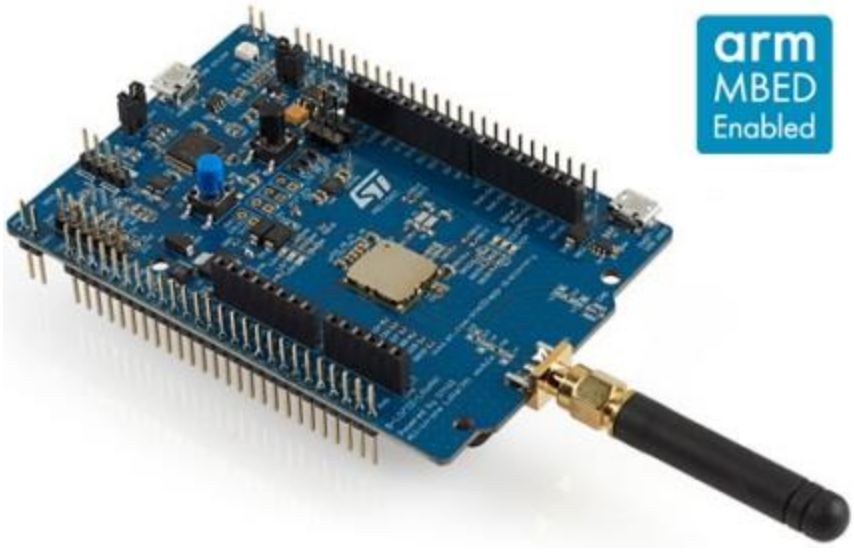

Figure 3.6 *STM32L0 Discovery Kit LoRa Low Power Wireless [42]*

3.3.2 Frequency Shift Keying

FSK is a modulation scheme where digital data is encoded into discrete changes in the carrier signals frequency. Binary FSK is the simplest and is shown below in figure 3.7, but other schemes also exist.

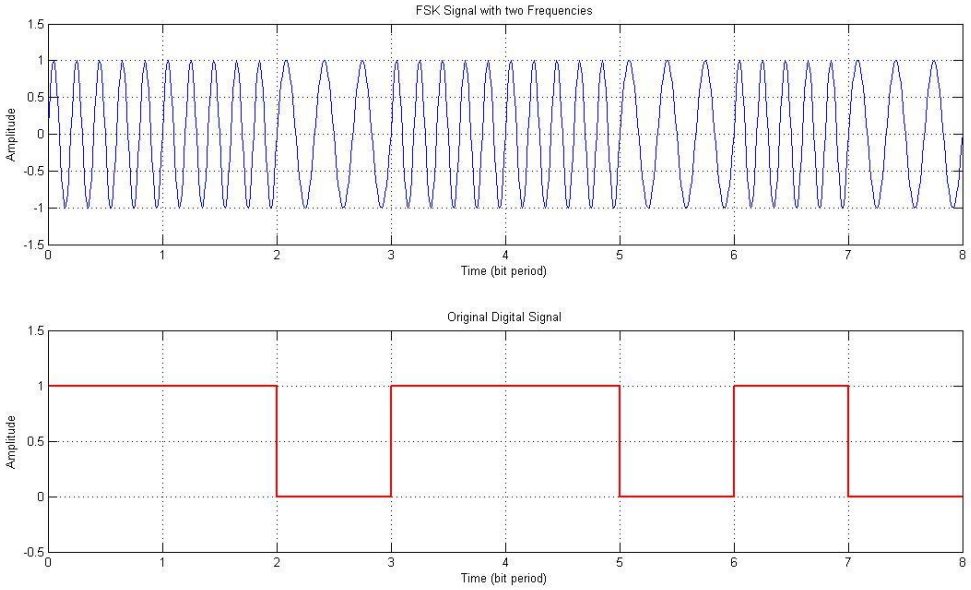

Figure 3.7 *FSK [43]*

Other forms of FSK consist of Continuous Phase Shift FSK (CPFSK), Gaussian FSK (GFSK), Minimum FSK (MSK), Gaussian Minimum FSK (GMSK), and Audio FSK (AFSK). CPFSK is a variation in which the transmitted signal maintains continuous phase while switching frequencies. A continuous phase is desirable when transmitting over a bandlimited channel. GFSK uses a gaussian filter to smooth the frequency transition. MSK is a more efficient from of FSK in which the difference between the high and low frequencies is equal to half of the carrier signals period. GMSK is a gaussian variant of MSK and uses a gaussian filter to smooth the transitions. AFSK represents changes in digital signals by variations in the frequency of an audio tone which makes the signal more suitable for radio or telephone transitions.

The RFM69HCW is a radio transceiver module that is made to operate in the license free Industry, Scientific, and Medical frequency bands. The module has a +20dBm power output capability, and uses FSK, although it supports other keying methods. The main use case of this module is to create RF networks that spread out farther than the 2.4GHz protocols such as 802.15.4. The development board chosen for this module is the Adafruit Feather 32u4 Radio or RadioFruit for short. The board claims to achieve 1,148ft of range. [44]

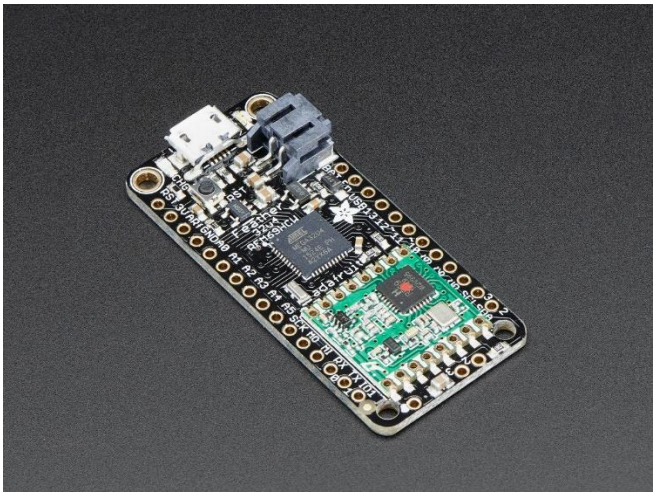

Figure 3.8 *Adafruit Feather 32u4 with RFM69HCW Packet Radio [44]*

The antennae used is a quarter wave whip antenna with a gain of 5.19 db. This gives us the following Received Power estimates as seen in Table 3.2.

Distance Between Antennas (m)	Power (dBm)
10	-14.79313672
100	-34.81317335
1000	-54.79313672

Table 3.3 *Estimated Received Power by Distance for 433 RFM69*

3.3.3 Bluetooth 5

Bluetooth at the protocol level operates in the ISM frequency band and is based on the Gaussian Frequency Shift Keying (GFSK) modulation. GFSK is a form of FSK, but it uses a gaussian filter to smooth the frequency transition. In FSK modulation the frequency shift happens very quickly, however in GFSK, there is a smooth transition between the different frequencies. This version of FSK reduces sideband power which has the advantage of decreasing interference. One downside is that the smoothing pulse can be used to determine the carrier frequency.

Bluetooth is low power, typically between 45mW and 84mW. [45] Bluetooth would be easy to deploy because most phones have a Bluetooth function. This would mean that the communication module could be deployed as a phone application. Bluetooth 5 was chosen specifically because it boasts a very long range. Bluetooth 5 Low Energy Long Range is advertised as 100 ft to 1,000 ft, and the board chosen for this experiment the Fanstel BT832x boasts an average range of up to 3,740ft. [46]

Figure 3.9 *BT832X The Longest Range Bluetooth 5 Module [46]*

Bluetooth 5 operates with a 2.4GHz signal which makes the technology very good for transmitting data at a high rate. The BT832X transmits at 20dBm, but unfortunately the module doesn't have an antenna that can be attached to the evaluation board. Without

the antenna, and with the high frequency this module should transmit the shortest distance of all 3 different RF technologies.

In summary, all three communication protocols can provide the necessary range in theory. They differ in communication methodologies and have various advantages such the FSK module can reach great distances at lower powers however the FSK module will be susceptible to multipath interference. The LoRa module uses CSS to reduce multipath interference but will draw more power. The Bluetooth module will transmit a shorter distance, but it has a higher data rate and is more accessible. Furthermore, the Bluetooth module will hand interference better than the FSK module, but not as well as the LoRa module.

CHAPTER IV - Data

The Data Section will be broken into the following parts, the first section will show a diagram of where the physical connection of the signal based involuntary grounding technique. The second section will demonstrate the power draw of the 3 boards. The third section will demonstrate the range of the module. The final section will show the waveform of the system when the module is turned on vs when the module is turned off.

4.1 Physical Layer

The system as seen in Figure 4.1 places a gate between the RF Receiver and the Flight Controller. The gate is controlled by the module, and the module responds to input from the RFM69HCW, Bluetooth 5, or LoRa WAN.

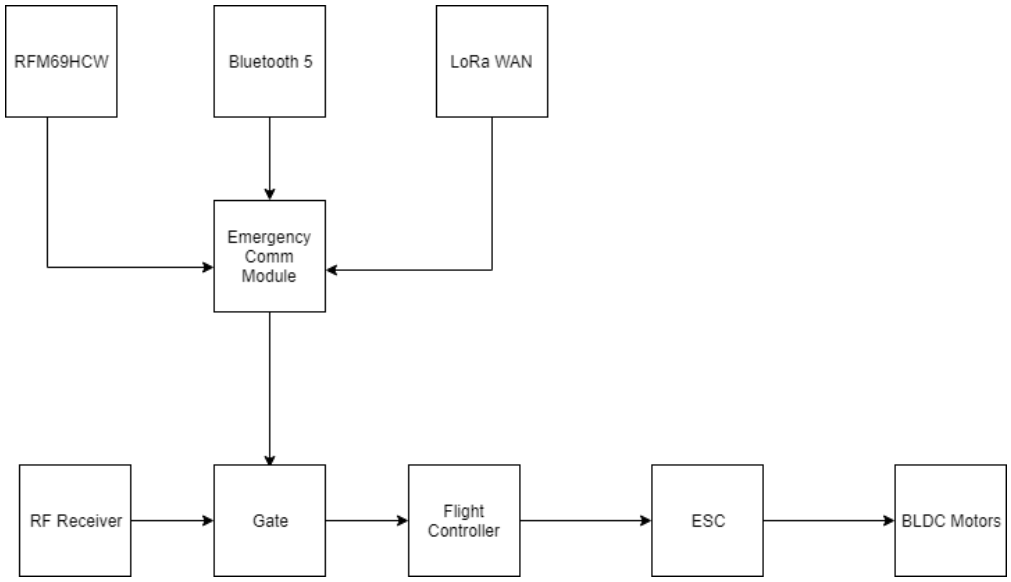

Figure 4.1 *Block Diagram of Drone Equipped with Communication Module*

The first direct implementation of the gate involved putting the microcontroller directly between the two modules. The microcontroller would read inputs on one side and then transfer the input to the output pins. When, a signal was received by the

communication module the processor would cut all output. Effectively, this setup used the microcontroller as a switch. This setup caused the motors to behave in a jerky manner. The jerky behavior was caused by the microcontroller adding delay to the signal from processing the input. This lag was overcome by using a digital AND gate to shut the signal off. The AND gate is also a simple digital logic circuit and the amount of signal lag that the circuit introduces is on the order of nanoseconds which is negligible in the system signal speed that drones use which is on the order of milliseconds.

4.2 Power Measurements

The power draw of the communication module is negligible compared to the power draw of the motors on a drone which have a free spin power draw of over 26W. That being said measuring the power draw is still important for making a final decision in order to state power supply specifications. The drone used for this study was powered by an 11.1V 3S LiPo battery rated for 2200mAH. The battery was wired into the ESCs which have a battery elimination circuit that provides a 5V output. This 5V output was then fed into the flight controller and the 5V rail was then spliced off to the microcontroller which has a voltage regulator on the development board to obtain a 3.3V rail. This rail was then used to power the communication boards.

The power of the three communication boards was measured with a Keithley 2280S-60-3 Precision Measurement Power Supply. The receiver was hooked up to the power supply and then measurements were taken with the transmitter set to send a signal every second.

	BL072 LoRa	BT832X Bluetooth 5	RFM 68HCW
Min Power	302.49 mW	54.85 mW	91.02291 mW
Max Power	345.69 mW	107.152 mW	108.30236 mW
Mean Power	336.35 mW	61.7 mW	91.69116 mW

Table 4.1 *Power Measurements*

4.3 Distance Measurements

The maximum distances of all 3 devices were measured in a mostly clear area near a hanger. The main obstacles were trees and hills in the area. The distance was measured by walking with the receiver and then dropping a pin on a location using an Android smart phone GPS. The maximum distance was reached when the receiver stopped receiving a ping every 40 seconds. A total distance of 1,367.53 ft was observed for LoRa WAN. A total distance of 417.27 ft was observed for Bluetooth 5. This distance was much less than the claimed 1,100+ ft. The distance may be extended with a Bluetooth 5 Smartphone or an antenna. The maximum distance of 861.26 ft was observed. These results are demonstrated in Table 4.2, and Figures 4.2 to Figure 4.4 show the maps of the areas that were used to demonstrate the communication.

	Distance	Base Location (Lat, Long)	Ending Location (Lat, Long)	Mean Power
LoRa WAN	1,367.53ft	32.305836, -90.8552461	32.3021512, -90.8551496	336.35mW
Bluetooth 5	417.27ft	32.305836, -90.8552461	32.3047349, -90.8555274	61.7mW
FSK	861.26ft	32.305836, -90.8552461	32.3035863, -90.8555271	91.69116mW

Table 4.2 *Communication Technology Distances and Power Draw*

Figure 4.2 *LoRa WAN Distance Measurements Maximum Distance: 1,138.79ft*

Figure 4.3 *Blue Tooth 5 Maximum Distance: 192.24ft*

Figure 4.4 *RFM69HCW Maximum Distance: 861.26ft*

DEVICE	RSSI Calculated	RSSI Measured	Difference	LAT	LONG
BASE				32.305836	-90.8552461
LoRa 1	-39	-60	42.42%	32.3054413	-90.8554
LoRa 2	-47	-70	39.32%	32.3047745	-90.8555613
LoRa 3	-50	-77	42.52%	32.304167	-90.8554584
LoRa 4	-52	-85	48.18%	32.3037022	-90.8552384
LoRa 5	-56	-92	48.65%	32.3027013	-90.855098
LoRa 6	-57	-97	51.95%	32.3021512	-90.8551496
bt832x 1	NA	-65	NA	32.305823	-90.8554922
bt832x 2	NA	-68	NA	32.305823	-90.8554832
bt832x 3	NA	-70	NA	32.3052518	-90.8554379
bt832x 4	NA	-75	NA	32.3051486	-90.8554691
bt832x 5	NA	-90	NA	32.3047349	-90.8555274
RFM69HCW	-25	-58	79.52%	32.305564	-90.8550738
RFM69HCW	-33	-68	69.31%	32.3051024	-90.8554295
RFM69HCW	-34	-72	71.70%	32.3049882	-90.8556324
RFM69HCW	-38	-75	65.49%	32.3045022	-90.8555975
RFM69HCW	-40	-77	63.25%	32.3040825	-90.8556988
RFM69HCW	-41	-79	63.33%	32.3038232	-90.8553524
RFM69HCW	-42	-82	64.52%	32.3036776	-90.8553497

Table 4.3 *RSSI Values at Distance*

The RSSI values of the LoRa module demonstrated a range of 40% to 51% difference at the farthest distance. The RSSI values of the FSK module differed between 63% and 79%. The percentage difference did increase as the distance increased. RSSI values for the Bluetooth 5 module were not able to be calculated due to a lackof data. The data points showed a drop in RSSI as the distance increased.

4.4 System Response

When the module is inactive, the drone behaves completely as normal. This was verified on a Keysight Infinivision DSOX2014A Digital Oscilloscope and the output waveform can be seen in Figure 4.5. The output waveform is a 55Hz signal with a 1.83V

amplitude. When the module is active, the system does not respond at all which can be seen in Figure 4.6. The waveform is taken from the gate to the Flight Controller.

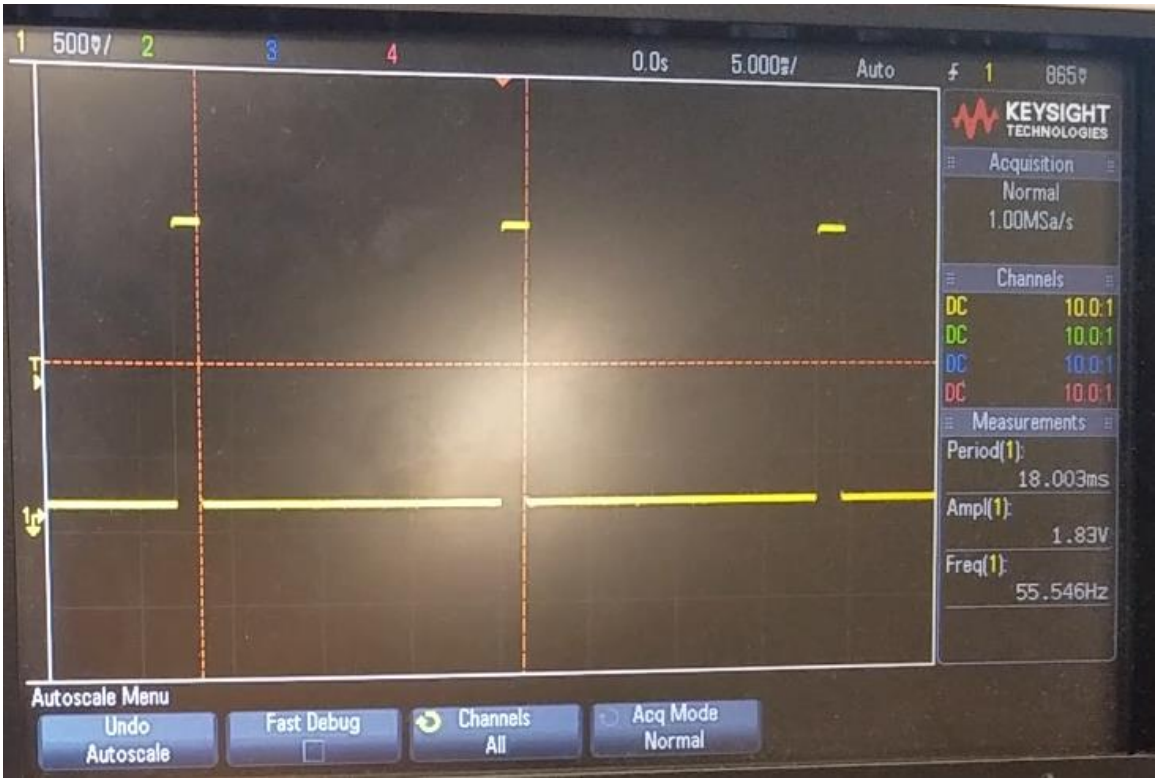

Figure 4.5 *Waveform from the Gate to the Flight Controller with the Communication Module Inactive*

Figure 4.6 *Waveform from the Gate to the Flight Controller with the Communication Module active*

The output signal is just a 0V level signal. This guarantees that no data will be received by the flight controller and the system will cease to function completely.

CHAPTER V – Discussion

This section provides an analysis of the previous chapter. Section 1 begins by discussing the physical layer of the grounding technique. Section 1 covers everything learned in connecting the devices and where the devices should be connected. Section 2 discusses the power measurements of the communication modules. Section 3 analyzes the distance of the communication modules and provides a discussion on the RSSI values by distance.

5.1 Physical Layer

There are several places to put a physical gate onto a drone. The two points that were investigated were between the flight controller and the ESCs, and between the RF Receiver and the flight controller. The first setup that tested was placing a microcontroller between the flight controller and the ESC. This setup had the following advantages: all signals were digital, and only two pieces of hardware would be needed. The flight controller transmits a PWM signal to the ESC to control motor speed. This is a digital signal that is easy for processors to understand, and it has the direct benefit that the motors can be shut off completely bypassing the flight controller completely. This placement would be a good place to ultimately put, the module, but for the initial prototype it includes the disadvantage of increasing the number of wires needed in order to shut off the drone.

The other place to put the shut off module is between the RF Receiver and flight controller. This was the chosen placement because the output signal is 55Hz which is slow enough to handle with any active circuit, and the RF receiver can transmit the SBus

signal which reduces the output signal to a single wire which is easy to wire up for the module.

5.2 Power Measurements

The Bluetooth 5 module demonstrated the lowest power draw overall with an average draw of 61.7mW. The low power draw can be partly attributed to the fact that Bluetooth 5 board was the least responsive board overall. Even with the app next to the board, the LED couldn't blink reliably every second. The RFM69HCW came in second with a mean power draw of 91.69116mW. The RFM69HCW also had the fewest LEDs on the board, and a smaller voltage regulator which all attributed to the low power draw. The LoRa came in last with a mean power draw of 336.35mW. The LoRa board also had the most LEDs and the LEDs were the brightest of the 3 boards which is correlated to power draw. All together the three boards power draw can be reduced even more, however the power measurements here would still scale down to some proportion.

5.3 Distance Measurements

The LoRa WAN module came in first with a distance measurement of 1,367.53ft. At the final distance the data was only being sent by maintaining a clear transmission path to the board. In practice the transmission distance will likely be around 700ft because there will be trees and other obstacles in an emergency. The RFM69HCW came in second with a distance measurement of 864ft. The RFM69HCW lost connection past that distance. It is theorized that distance comparable to the LoRa board could be achieved with a more open line of sight, however the hilly terrain as well as the tree cover make it difficult to maintain line of sight. The Bluetooth 5 Module came in last place with a distance measurement of 417.27ft. Many problems were had with the Bluetooth 5

board. The Bluetooth 5 board was kept parallel to the phone the entire time. The boards response to trees and other obstacles were not tested due to the low distance. It would be possible to get more distance by attaching an antenna, but a place to attach an antenna conveniently wasn't available on the board. Similarly, a 2.4GHz antennae would have to be obtained. Also, in a very interesting turn, the measured RSSI values did not align with the predicted RSSI values. The current working theory is that the difference is caused by changes in elevation, and that the modules are being used on the ground.

The difference in RSSI values actually increased as the distance increased. RSSI values are reported as dBm which is a logarithmic scale where every 3 decibels demonstrate a doubling. The logarithmic scale explains that as the distance increases, the drop in RSSI relative to distance decreases. This is shown in the measured values for the FSK module wherein the difference between 83m and 100m, a difference of only 17m, is 4dBm whereas the difference between 100m and 150m, a difference of 50m, is 3dBm.

The FKS module reports values that are between 63% and 52% off. The FSK module did not come with an antenna and a quarter wave wire antennae was made by hand for it. Antennae gain is also a logarithmic scale, so it stands to reason that the percent difference is due to human error in making the antennae. The LoRa module in contrast showed a difference range of 42% to 52%. The LoRa module also used an omnidirectional antenna that was manufactured and shipped with the device.

In Summary, the Bluetooth 5 module performed the worst overall by not meeting distance needs. The LoRa module performed the best in terms of distance and handling interference as was predicted previously. The FSK module performed good in terms of distance although it did not reach the distances of the LoRa module. The FSK module did

however use the least power to transmit over long range as was predicted via the frequency used.

CHAPTER VI – Conclusion

This thesis investigates the involuntary signal-based grounding of civilian unmanned aerial systems in unauthorized air spaces. The technique proposed here forcibly lands unauthorized UAS in a given area in such a way that the UAS will not be harmed, and the pilot cannot stop the landing. The technique will not involuntarily ground authorized drones which will be determined prior to the landing. Unauthorized airspaces that require an involuntary grounding solution include university campuses, areas affected by a natural disaster, and stadiums for public events. Three communication protocols were evaluated due to their long-range capabilities: LoRa WAN, Bluetooth 5, and FSK. LoRa was chosen because LoRa as a communication protocol not only provided long range but also low power and was was designed for use in IoT applications. Bluetooth 5 not only had long range capabilities, but Bluetooth5 is already ntegrated into common mobile devices. FSK was chosen because it is a simple protocol and low frequencies can be used to cover large distances with very low power. The system placement of the communication modules was proposed in two different places: between the rf receiver and the flight controller, and between the flight controller and the speed controllers. Out of the two placements, between the flight controller and the speed controllers is the best placement however between the rf receiver and the flight controller is the simplest to implement. Of the three technologies, LoRa WAN transmitted the farthest, however the FSK module transmitted a comparable distance at a lower power. The power measurements were taken using existing modules, however, due to LoRa using a higher frequency than the FSK module this outcome was expected.

Interestingly, the communication boards did not reach advertised distances. Furthermore, the predicted RSSI values did not correlate with the measured RSSI values. The predicted theoretical values are only correct in ideal conditions such as both antennas are elevated a certain height above the ground with flat terrain, and ideal line of sight conditions. It's impossible to guarantee ideal conditions in real-world use cases as can be demonstrated with the 79.52% disparity with the FSK module. Granted part of the disparity with the FSK module can be explained with a hand crafted nonideal antennae. Unfortunately, companies test their product in ideal conditions with their own ideal antennas and report ideal performance. This causes a disparity between advertised performance and real-world performance. This disparity can cause problems when designing new products and demonstrates a need to measure performance before using a certain product or technology.

The next steps for this research will involve creating a weather ruggedized module. The module needs to be ruggedized in order to allow it to be used by UAS in practice. After the module itself is ruggedized, a discrete transmitter will be created in order to reduce potential problems with the transmission software. The next steps will involve crafting the new transmission protocol to distribute keys and writing the software to maintain the authorized UAS. Finally, a prototype flight control board will be crafted to supply the hardware keys that will be used to grant authorization.

This thesis focuses on UAS in emergency situations and views the use of UAS as a net good, however many express concerns for UAS in civilian airspaces during peace time. This general unease can be seen through works by those such as Ravich who writes about upcoming regulatory frameworks for UAS. [47] Ravich states that governments

around the world are viewing UAS as a force which can upend society. UAS present many problems in society such as increasing noise pollution and allowing regular people the ability to spy on others and record video without being bounded. Other concerns with UAS involve UAS interacting with animals. Horses, and other large animals are normally spooked when they come into contact with UAS. These concerns are being reported on which demands a response from regulatory bodies. Ravich furthers reports that the FAAs normal policy is nonenforcement. [48] The national airspace is heavily regulated, but most of these regulations apply to aircraft whereas UAS are designated as model aircraft.

UAS privacy concerns is a very interesting problem and it ties into other ethical concerns that are relevant in our society right now such as data privacy. Smartphones are constantly sending data back to their perspective companies, and a UAS is no different. The U.S. Department of Defense is especially concerned with UAS data, and have responded by banning all UAS, except for approved models from approved vendors, from being flown.

The right to privacy and the ownership of data is a major concern in the 21rst century, and a concern that has not been adequately addressed. The EU has impelemented the General Data Protection Regulation (GDPR) in 2018. The GDPR does apply pressure on UAS companies. [49] Under the GDPR fines can be issued if a person's face is visible without consent or if a person can be identified in any other way such as location, landmarks, etc. A criticism of regulatory responses such as the GDPR is that large companies can afford the fines whereas small companies and startups will just close up shop. In the case of the U.S. Department of Defense, an approved vendor list shuts down market competition. In the case of the GDPR, the regulation means that a large company

such as Google can operate UAS, but an aspiring photographer can be bankrupt from fines. In order to handle these cases, the FAA has created a waiver process which Ravich criticizes by stating “a system of waivers in itself creates the prospect of writing policy through a series of exemptions rather than purposeful design.” [47]

One of the bigger concerns with drone regulation is that the process is inconsistent with the process other innovations have underwent. Ravich uses the example of self-driving vehicles, as automakers have not been required to obtain preapproval to pursue this technology. As an addendum, UAS deliver the same privacy concerns as smartphones delivering cameras to the masses. However, the regulatory concerns on everyone having access to a camera was minor. Either way, research in the UAS space will ever march forward as inventions cannot be uninvented.

REFERENCES

[1] “Communications Status Report for Areas Impacted by TS Harvey.” Federal Communications Commission, 6 Oct. 2018, www.fcc.gov/document/communications-status-report-areas-impacted-ts-harvey-0.

[2] “2017 Hurricane Season FEMA After-Action Report”, United States Federal Emergency Management Agency, 12 July 2018 https://www.hsdl.org/?view&did=812985 accessed on May 2019

[3] “FAA's Hurricane Michael Update.” FAA Seal, 12 Oct. 2018, www.faa.gov/news/updates/?newsId=91886.

[4] Schalk, L. M., & Herrmann, M. (2017). Suitability of LTE for drone-to-infrastructure communications in very low level airspace. AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2017-Septe. https://doi.org/10.1109/DASC.2017.8102112

[5] P. Blank, S. Kirrane and S. Spiekermann, "Privacy-Aware Restricted Areas for Unmanned Aerial Systems," in IEEE Security & Privacy, vol. 16, no. 2, pp. 70-79, March/April 2018, doi: 10.1109/MSP.2018.1870868

[6] U. C. Fiebig, “ICNS - interactive workshop ”How drones are changing the world we live in”,” in 2016 Integrated Communications Navigation and Surveillance (ICNS), April 2016, pp. 1–10.

[7] B. Kloiber, C. Rico-Garcia, J. Harri, and T. Strang, “Update delay: A new information-centric metric for a combined communication and application level

reliability evaluation of cam based safety applications," in ITS World Congress, 2012. [Online]. Available: http://elib.dlr.de/76812/

[8] Van Der Bergh, B., Chiumento, A., & Pollin, S. (2016). LTE in the sky: Trading off propagation benefits with interference costs for aerial nodes. IEEE Communications Magazine, 54(5), 44–50. https://doi.org/10.1109/MCOM.2016.7470934

[9] Lin, X., Wiren, R., Euler, S., Sadam, A., Maattanen, H.-L., Muruganathan, S. D., … Yajnanarayana, V. (2018). Mobile Networks Connected Drones: Field Trials, Simulations, and Design Insights. (c), 1–8. Retrieved from http://arxiv.org/abs/1801.10508

[10] Wigard, J., Sorensen, T. B., Nguyen, H., Kovacs, I. Z., Amorim, R., & Mogensen, P. (2017). Radio Channel Modeling for UAV Communication Over Cellular Networks. IEEE Wireless Communications Letters, 6(4), 514–517. https://doi.org/10.1109/lwc.2017.2710045

[11] Zhao, T., Luo, C., Min, G., Miao, W., Zhou, J., Guo, D., … May, S. P. (n.d.). A DoA Estimation Based Robust Beam Forming Method for UAV-BS Communication, 1–9.

[12] Muruganathan, S. D., Lin, X., Maattanen, H.-L., Zou, Z., Hapsari, W. A., & Yasukawa, S. (2018). An Overview of 3GPP Release-15 Study on Enhanced LTE Support for Connected Drones. 1–7. Retrieved from http://arxiv.org/abs/1805.00826

[13] Li, J., Zhou, Y., & Lamont, L. (2013). Communication architectures and protocols for networking unmanned aerial vehicles. 2013 IEEE Globecom

Workshops, GC Wkshps 2013, 1415–1420. https://doi.org/10.1109/GLOCOMW.2013.6825193

[14] Asadpour, M., Giustiniano, D., Hummel, K. A., & Heimlicher, S. (2013). Characterizing 802.11n aerial communication. 7. https://doi.org/10.1145/2491260.2491262

[15] Raffelsberger, C., Muzaffar, R., & Bettstetter, C. (2019). A Performance Evaluation Tool for Drone Communications in 4G Cellular Networks. Retrieved from http://arxiv.org/abs/1905.00115

[16] Merwaday, A., & Guvenc, I. (2015). UAV assisted heterogeneous networks for public safety communications. 2015 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2015, 329–334. https://doi.org/10.1109/WCNCW.2015.7122576

[17] Chandrasekharan, S., Rasheed, T., Goratti, L., Reynaud, L., Grace, D., Bucaille, I., … Allsopp, S. (2016). Designing and Implementing Future Aerial Communication Networks. IEEE Communications Magazine, 54. https://doi.org/10.1109/MCOM.2016.7470932

[18] Leszek T. Lilien, Lotfi Ben Othmane, Pelin Angin, Andrew Decarlo, Raed M. Salih, and Bharat Bhargava. 2014. A simulation study of ad hoc networking of UAVs with opportunistic resource utilization networks. J. Netw. Comput. Appl. 38 (February 2014), 3–15.

[19] Tareque, M. H., Hossain, M. S., & Atiquzzaman, M. (2015). On the Routing in Flying Ad hoc Networks. Proceedings of the 2015 Federated Conference on

Computer Science and Information Systems, 5(October), 1–9. https://doi.org/10.15439/2015f002

[20] Aranzazu Suescun, C., & Cardei, M. (2016). Unmanned Aerial Vehicle Networking Protocols. (January). https://doi.org/10.18687/laccei2016.1.s.078

[21] Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. IEEE Communications Surveys and Tutorials, 18(4), 2624–2661. https://doi.org/10.1109/COMST.2016.2560343

[22] Alshabtat, A., Dong, L., Li, J., & Yang, F. (2010). "Low latency routing algorithm for unmanned aerial vehicles ad-hoc networks." International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 6(1), 48–54. Retrieved from http://waset.org/journals/waset/v56/v56-137.pdf

[23] Hayat, Samira & Yanmaz, Evsen & Bettstetter, Christian. (2015). Experimental analysis of multipoint-to-point UAV communications with IEEE 802.11n and 802.11ac. 1991-1996. 10.1109/PIMRC.2015.7343625.

[24] Kopeikin, A., Ponda, S. S., Johnson, L. B., & How, J. P. (2012). Multi-UAV network control through dynamic task allocation: Ensuring data-rate and bit-error-rate support. 2012 IEEE Globecom Workshops, GC Wkshps 2012, 1579–1584. https://doi.org/10.1109/GLOCOMW.2012.6477821

[25] Mozaffari, M., Saad, W., Bennis, M., & Debbah, M. (2017). Wireless communication using unmanned aerial vehicles (UAVs): Optimal transport theory for hover time optimization. IEEE Transactions on Wireless Communications, 16(12), 8052–8066. https://doi.org/10.1109/TWC.2017.2756644

[26] Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Communications Magazine, 54(5), 36–42. https://doi.org/10.1109/MCOM.2016.7470933

[27] Bunse, C., & B, S. P. (2018). Engineering Secure Software and Systems (Vol. 10953). https://doi.org/10.1007/978-3-319-94496-8

[28] Valente, J., Sanz, D., Barrientos, A., del Cerro, J., Ribeiro, Á., & Rossi, C. (2011). An air-ground wireless sensor network for crop monitoring. Sensors, 11(6), 6088–6108. https://doi.org/10.3390/s110606088

[29] Tansuriyavong, S., Koja, H., Kyan, M., & Anezaki, T. (2018). The Development of Wildlife Tracking System Using Mobile Phone Communication Network and Drone. 2018 International Conference on Intelligent Informatics and Biomedical Sciences, ICIIBMS 2018, 3, 351–354. https://doi.org/10.1109/ICIIBMS.2018.8549936

[30] Deaconu, I., & Voinescu, A. (2014). Mobile gateway for Wireless Sensor Networks utilizing drones. Proceedings - RoEduNet IEEE International Conference. https://doi.org/10.1109/RoEduNet-RENAM.2014.6955319

[31] He, X., Bito, J., & Tentzeris, M. M. (2017). A drone-based wireless power transfer and communications platform. WPTC 2017 - Wireless Power Transfer Conference, 1–4. https://doi.org/10.1109/WPT.2017.7953846

[32] Choi, S. C., Sung, N. M., Park, J. H., Ahn, I. Y., & Kim, J. (2017). Enabling drone as a service: OneM2M-based UAV/drone management system. International Conference on Ubiquitous and Future Networks, ICUFN, 18–20. https://doi.org/10.1109/ICUFN.2017.7993739

[33] Celtek, S. A., Durdu, A., & Kurnaz, E. (2019). Design and Simulation of the Hierarchical Tree Topology Based Wireless Drone Networks. 2018 International Conference on Artificial Intelligence and Data Processing, IDAP 2018, 1–5. https://doi.org/10.1109/IDAP.2018.8620755

[34] Gharibi, M., Boutaba, R., & Waslander, S. L. (2016). Internet of Drones. IEEE Access, 4(JANUARY), 1148–1162. https://doi.org/10.1109/ACCESS.2016.2537208

[35] C. Bohm, M. Hofer, and W. Pribyl, "A microcontroller sram-puf," in Network and System Security (NSS), 2011 5th International Conference September 2011, pp. 269–273.

[36] Amos Fiat, Moni Naor (1994). Broadcast encryption. Proc. Advances in Cryptology – CRYPTO '93 (Extended abstract). Lecture Notes in Computer Science. 773. pp. 480–491. doi:10.1007/3-540-48329-2_40. ISBN 978-3-540-57766-9.

[37] “CopterControl / CC3D / Atom Hardware Setup”. Copyright LibrePilot/OpenPilot community. Revision 7a5018f0. Accessed, September 15, 2019, https://opwiki.readthedocs.io/en/latest/user_manual/cc3d/cc3d.html

[38] González-Jorge, Higinio & Martínez-Sánchez, Joaquin & Bueno, Martín & Pedor Arias, and. (2017). Unmanned Aerial Systems for Civil Applications: A Review. Drones. 1. 2. 10.3390/drones1010002.

[39] Friis, H.T. (May 1946). "A Note on a Simple Transmission Formula". IRE Proc.: 254–256.

[40] The LoRa Protocol, Raveon technologie, Accessed September 7, 2019, https://www.raveon.com/data_radio_info/the-lora-protocol-1159/

[41] Ferran Adelantado, Xavier Vilajosana, “Understanding the Limits of LoRaWAN”, 8 September 2017 IEEE Communications Magazine Volume: 55 issue 9

[42] B-L072Z-LRWAN1 STM32L0 Discovery kit LoRa, Sigfox, low-power wireless, ST Microelectronics, Accessed September 7, 2019, https://www.st.com/en/evaluation-tools/b-l072z-lrwan1.html

[43] Shah Gul Khan “Binary Frequency Shift Keying” Mathworks March 2011 https://ch.mathworks.com/matlabcentral/fileexchange/30581-binary-frequency-shift-keying?s_tid=FX_rc1_behav

[44] Adafruit Feather 32u4 with RFM69HCW Packet Radio - 433MHz – RadioFruit, Adafruit, Accessed September 1, 2019, https://www.adafruit.com/product/3077

[45] Siekkinen, M., Hiienkari, M., Nurminen, J. K., & Nieminen, J. (2012). How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4. 2012 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2012, 232–237. https://doi.org/10.1109/WCNCW.2012.6215496

[46] BT832X, The Longest Range Bluetooth 5 Module, Fanstel, Accessed September, 4, 2019, https://www.fanstel.com/bt832x-bluetooth-5-module

[47] T. Ravich, “Grounding Innovation”, *CBLR*, vol. 2018, no. 2, pp. 495-585, Jun. 2019.

[48] Ravich, Timothy, Emerging Technologies and Enforcement Problems: The Federal Aviation Administration and Drones as a Case Study (June 1, 2018). Journal of Regulatory Compliance, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3358451

[49] 8 Data Protection Guiding Principles Under the GDPR for Drone Pilots, 23 May, 2018, Accessed: September 2019, https://dronerules.eu/en/recreational/news/8-data-protection-principles-under-the-gdpr-for-drone-pilots