



Georgia Southern University
Digital Commons@Georgia Southern

Electronic Theses and Dissertations


Graduate Studies, Jack N. Averitt College of

Spring 2016

Design, Analysis and Evaluation of Unmanned Aerial
Vehicle Ad hoc Network for Emergency Response
Communications

Robin D. Grodi

Follow this and additional works at: <https://digitalcommons.georgiasouthern.edu/etd>

 Part of the [Signal Processing Commons](#), and the [Systems and Communications Commons](#)

Recommended Citation

Grodi, Robin D., "Design, Analysis and Evaluation of Unmanned Aerial Vehicle Ad hoc Network for Emergency Response Communications" (2016). *Electronic Theses and Dissertations*. 1372.
<https://digitalcommons.georgiasouthern.edu/etd/1372>

This thesis (open access) is brought to you for free and open access by the Graduate Studies, Jack N. Averitt College of at Digital Commons@Georgia Southern. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact digitalcommons@georgiasouthern.edu.

DESIGN, ANALYSIS AND EVALUATION OF UNMANNED AERIAL VEHICLE AD
HOC NETWORK FOR EMERGENCY RESPONSE COMMUNICATIONS

by

ROBIN GRODI

(Under the Direction of Danda B. Rawat)

ABSTRACT

In any emergency situation, it is paramount that communication be established between those affected by an emergency and the emergency responders. This communication is typically initiated by contacting an emergency service number such as 9-1-1 which will then notify the appropriate responders. The communication link relies heavily on the use of the public telephone network. If an emergency situation causes damage to, or otherwise interrupts, the public telephone network then those affected by the emergency are unable to call for help or warn others. A backup emergency response communication system is required to restore communication in areas where the public telephone network is inoperable. The use of unmanned aerial vehicles is proposed to act as mobile base stations and route wireless communication to the nearest working public telephone network access point. This thesis performs an analysis based on wireless attributes associated with communication in this type of network such as channel capacity, network density and propagation delay.

Index Words: Unmanned Aerial Vehicle, Emergency Response Communication

DESIGN, ANALYSIS AND EVALUATION OF UNMANNED AERIAL VEHICLE AD
HOC NETWORK FOR EMERGENCY RESPONSE COMMUNICATIONS

by

ROBIN GRODI

B.S. in Electrical Engineering, Georgia Southern University, 2014

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial
Fulfillment
of the Requirement for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

©2016

ROBIN GRODI

All Rights Reserved

DESIGN, ANALYSIS AND EVALUATION OF UNMANNED AERIAL VEHICLE AD
HOC NETWORK FOR EMERGENCY RESPONSE COMMUNICATIONS

by

ROBIN GRODI

Major Professor: Danda B. Rawat

Committee: Sungkyun Lim

Fernando Rios-Gutierrez

Electronic Version Approved:

May 2016

DEDICATION

I would like to dedicate my thesis to my parents for everything they have given me. I cannot thank them enough.

My mom, for always pushing me to go one step farther. I used to hate the fact that no matter how good I did at something, you would always point out something that could be improved. I see that as a gift now, I am able to come up with a plan and follow it to completion for anything that I work on.

My dad, for teaching me to work with my hands. From being able to change my oil or brake pads to home improvements like that TV shelf we built, I have learned so much from you - even if it just started out with me watching you do everything.

Both you and mom have taught me to be a well-rounded person and I love you both for that. Thank you!

ACKNOWLEDGMENTS

First and foremost I would like to acknowledge Dr. Frank Goforth for convincing me to continue on to get my masters degree. Without his influence, I would not have pursued further education.

Dr. Danda B. Rawat for taking me under his wing as my advisor. When I started my masters degree, I had no idea what type of research I was interested in. I thought that joining a research lab meant I would have to work on a very specific topic related and designated by the advisor. Dr. Rawat showed me that almost every topic can be connected in one way or another and led to my work on UAVs being connected with his work on communication systems. Also, I feel like I now know how to write a proper research paper and present it clearly after all the practice I got during my time in his research lab.

My lab colleagues and friends: Swetha Reddy, Nimish Sharma, and Tanjil Amin. While we all worked on different research topics, we were able to provide feedback and suggestions to each other to further our research. Finishing our masters degree was a team effort and I am grateful to all of you.

I would also like to acknowledge all of the professors that taught me during my time at Georgia Southern University. Through your teachings I have been equipped with knowledge to join the work force and contribute to society.

Finally, I would like to thank and acknowledge the National Science Foundation (NSF Grant # CNS-1405670) and Georgia Southern University for helping to fund my research.

TABLE OF CONTENTS

	Page
DEDICATION	2
ACKNOWLEDGMENTS	3
LIST OF FIGURES	7
CHAPTER	
1 INTRODUCTION	9
1.1 Background	9
1.1.1 Emergency Response Communication	9
1.1.2 Wireless Communication	10
1.1.3 Unmanned Aerial Vehicles	11
1.2 Problem Statement	12
1.3 System Model	13
1.4 Thesis Outline	14
2 ENHANCING CONNECTIVITY FOR COMMUNICATION AND CONTROL IN UNMANNED AERIAL VEHICLE NETWORKS . . .	16
2.1 Introduction	16
2.2 System Model	17
2.3 Adaptive Connectivity Analysis	18
2.4 The Algorithm	21
2.5 Numerical Results and Discussion	21
2.6 Chapter Summary	24

3	PERFORMANCE EVALUATION OF UNMANNED AERIAL VEHICLE AD HOC NETWORKS	25
3.1	Introduction	25
3.2	System Model and Problem Formulation	27
3.3	Performance Analysis	28
3.4	Performance Evaluation and Numerical Results	30
3.5	Chapter Summary	37
4	UAV-ASSISTED BROADBAND NETWORK FOR EMERGENCY AND PUBLIC SAFETY COMMUNICATIONS	38
4.1	Introduction	39
4.2	System Model	41
4.3	Analysis	43
4.4	Performance Evaluation and Results	47
4.5	Chapter Summary	52
5	ROUTING SECURITY IN UAV-SUPPORTED MOBILE NETWORKS FOR DISASTER RESPONSE COMMUNICATION	54
5.1	Introduction	54
5.2	UAV Ad hoc Network Constraints	56
5.3	System Model	58
5.3.1	Scenario	59
5.3.2	UAV Mobile Base Stations	60
5.3.3	Deployment Centers	60
5.4	Routing Protocols for Mobile Ad Hoc Networks	61

	6
5.4.1 Proactive Routing	62
5.4.2 Reactive Routing	64
5.4.3 Hybrid Routing	66
5.5 Security in UAV Ad hoc Networks	66
5.5.1 Confidentiality, Integrity, Availability Triad	66
5.5.2 Routing Attacks	68
5.5.3 UAV Ad hoc Networks Security Solutions	70
5.6 Research Challenges	71
5.7 Chapter Summary	72
6 DISCUSSION, CONCLUSION, AND FUTURE WORK	73
6.1 Future Work	74
REFERENCES	76

LIST OF FIGURES

Figure	Page
1.1 A sample network of 7 UAVs and a ground station where UAVs form a communication link between the target of interest and the ground station via single or multi-hop communication.	13
2.1 Angle of Arrival Calculation for two UAVs.	21
2.2 The change in probability of successful connectivity after a given time. At time = 400, a UAV moves in such a way that it is no longer within communication range of the rest of the network. The adaptive connectivity algorithm is able to increase transmission power in order to minimize loss of connectivity. The static scenario is unable to adapt and therefore has a much lower probability of connectivity when such an event occurs.	23
3.1 A network of 3 UAVs showing transmission range and distance between UAVs where distance between UAVs can be computed using GPS locations. Note that the distance between them depends on relative velocity and direction of travel.	30
3.2 Datarate needed to transmit a given amount of data vs. the total available transmission time.	31
3.3 Total transmission range of the network vs. the number of UAVs in the network.	32
3.4 Worst case propagation delay of the network vs. the number of UAVs in the network.	33
3.5 Amount of data sent successfully (goodput) vs. the probability of a packet failing to reach the destination.	34
3.6 Goodput per unit energy vs. the number of UAVs in the network.	35

4.1	Typical scenario of cellular network with controller, disaster response center and disaster affected area.	40
4.2	Destroyed communication tower being covered by a network of 5 UAVs where these UAVs communicate with each other and nearby towers to be able to restore communication to the affected area.	41
4.3	Overlap of two UAVs' transmission ranges.	46
4.4	Assume a transmission power, P_t , of 2 watts and a threshold received power, P_r , of -90dBm (10^{-12} watts). The frequency range listed is from 900 MHz to 2100 MHz which is the typical cell phone operating frequencies. Note that increasing the transmission frequency results in a decreased max obtainable transmission range.	48
4.5	Given 1 km transmission range of a original cell tower, the amount of UAVs needed are shown based on their respective transmission range.	49
4.6	Channel Capacity vs. Signal to Interference plus Noise Ratio (SINR) γ_k for $\frac{R_D}{R} = 4$, path loss exponent $\alpha = 2$ and different K values.	50
4.7	Channel Capacity vs. the ratio $\frac{R_D}{R}$ for Signal to Interference plus Noise Ratio (SINR) $\gamma_k = 10dB$, path loss exponent $\alpha = 4$ and different K values.	51
5.1	Unmanned Aerial Vehicle (UAV) ad hoc network connecting and routing communication between two disjointed cell towers. Such a network can connect users and devices cutoff from the Public Telephone Network due to a damaged or destroyed cell towers.	58
5.2	The groupings of different types of Mobile Ad hoc Networks	62
5.3	Increasing the amount of overhead traffic (the control signals and other path information) results in the delay time associated with sending a message from one point of the network to the other to decrease.	63
5.4	A wormhole attack where an attacker node routes data to another part of the network while eavesdropping on the information. This attacker node can be turned on and off to cause havoc with the routing table in the network.	69

CHAPTER 1

INTRODUCTION

In any emergency situation, it is crucial that emergency services and responders be contacted as soon as possible in order to minimize loss of life and property. Typically, contacting emergency services is as easy as using a telephone to call an emergency number such as 9-1-1 for the United States or 9-9-9 for the United Kingdom. An operator will pickup and contact the appropriate emergency responders depending on the needs of the caller. The key requirement is the ability to communicate with the emergency number. This is done through the use of the public telephone network.

In the past, most homes were equipped with land-line phones that provided a direct physical connection to the public telephone network. This connection could easily be damaged or destroyed during emergencies such as natural disasters and would prevent people from calling for help. With the advent of wireless mobile phones, damage to the connections became more rare. For wireless phones, connections in an area rely on a cell tower to provide a stable link to the public telephone network. It is still possible for cell towers to become damaged or inoperable and so it is required that a response system be in place that can restore communication during times when connection to the telephone network becomes interrupted.

1.1 Background

1.1.1 Emergency Response Communication

Emergency Response Communication is a component of communication focusing on the communication between emergency responders during emergency situations. The main categories of emergency responders can be classified as Fire and Rescue, Emergency Medical Services (EMS), and Police. Each of these services focus on different tasks during

an emergency and currently use their own wireless communication frequencies and channels. This separation of communication between responder services can cause confusion and misinformation that could lead to loss of life. In order to counter this problem, congress and the FCC have created the Spectrum Act [4] that reserves the 700 MHz frequency band specifically for communication between emergency responders. Interoperability between emergency responders allows for the most up-to-date information to always be present. This reserved frequency band would also allow for more than just voice to be sent along communication links. Broadband data including pictures, videos, and other important information can be sent to emergency responders before they arrive at a location. The more detailed information that is accessible to emergency responders, the better they will be able to respond to a situation.

Fire and Rescue responders are responsible for fighting fires and conducting rescue operations. These operations can range from rescuing people from burning buildings to responding to car accidents. Emergency Medical Services focus on preserving life. These responders will attempt to keep a person alive until they can deliver them to a more equipped environment, such as a hospital. Police are responsible for protecting life and enforcing laws. They respond to calls that involve any sort of crime.

1.1.2 Wireless Communication

Wireless communication is an ongoing topic of research that focuses on efficient and stable wireless connections between multiple users. There are multiple branches of wireless communication but this thesis will focus mainly on ad hoc networks and their use for emergency response communication. In its most basic form, ad hoc networks are composed of devices that communicate without any predetermined infrastructure. Each user, or node, in the network acts as both a client and a router. In this way, messages travel along the network hopping between nodes until it reaches its destination. Each intermediate node

forwards the information onto the next node. Since only the sender of the message and the intended receiver have the encryption keys, the message can be forwarded without intermediate nodes being able to read the message.

There are two main types of ad hoc networks, proactive (table-driven) and reactive (on-demand). Both types of networks have advantages and disadvantages but the key difference is in how they form paths. For proactive routing protocols, paths between nodes are constantly updated and stored in a routing table. When a message needs to be sent, the path is ascertained from the routing table and the message is sent along that path. Proactive protocols requires the least amount of time to send and receive the message but at the cost of increased overhead traffic caused by constantly updating the routing table. For reactive protocols, the paths between nodes are only determined when a message needs to be sent. This type of protocol is slightly slower but saves bandwidth since there is no routing table required to be updated.

Due to it's dynamic nature, ad hoc networks are perfect for UAV networks since they can enter or leave the network at any time. Ad hoc networks sense this change in the overall network and will adjust routing paths in order to avoid communication interruption within the network.

1.1.3 Unmanned Aerial Vehicles

UAVs are devices capable of both controlled and autonomous flight. As it's name suggests, UAVs are controlled without the aid of an on-board human operator. For controlled flight, signals are received and processed by an on-board microcontroller which then forwards the appropriate signals to the motor's electronic speed controllers. For autonomous flight, signals are received by sensors attached to the UAV and then processed by the microcontroller before forwarding the required signals to the motor's electronic speed controllers.

UAVs are designed to replace humans in tasks that are considered too "dull, dirty, or

dangerous” [5]. As improvements in technology have made IC chips and other equipment smaller, UAVs have become more suited to nimbler and more precise tasks. Typically, UAVs are thought of as military technology but recently have started to have applications in civilian life as well. UAVs can be used for taking videos or photos, for remote sensing, or even for package delivery [6].

While each UAV design is different, each follow a similar pattern. The basic parts that every UAV must have to achieve flight are the microcontroller, the electronic speed controllers (ESCs) and the motors. Other equipments such as sensors, antennas and GPS can be included for additional functions. The microcontroller is the brains of the machine; it processes inputs and sends the appropriate signals as outputs to maintain and control flight. Brushless DC electric motors are typically used with UAVs as their power-to-weight ratio is complimentary to the weight requirements needed to achieve flight.

1.2 Problem Statement

In order to save lives and best respond to any emergency, it is imperative that communication be established between those affected by the emergency and the emergency responders. With the onset of wireless mobile phones, this has become much easier to accomplish since those affected by emergency situations are able to call emergency services without needing to find a fixed land-line. A problem still exists when the access points (cell towers or base stations) become damaged or destroyed during the emergency situations, causing communication to become impossible. When this happens, mobile phones become unable to send or receive calls, effectively isolating them from communicating with emergency responders.

One solution to this problem is to employ the use of a mobile base station. Mobile base stations act as a faux mobile cell tower that can route calls through a satellite link. Typical these mobile base stations are large antennas maneuvered by trucks that are driven to the affected area. Ground-based mobile base stations are limited to driving on roads and

are therefore inherently slow. In addition, emergency situations can damage roads making response times even slower. There is a need for a way to restore communication more quickly in order to minimize damage to life and property.

The main objectives of this thesis are to:

1. develop an adaptive connectivity algorithm for an UAV network.
2. analyze goodput and energy efficiency for an UAV network.
3. evaluate the effect of reuse distance and signal to interference plus noise ratio (SINR) on an UAV network.
4. investigate security concerns within an UAV network.

1.3 System Model

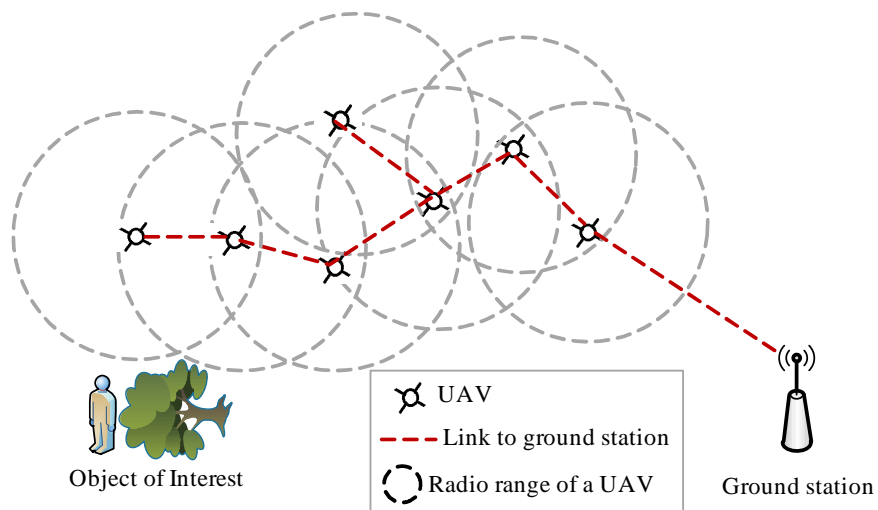


Figure 1.1: A sample network of 7 UAVs and a ground station where UAVs form a communication link between the target of interest and the ground station via single or multi-hop communication.

The use of an UAV ad hoc network to act as mobile base stations is proposed. Each UAV in the network would provide coverage for a certain area while also maintaining connection with the rest of the network (either through single or multi-hop communication). Depending on the size of the affected area and the number of users affected, a designated number of UAVs would be deployed to that area. The network will also need to form a connection to the nearest working mobile access point and begin routing calls through that point. The UAV network will continue operation until a more permanent solution can be put in place to restore communication to the affected area.

The design of the system would include deployment centers that act as warehouses. The deployment centers would house the UAVs until needed and deploy the appropriate number to the affected area. This number is determined based on the coverage area needed and the number of users affected. As the area and users increase, the number of UAVs needed would also increase proportionally. These warehouses also serve as recharge, repair, and upgrade shops for the UAVs. Battery life is a problem associated with UAV longevity. Batteries are inherently transient and therefore will need to be replaced or recharged after a certain amount of time in operation. One solution to this problem is to cycle out UAVs as their batteries run low. The UAVs are able to fly back to the deployment center and swap batteries before returning to the designated area to continue operation. Since the UAVs are assumed to be deployed at the same time, a way to cycle out the UAVs effectively would need to be determined in order to prevent all of the UAVs from leaving the area at the same time.

1.4 Thesis Outline

Chapter 2 develops an adaptive connectivity algorithm that prevents collisions within the network while maintaining connectivity through the use of dynamic power scaling and is based on "Enhancing Connectivity for Communication and Control in Unmanned Aerial

Vehicle Ad hoc Networks”[1] that was presented in IEEE Radio and Wireless Week (IEEE RWW) 2015.

Chapter 3 presents a performance analysis on the goodput and energy efficiency within an UAV ad hoc network. This chapter is based off of ”Performance Evaluation of Unmanned Aerial Vehicle Ad hoc Network”[2] that was presented in IEEE Southeastcon 2015.

Chapter 4 discusses and analyses the effects of signal to interference plus noise ratio (SINR) and reuse distance on channel capacity. This work is based off of ”UAV-assisted Broadband Network for Emergency Response Communication” [3] that was presented in IEEE Global Conference on Signal and Information Processing (IEEE GlobalSIP) 2015.

Chapter 5 lists and considers the constraints of an UAV network. The available ad hoc communication protocols for UAV networks as well as security issues are also presented.

Chapter 6 concludes the thesis by presenting an overview of results shown in each chapter as well as discussing the impact of each. Future works are suggested for continued research on this topic.

CHAPTER 2

ENHANCING CONNECTIVITY FOR COMMUNICATION AND CONTROL IN UNMANNED AERIAL VEHICLE NETWORKS

UAVs working autonomously must be able to sense their surroundings and prevent collisions with other UAVs in the network as well as other objects. At the same time, the connection to the network must be maintained to allow for continual flow of data between nodes. The research presented describes an adaptive connectivity algorithm for use in autonomous UAV ad hoc networks. The purpose of this algorithm is to prevent collisions between UAVs while also preventing an interruption in connection caused by the dynamic movement of each node. The work in this chapter is based off of the published paper "Enhancing Connectivity for Communication and Control in Unmanned Aerial Vehicle Ad hoc Networks"[1] that was presented in IEEE Radio and Wireless Week (IEEE RWW) 2015 and portions of material have been copied verbatim.

2.1 Introduction

UAV networks are not only envisioned for military applications to provide battlefield assistance, target detection, tracking and sensing target areas, but also are considered for civilian applications for monitoring areas that are not easily accessible (such as in disaster situations). Performance of UAV networks depend on connectivity among UAVs and connectivity between UAV and ground stations since reliable connectivity for single hop or multi-hop communication is very important to forward time-critical information.

Recent related works concerning the network connectivity in UAV networks include [7, 8, 9, 10, 11, 12]. The work in [7] has considered connectivity based mobility using heuristic approach for next direction for a given UAV. The authors in [8] have analyzed the performance of UAV communication networks with directional antennas to maximize the throughput and minimize the end-to-end delay. Similarly, Teacy, *et al.* in [9] have

integrated an on-line learning procedure and flight path within the network to adapt to the radio propagation characteristics of an UAV network. Han *et al.* in [10] have proposed an approach to improve connectivity using location and movement of UAVs. The authors in [11] have presented network connectivity in UAV and ground mobile ad hoc networks. The UAV fleet area coverage with network connectivity constraints has been presented in [12].

Note that the connectivity in UAV networks is directly related to the density of UAVs, velocity of UAVs, angle of arrival, and transmission range/power used by UAVs and *none* of these existing works in the literature consider the joint effect of these essential parameters in UAV networks.

The goal in this setup is to enhance the connectivity in UAV mobile ad hoc networks where the transmission range/power of each UAV is adapted based on its local information (density of UAVs, relative velocity of the UAVs, transmission range/power, and angle of arrival).

The remainder of the chapter is organized as follows: A system model is presented in Section 2.2 followed by the connectivity analysis in Section 2.3. The algorithm is presented in Section 2.4 followed by the simulation results in Section 2.5. Finally, the chapter is concluded in Section 2.6.

2.2 System Model

In this section, consider a network of UAVs equipped with cameras/sensors for sensing, GPS unit, and with wireless devices (a transceiver with omnidirectional antenna) for networking and transferring information to another UAV or a ground station using single-hop or multi-hop communication as shown in Fig. 1.1. The aim of this network is to sense for monitoring certain area to provide an overall image where the sensing area is likely not known a priori (i.e., changes dynamically). In this setup, our main goal is to investigate the network connectivity based on the density of UAVs, relative velocity of the UAVs, transmission

range/power, and angle of arrival.

2.3 Adaptive Connectivity Analysis

In an UAV network, once two UAVs are within the communication range, whether or not they are reachable after certain time t can be checked by using their velocities, their accelerations and the time interval. For a given UAV with its initial velocity $\vec{v}(0)$, the instantaneous velocity $\vec{v}(t)$ at time t is defined as

$$\vec{v}(t) = \vec{v}(0) + \int_0^t a(y)dy \quad (2.1)$$

where $a(y)$ is the acceleration of a UAV at time y . Using (2.1), the distance traveled by a UAV for an interval $[0, t]$ is

$$D(t) = \int_0^t \vec{v}(y)dy \quad (2.2)$$

Thus, using (2.2) for a time interval $[0, t]$, the distances traveled by any UAV can be calculated. Consider i and j UAVs calculate $D_i(t)$ and $D_j(t)$ using (2.1). Then the distance between the UAVs i and j for the interval $[0, t]$, where UAV i is following j and initial separation distance was z , is given by

$$D_e = I(i, j)[D_i(t) - D_j(t)] + z, \quad I(i, j) \in \{1, -1\} \quad (2.3)$$

where if $D_i(t) > D_j(t)$, $I(i, j) = -1$, otherwise $I(i, j) = 1$. Note that the distance traveled by the ground/base station $D(t) = 0$ as it is fixed. After time t , UAVs to be able to reach wirelessly and UAVs not to crash with others, the following condition (for both longitude and latitude) should be satisfied

$$S_d \leq D_e \leq \min\{R(n)\}_{\forall n} \leq \bar{R} \quad (2.4)$$

where S_d is the safety separation distance between UAVs. The transmission range R can be computed as [13]

$$R = \sqrt{\frac{P_t G}{P_r}} \frac{c}{4\pi f} \quad (2.5)$$

where P_t is transmit power, G is an effective gain, P_r is received power, $c = 3 \times 10^8 \text{ m/s}$ is velocity of light, and f is frequency used to communicate. Maximum allowed transmission power (i.e., $P_t = P_{max}$) for a given band f can be used to calculate the maximum transmission range \bar{R} . If $S_d \leq D_e$ in (2.4) is not satisfied, UAVs must repel each other, otherwise they are close enough to crash into each other. If $D_e \leq \min\{R(n)\}_{\forall n} \leq \bar{R}$ is not satisfied, UAVs would not be able to communicate with each other using single-hop communication. In both cases, UAVs change their directions and/or speeds to avoid a collision and maintain a communication link with each other. In this case, UAV n computes resultant vector by adding a unit vector in direction $\theta_n(t)$ to unit vector $\frac{\vec{v}_n(t)}{\|\vec{v}_n(t)\|}$ and the angle of the resultant vector is the new direction of a given UAV n , $\theta_n(t+1)$ based on the angle of arrival. Each UAV determines the new direction based on current position of the UAV and angle of arrival from other UAVs. The angle of arrival can be computed with the help of Fig. 2.1. The dashed parallel lines represents isoplanes for two UAVs, and θ_1 is the angle for UAV 1 in Fig. 2.1. The distance $d_{T,1}$ can be expressed as

$$d_{T,1} = d_1 \cos \theta_1 \quad (2.6)$$

This distance can be expressed as the distance that light travels in τ seconds as

$$d_{T,1} = c\tau \quad (2.7)$$

Note that the propagation delay τ for a signal between source and destination can be expressed as $\tau = \frac{m}{f_s}$, where m is the delay in samples and f_s is the sample frequency. Then

the angle of arrival θ_1 with respect to perpendicular distance of isoplanes is given by

$$\theta_1 = \cos^{-1} \left[\frac{cm}{d_1 f_s} \right] \quad (2.8)$$

The given UAV can repeat this process for angle of arrivals for other UAVs and find θ_n , for $n = 1, 2, 3, \dots$. As mentioned, each UAV knows its current direction (e.g., from an on-board GPS module) and thus once the given UAV has information about angle of arrival and direction of other UAVs, it can choose the safe direction to avoid any collision.

UAVs communicate with each other using common control channels and thus each UAV can estimate *actual* number of UAVs (N_e) that are communicating with the given UAV currently. The *total* number of UAVs that can be present around a given UAV for a given maximum transmission range \bar{R} and number possible parallel paths P_p in space can be computed as $N_t = \frac{\bar{R}P_p}{S_d}$. Thus, an UAV could estimate a normalized UAV density as

$$K = \frac{N_e}{N_t} \quad (2.9)$$

Then, based on the estimated normalized UAV density, each UAV can adapt its transmission range as [14]

$$R = \min \left\{ \bar{R}(1 - K), \sqrt{\frac{\bar{R} \ln(\bar{R})}{K}} + \alpha \bar{R} \right\} \quad (2.10)$$

where $0 < \alpha < 1$ is a constant. For instance, when a given UAV has no neighbors (i.e., $K = 0$), it adapts its transmit range to the maximum allowed range using (2.10). Once the transmission range is estimated by a given UAV, it is mapped with a suitable transmit power using signal propagation model (2.5). Note that the successful probability (P_s) for connectivity can be obtained by taking a ratio of number of UAVs who satisfy (2.4) to total number of UAVs.

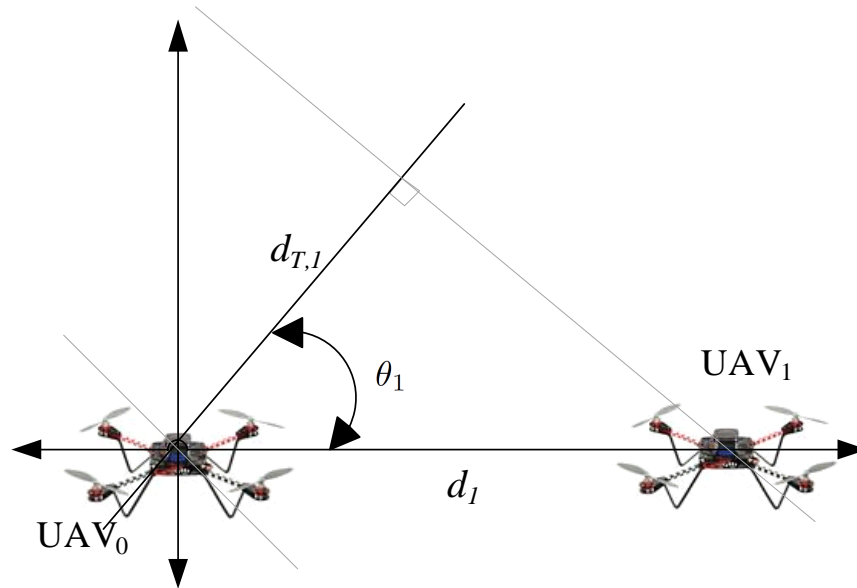


Figure 2.1: Angle of Arrival Calculation for two UAVs.

2.4 The Algorithm

Based on the analysis presented, a formal algorithm is presented as **Algorithm 1**.

2.5 Numerical Results and Discussion

In order to illustrate the performance of the proposed approach, an UAV mobile network of $N = 10$ UAVs was simulated where each UAV is assumed to be configured with a fixed transmission range of 200 meters (scenario S1) and with an adapted transmission range ≤ 1000 meters (scenario S2). Initial speed of the UAV was 3 m/s. The variation of successful probability vs. the simulation time was plotted for both scenarios S1 and S2 as shown in Fig. 2.2 (a). It was noted that the successful probability dropped suddenly below 20% in scenario S1 where transmission range was fixed to 200 meters. This happens because UAVs fly around and they may not have sufficient transmission range/power to communicate with other UAVs while avoiding collision with others. Whereas the successful probability has never dropped below 80% in scenario S2 where variable transmission range/power is

Algorithm 1 Adaptive Connectivity for UAVs

- 1: **Input:** initial velocities $\vec{v}_n(0)$, maximum allowed transmit power P_{max} , current direction $\theta_n(t)$, and safety distance S_d .
 - 2: **Output:** Adapted transmission range in (2.10), new direction of UAV n : $\theta_n(t + 1)$, and the probability of successful connectivity.
 - 3: Initialize a counter: $counter = 0$;
 - 4: **for** each sensing time interval, t **do**
 - 5: **for** each UAV n **do**
 - 6: **if** UAV n is connected to base station (BS) by single-hop (i.e., condition (2.4) is satisfied) **then**
 - 7: Estimate the new location after time t based on the current velocity and transmit range.
 - 8: **if** UAV n will still be connected to BS based on estimated location in step 7, then continue with the current settings for UAV n . Increment the counter by 1.
 - 9: **otherwise** Adapt the transmission range using (2.10) and change the direction of a given UAV n towards BS with the help of angle of arrival, and GOTO Step 6. **end if.**
 - 10: **else if** UAV n is not connected to BS **then**
 - 11: Check if it has neighboring UAVs. If not, adapt transmission range using (2.10) and check if it can reach other UAVs. If yes, continue with existing settings and increment the counter by 1.
 - 12: Check if at least one neighbor exists, estimate location and check if it is reachable after t time. If not, change the direction and transmit range, and GOTO step 10. **end if.**
 - 13: **end for**
 - 14: Successful probability $P_s = \frac{counter}{N}$;
 - 15: **end for**
-

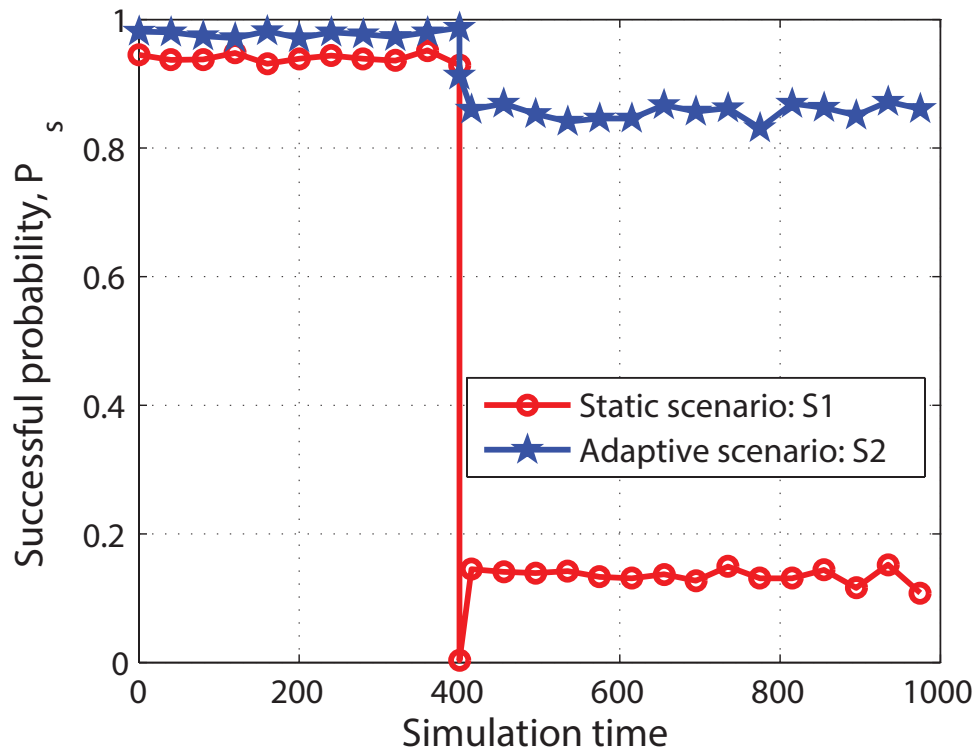


Figure 2.2: The change in probability of successful connectivity after a given time. At time = 400, a UAV moves in such a way that it is no longer within communication range of the rest of the network. The adaptive connectivity algorithm is able to increase transmission power in order to minimize loss of connectivity. The static scenario is unable to adapt and therefore has a much lower probability of connectivity when such an event occurs.

used by each UAV. It is worth noting that when direction and transmission range is adjusted based on the interaction with other UAVs, each UAV was able to adapt its direction and transmission range to reach other UAVs.

The variation of connectivity with respect to the number of UAVs for a given area was then plotted. As expected, connectivity increased with the number of UAVs in both static and adaptive scenarios but the proposed adaptive approach outperforms the static one as in Fig. 2.2 (b).

2.6 Chapter Summary

This chapter has presented an analysis for enhancing connectivity in UAV networks using density, angle of arrival, velocity, and transmission range/power used by UAVs. The performance of the proposed approach has been evaluated using numerical results obtained from simulations. The results have shown that the connectivity for UAV network is improved significantly when the proposed adaptive approach is used.

CHAPTER 3

PERFORMANCE EVALUATION OF UNMANNED AERIAL VEHICLE AD HOC NETWORKS

Within an UAV ad hoc network, performance metrics must be known. The research presented in this chapter shows the results of increasing the number of UAVs in the network and their effect on the total transmission range of the network and the worst case propagation delay. The effect of available transmission time on goodput per unit energy (energy efficiency) and datarate are also compared. This work is based off of the published paper "Performance Evaluation of Unmanned Aerial Vehicle Ad hoc Network"[2] that was presented in IEEE Southeastcon 2015 and portions of material have been copied verbatim.

3.1 Introduction

UAVs are emerging for different applications in many fields [15, 16, 17, 5]. In addition, these technologies can be implemented with different technologies to enhance their capabilities [14, 18, 19, 20, 21, 22, 23, 24, 25, 26]. and UAVs can be used for everything from reconnaissance in military uses to photography in the civilian world. These UAVs are equipped with a microcontroller for processing inputs and can be externally controlled via remote control if desired. UAVs can also be equipped with wireless transceivers to allow for communication with other UAVs or with units on the ground. If multiple UAVs are communicating with each other, they can form an ad hoc network. An ad hoc network allows for data to be collected at one node within the network and sent to any other node within the network [27, 28]. Data is routed through the network and the path taken depends on the routing protocol used. In [29] the pros and cons of different routing protocols are discussed; they consider two kinds of routing protocols: proactive and reactive. Proactive routing protocols require that each UAV within the network knows the shortest path to any other UAV within the network. This data is stored into a table and is updated frequently. By having

to update shortest paths within a network periodically, proactive routing protocols require a large amount of protocol overhead. This means that a large amount of data is needed to be sent by the network regularly to maintain connectivity, thus reducing the amount of available bandwidth within the network. Reactive protocols only require that paths be found when data needs to be sent which means that there is minimized protocol overhead. While reactive protocols do require a large amount of protocol overhead, knowing paths ahead of time allows for a low end-to-end delay time for sending data. Reactive routing protocols do not have this advantage. When choosing a routing protocol, a tradeoff must be made between delay time and available bandwidth.

In an UAV network all nodes are connected to a ground station via single or multi-hop communication. The goal of this network is to relay information from mobile UAV nodes back to the stationary ground node. This type of technology can be used in disaster situations where continuous updates are needed but rescue workers cannot reach the target area in a timely manner (due to debris or other obstacles). UAVs would be able to fly over the target area and relay information (pictures, videos, etc.) back to the rescue workers to keep them updated. For an UAV network to be useful in the described situation, it must maintain both connection and throughput between individual UAVs within the network.

A typical ad hoc routing protocol works well for 2-dimensional stationary networks. A new routing protocol was proposed in [30] that would work well in a 3-dimensional heterogeneous network where communication is needed between highly mobile aerial and ground nodes. The authors consider hierarchical clustering where similar nodes are grouped into clusters. These clusters are then grouped into levels. Within these levels, a cluster head is appointed to facilitate communication between levels. This organization of the network allows for reduced bandwidth as only the cluster heads need to worry about communicating with other clusters.

Besides for routing, throughput is also extremely important in UAV networks. The

authors of [31] examine the effects of lossy links on throughput and energy consumption within a network. The paper mentions that lossy links can have a huge impact on throughput — in some cases reducing network throughput by up to half. The effects of lossy links on energy consumption was seen as less significant as compared to throughput. In [32], a Load-Carry-and-Deliver (LCAD) model is created for use in UAV networks where delay-tolerant bulk data needs to be sent. An analysis is done to show how the LCAD model performs as compared to multi-hop transfer of data. An in-depth throughput analysis for 802.11 multi-hop networks with regards to hidden nodes is done in [33]. Optimum node density is analyzed in [34] for mobile ad hoc networks relating to transmission power. It was seen that there is no optimal node density for ad hoc networks. Instead, it was noted that as node mobility increases, the number of nodes should also increase to achieve the highest throughput.

The goal of this chapter is to analyze the effect of network size on throughput, energy consumption and transmission range. While throughput and energy consumption have been studied in the referenced papers, none of them have taken into account how the size of the network would affect the various parameters. Simulations are done to show a graphical representation of the results.

The remainder of the chapter is organized as follows: A system model is presented in Section 3.2 which describes what our analysis will be based off of. Section 3.3 consists of a performance analysis. Simulation results are shown in Section 3.4 and we conclude the paper in Section 3.5.

3.2 System Model and Problem Formulation

In this section, a network is considered consisting of UAVs equipped with cameras/sensors for sensing, GPS unit, and with a wireless device (a transceiver with omnidirectional antenna) for networking and transferring information to another UAV or a ground station

using single-hop or multi-hop communication as shown in Fig. 1.1. We have considered a disaster situation where rescue workers are not able to reach a target area in a timely manner. This network of UAVs is able to configure itself in such a way that it creates a temporary link between a ground station and the target area. This temporary link provides a crucial data link to rescue workers as they approach the target area.

In this section, using this system model, the goal is to look into how throughput is affected by network size, energy consumption and transmission range.

3.3 Performance Analysis

If goodput is considered to be the total amount of useful data transmitted from one node to another over a certain period of time, the goodput can be calculated using the following equation:

$$G = \frac{(d - h) \times N_p}{T} (1 - p_f) \quad [bps] \quad (3.1)$$

This equation takes the useful information (d data bits) and subtract out the h header bits. This is then multiplied by N_p number of packets and divided by the total transmission time T . Consider P_f to be the probability of failure. The goodput differs from the throughput as throughput considers all data, not just the useful information. Goodput is a better measurement as it does not consider the network overhead. For UAV ad hoc networks, the data being transmitted by the network is broken into two sections; the data being sent between UAVs for network control and coordination, and the data being sent and received from the intended users.

Eq.(3.1) shows the total network goodput. If goodput per UAV is required then it is needed that all of the UAVs in the network are taken into account. In this type of network, all users are considered to be equal and share bandwidth evenly. Eq.(3.2) shows the goodput per UAV by dividing the total network goodput by the number of UAVs. N_{uav} represents

the number of UAVs using the same channel within the network.

$$G_p = \frac{G}{N_{uav}} \quad [bps] \quad (3.2)$$

Each UAV in the network will need to use a certain amount of energy to achieve the specified goodput. That energy is represented as E . An equation can be created to represent the amount of goodput achievable per unit energy by dividing goodput per UAV, G_p , by the needed energy E .

$$G_e = \frac{G_p}{E} \quad [bps/J] \quad (3.3)$$

Looking back to the example of using an UAV network in a disaster situation, it is important to know the maximum possible transmission range for the network. This is achievable when each UAV is put into a straight line. Each individual UAV in the network will have a max transmission range. That transmission range might vary from UAV to UAV. The transmission range between any two UAVs needs to be the smaller transmission range achievable between those two UAVs. From Fig.3.1, it can be seen that there are three UAVs in the network. To get the transmission range of the network, the transmission range of UAV 1, T_1 , must be added to the smaller of the two transmission ranges between UAV 1 and UAV 2. That sum is then added to the smaller of the two transmission ranges between UAV 2 and UAV 3 and then added the transmission range of UAV 3. This total sum gives us the total network transmission range, which we will define as T_r . Eq.(3.4) shows how this can be defined mathematically. The first and last transmission ranges, T_1 and T_n respectively, must be added to the sum of all the intermediate transmission ranges, A_i . The equation for A_i can be seen in (3.5) and will sum for all UAVs in the network, N_{UAV} .

$$T_r = T_1 + T_n + \sum_{i=1}^{N_{UAV}} A_i \quad (3.4)$$

where the value of A_i is computed as

$$A_i = \min\{T_i, T_{i+1}\} \quad (3.5)$$

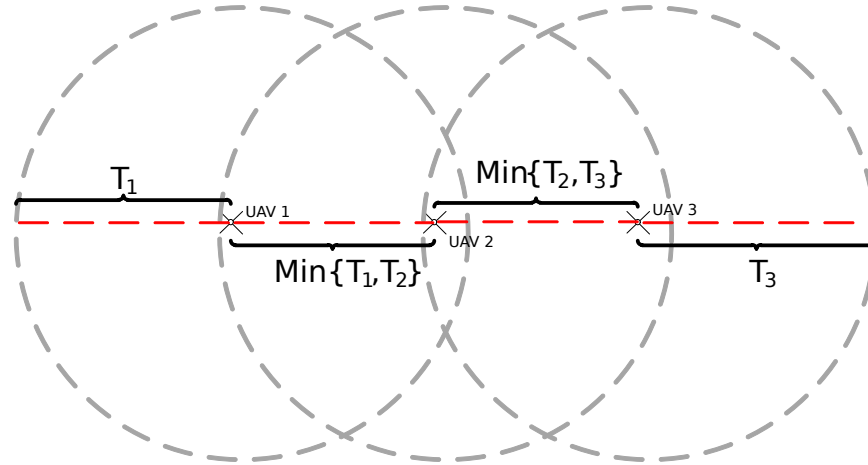


Figure 3.1: A network of 3 UAVs showing transmission range and distance between UAVs where distance between UAVs can be computed using GPS locations. Note that the distance between them depends on relative velocity and direction of travel.

3.4 Performance Evaluation and Numerical Results

Using eq.(3.1), a one megabit data packet being sent over various time periods is simulated. Time periods ranging from one second to sixty seconds at one second intervals is used. Fig. 3.2 shows the needed data rate to send that one megabit data packet over the specified time period. From the graph, it can be seen that as the amount of available time increases, the needed datarate decreases.

Using eq.(4.3) the maximum network transmission range versus the number of UAVs in the network is simulated. This simulation considers that the UAVs are all at the same altitude and that the maximum transmission range between any two UAVs is the shortest Fig. 3.3 shows max network transmission range as a function of the number of UAVs in the network. The furthest possible transmission range is considered by simulating the UAVs in a straight line at maximum range from each other. The result is a linear graph showing that as the number of UAVs in the network increases, the maximum possible transmission range increases as well.

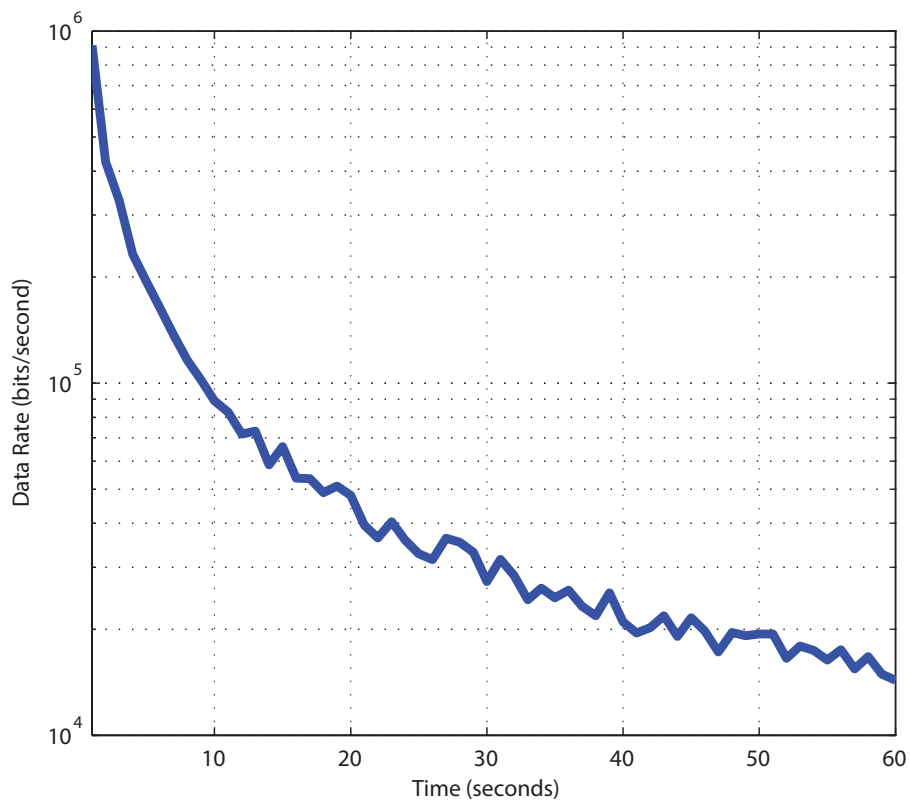


Figure 3.2: Datarate needed to transmit a given amount of data vs. the total available transmission time.

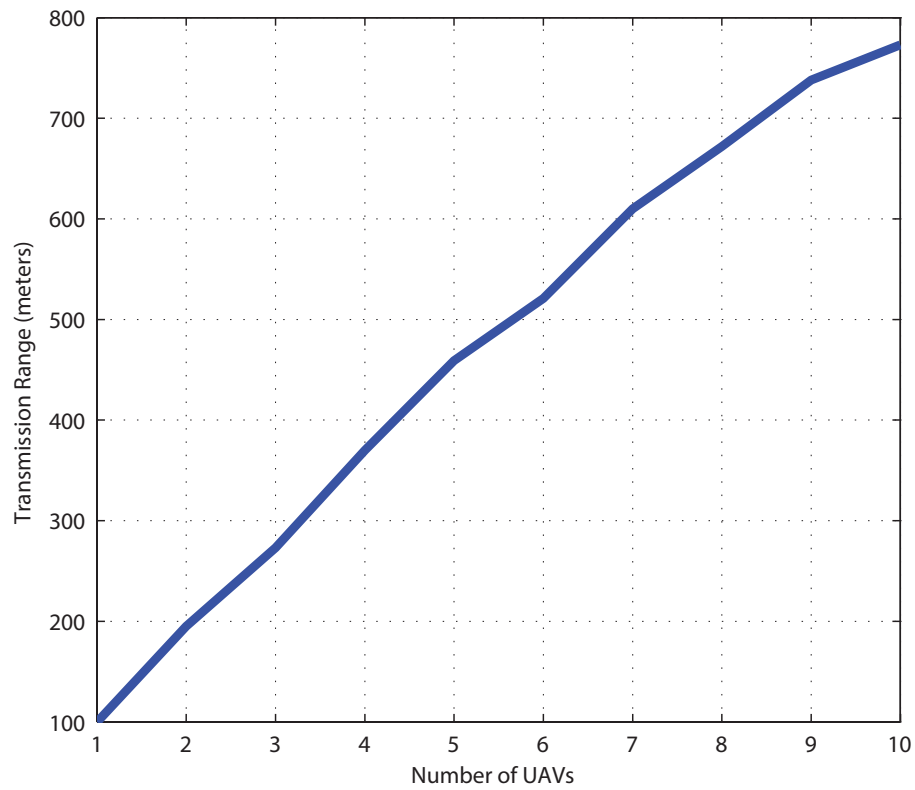


Figure 3.3: Total transmission range of the network vs. the number of UAVs in the network.

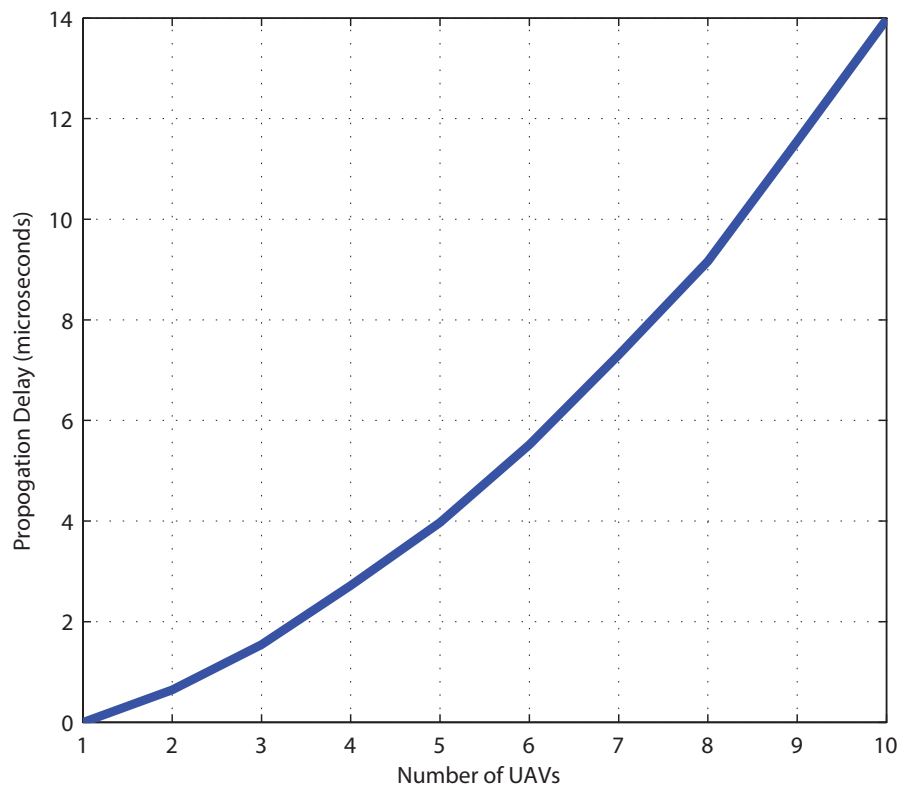


Figure 3.4: Worst case propagation delay of the network vs. the number of UAVs in the network.

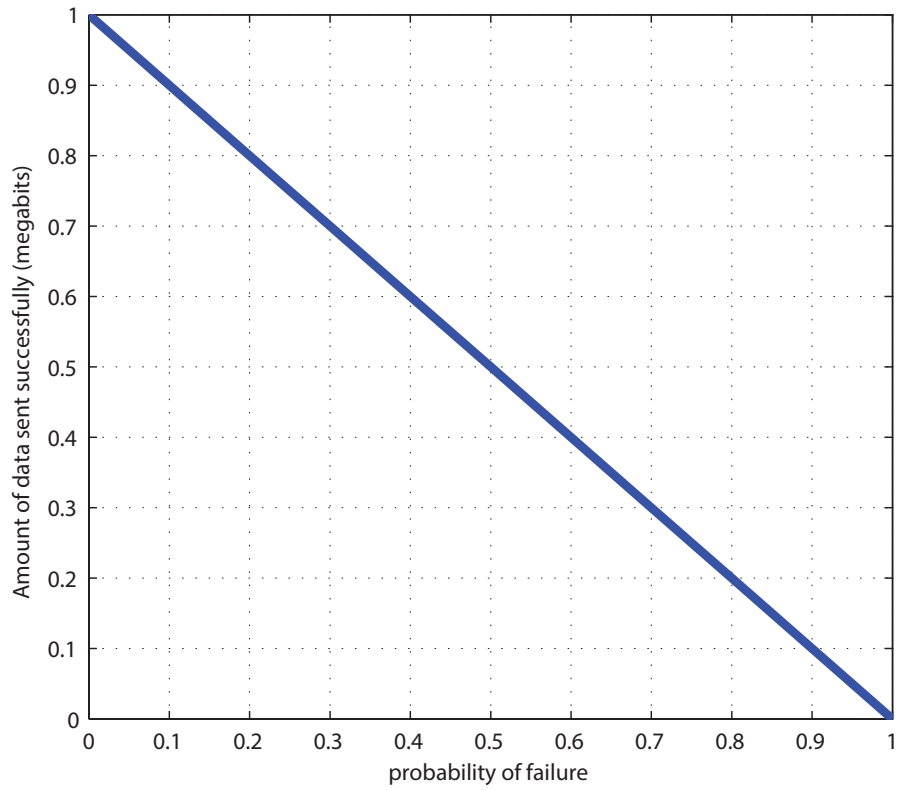


Figure 3.5: Amount of data sent successfully (goodput) vs. the probability of a packet failing to reach the destination.

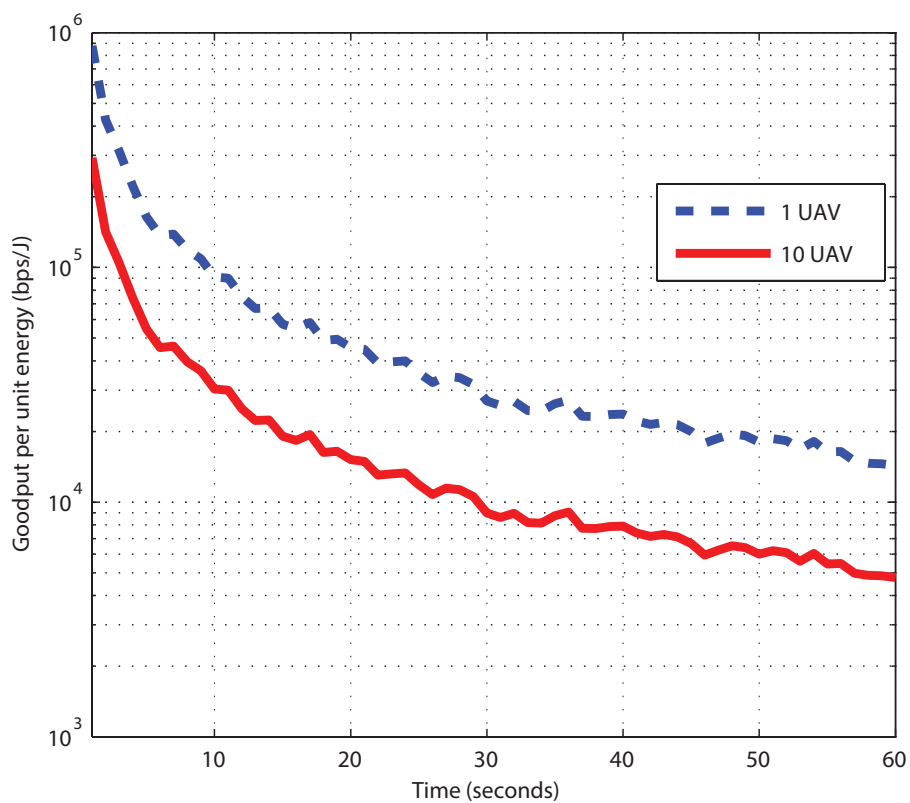


Figure 3.6: Goodput per unit energy vs. the number of UAVs in the network.

Considering the same model as the transmission range graph, the effect on propagation delay is plotted. Fig. 3.4 plots propagation delay as a function of the number of UAVs in the network. As the number of UAVs in the network increases, the propagation delay increases exponentially since each new UAV adds a new point of possible failure.

As mentioned, as more UAVs enter the network, there are more points of possible failure. Fig. 3.5 shows a one megabit packet being sent through a UAV network with varying probabilities of failure. Adding additional UAVs to the network increases the amount of possible points of failure. This probability of failure can range anywhere from 0% to 100%. It can be seen that at 100% probability of failure, no data is transmitted and at 0% probability of failure, all of the data is transmitted.

This chapter has shown the relationship between network size, transmission range and propagation delay. Each UAV in the network will require a certain amount of energy to send data. By summing the energy used by each UAV the total energy consumption of the network can be known. The affect of increasing the number of UAVs in the network on energy efficiency is also of interest.

Fig. 3.6 shows the effect of an increased transmission time on goodput per unit energy. It can be seen that as the number of available transmission time in the network increases, the goodput per unit energy decreases exponentially. This is to be expected since as the transmission time available in the network increases, the total available data being sent per unit time decreases. This means that the amount of energy needed per unit time will also decrease. Two scenarios were presented on the graph; one scenario is analysis of a single UAV in the network while the second scenario is of 10 UAVs in the network. Increasing the number of UAVs decreases the available bandwidth for each UAV (shared bandwidth). This means that less data will be sent per unit time resulting in less energy spent per unit time.

3.5 Chapter Summary

An analysis for throughput of UAV ad hoc networks with regards to network size has been performed. Numerical results obtained from simulations have shown that the performance of the network depends on the number of UAVs in the networks, the transmission range of UAVs and their energy consumptions. It has been shown that as the amount of available transmission time increases, the amount of data rate needed to send a specified amount of data decreases exponentially. With the knowledge of the needed data rate for a specified time and data size, transmission range and propagation delay were then investigated. It is shown that as the number of UAVs in the network increases, the total transmission range increases but so does the propagation delay. Different probabilities of failure are then considered. It was shown that probability of failure has a linear correlation with the amount of data received. The last simulation shows the goodput over time of the network per unit energy for each UAV in the network. If the number of UAVs in the network increases, the amount of throughput available to each UAV decreases, which in turn decreases goodput per unit energy for each UAV. From Fig.3.6 it can be seen that the goodput per unit energy for 10 UAVs in the network is lower than when only one UAV is in the network.

The simulations performed in this chapter can be used to analyze and to add a more detailed explanation of what factors most affect a UAV network. Future research includes showing the effect of different routing protocols (proactive vs reactive) on the throughput along with the number of UAVs and transmission ranges of UAVs.

CHAPTER 4

UAV-ASSISTED BROADBAND NETWORK FOR EMERGENCY AND PUBLIC SAFETY COMMUNICATIONS

The work in this chapter is based off of "UAV-assisted Broadband Network for Emergency and Public Safety Communications" [3] that was presented in IEEE Global Conference on Signal and Information Processing (IEEE GlobalSIP) 2015 and portions of material have been copied verbatim.

Communication during emergency situations is crucial to saving lives. Rescue workers at an emergency scene need to be able to coordinate and communicate effectively. Despite the vast improvements in personal communication networks, public safety communication has been lacking. A recent bill from Congress and the FCC has provided the groundwork for the creation of a nationwide broadband public safety communication network. This advancement in technology will allow rescue workers to receive critical information updates in all forms of media (e.g., video, text and voice). A problem arises when a communication tower is destroyed; this network will no longer function for that area. A solution must be created to temporarily cover the partially or completely destroyed network's or tower's assigned area to restore their connectivity and to connect them to the global network. In this chapter, an UAV network that can be used to route broadband data similar to a communication tower for when the main network is unusable is designed. Using a global geolocation map, the optimal/sufficient number of UAVs can be sent out quickly to the geolocation of a destroyed tower and route traffic accordingly. UAVs also have the advantage of being airborne, allowing for better line of sight with ground users. Simulation results show that the proposed design has better performance in terms of channel capacity and throughput when signal strength is lower.

4.1 Introduction

Public safety communication (PSC) is extremely vital during emergency situations [35, 36]. When a disaster occurs, it is important that first responders are able to communicate and coordinate to prevent loss of life and confusion at the scene. An increase in the advancement for personal communication technology such as 3G and LTE has been seen but unfortunately, this same technology has not been implemented for PSC. Adding to this, most PSC departments (Fire and Rescue, Emergency Medical Services, Police) communicate using their own separate networks. Even within these separate networks, interference can cause communication problems. These various problems have led to the FCC and Congress passing the Spectrum Act which aims to build a unified broadband communication network specifically for use by public safety operators [4, 37, 38]. The Spectrum Act assigns the 700MHz frequency band for use by public safety operators as well as creating the First Responder Network Authority (FirstNet). FirstNet is in charge of overseeing the creation of the nationwide public safety broadband communication network. This new broadband network should allow for better coordination between different public safety departments as well as allow for voice, video, pictures, and other data to be sent and received. The ability to send other forms of data (other than voice) allows for rescue workers to be better prepared when they arrive at an emergency scene. Things such as floor plans, civilian information and other data can be known beforehand.

The most likely configuration of the infrastructure of this network will consist of communication towers strategically placed throughout the nation to allow for total coverage. The problem with this type of statically placed network is that if a tower is destroyed or otherwise made unusable, how do you recover quickly? Constant coverage and communication is vital for public safety and cannot afford downtime. One approach to solve this problem would be to implement cognitive radio with software defined radio [21, 39, 40, 41, 42, 43]. Cognitive radio allows devices to sense the frequency bands and determine if they are

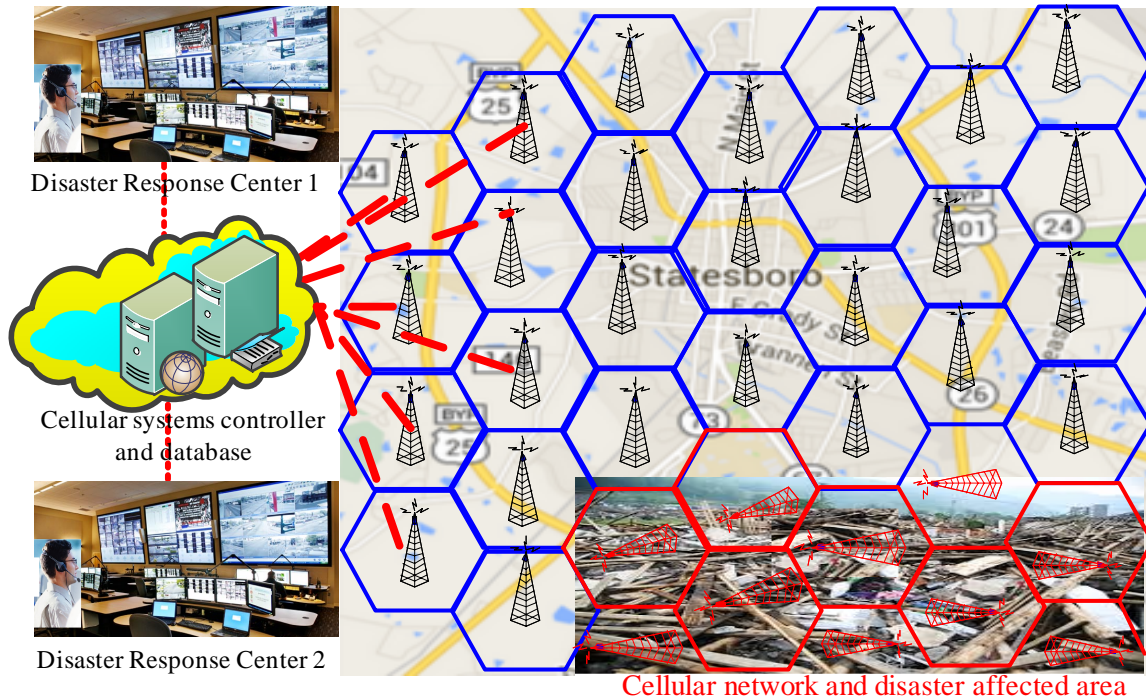


Figure 4.1: Typical scenario of cellular network with controller, disaster response center and disaster affected area.

being used or interfered with. If the standard communication frequency is being blocked, cognitive radio allows the device to scan for another suitable frequency. When a suitable frequency is found, it can communicate on that frequency. Another proposed solution is to form wireless mesh networks with devices in the affected area [44, 45]. Smaller mesh networks between first responders can be formed allowing direct communication between them. This network can also relay information to a bigger area mesh network consisting of different PSC departments. This bigger area mesh network be used to monitor each department and make actions accordingly. All of these approaches assume that every first responder in the area will be deployed with their technology. If any of the PSC or departments do not have the technology, their solution will not work. Instead of focusing on the users of the network, this chapter will focus on quickly and efficiently repairing the network which is not considered in the existing works. In this chapter, the goal is to design a disaster

response communication network to reconnect (completely or partially) destroyed areas to the backbone communication networks using UAVs equipped with both cognitive radio and base station like capabilities with heterogeneous broadband networking features.

The remainder of this chapter is organized as follows: Section 4.2 describes the system model and problem statement where a solution for how to quickly provide communication when a tower is destroyed is proposed. Section 4.3 presents analysis followed by simulation results in Section 4.4. Section 4.5 concludes the chapter.

4.2 System Model

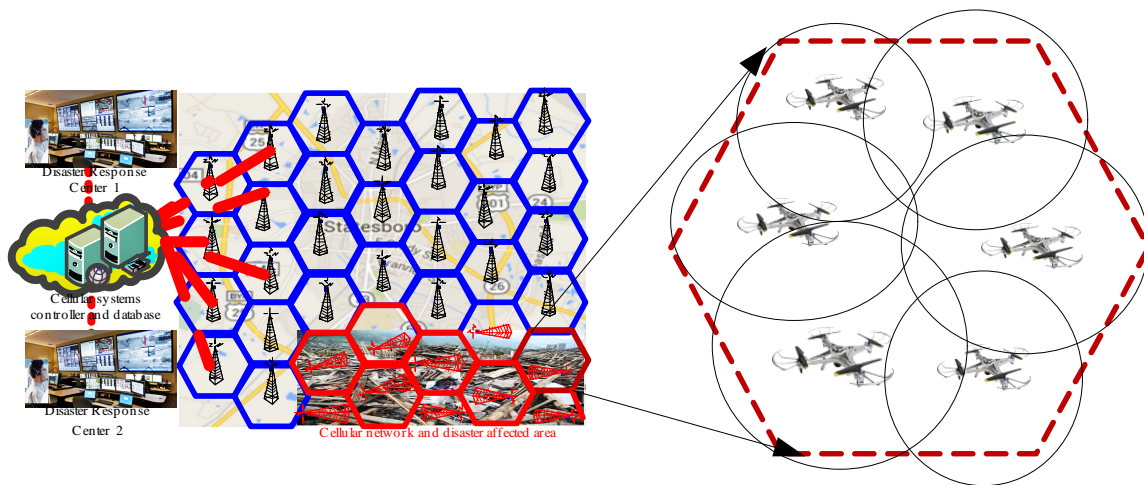


Figure 4.2: Destroyed communication tower being covered by a network of 5 UAVs where these UAVs communicate with each other and nearby towers to be able to restore communication to the affected area.

A disaster situation where multiple public safety departments have been called to the area is considered. Rescue workers need to be able to communicate with workers in their department as well as with other departments. The use of the broadband network described in the introduction would allow for this. With the infrastructure for this network in place, two different problems are considered that could arise at the rescue area. The first

problem that could happen is that the infrastructure could be destroyed during the disaster and make communication on the network unavailable. The rescue workers in the field would be unable to communicate with each other and with other departments. This loss of communication can lead to inefficiency and loss of life. The second problem is that outside interference could make communication on the standard frequency unavailable. Again, communication is being blocked but this time the network is still available but unreachable due to interference. In both problems, communication through the broadband network is not possible due to outside influence. A solution to both of these problems is needed.

Adding multiple database centers to the infrastructure of the new public safety broadband network is proposed. Each database center would be responsible for a certain area around itself and monitoring the status of communication towers within that area. These database centers should be strategically placed to allow for efficient coverage of a large area. Communication towers should have the ability to scan the communication frequency and determine if interference is present. If interference is present, a signal should be sent back to the database requesting UAV support. Along these same lines, the communication towers should also periodically send a heartbeat packet to the database centers. The heartbeat packet would mean that the tower is operating correctly. If the heartbeat packets fails to be sent within a certain threshold time, the tower will be considered destroyed and will result in UAVs being sent to the tower. In both scenarios, UAVs are sent to the area to support the tower. In the case of interference, the UAVs should be able to communicate using a different frequency to allow traffic to be routed to the nearest working tower. For both scenarios, the number of UAVs depends on the coverage area of both the individual UAVs and the unusable communication tower. The number of UAVs needed to fill the coverage area of the tower is known as a packing problem [46]. Optimization must be done to determine how to efficiently place the UAVs with minimal overlap while still filling the desired area. To avoid inter-cell interference [47], UAVs choose their frequency based on

the index $F = [(i + 1)x + y] \bmod C_s$ for a given center cell's location (x, y) where cluster size $C_s = i^2 + i + 1$.

In this chapter, the goal is to cast a problem to design a UAV network to reconnect completely or partially destroyed communication networks where UAVs are equipped with both cognitive radio capability and base station with heterogeneous networking features.

4.3 Analysis

Several factors need to be considered to optimize this solution including response time, propagation delay and channel capacity. Each database center will have knowledge of the location of each tower within range as well as the status. From this location, the distance to each tower can also be found. If the distance to a tower, D is known and the velocity of a UAV, V , is also known the total flight time to a location can be found. This flight time is crucial to determine if a UAV should be sent from one disaster response center or from another center.

$$T_{Flight} = \frac{D}{V} \quad (4.1)$$

The flight time from a database center to a destroyed tower was shown in eq. (4.1). This can be added together with the activation time of the UAV and the setup time to determine the total response time.

$$T_{Response} = T_{Activation} + T_{Flight} + T_{Sensing} + T_{Setup} \quad (4.2)$$

The time it takes for the database to acknowledge that a tower is offline as well as the time it takes for the UAV to turn on is represented by $T_{Activation}$. It is shown in eq. (4.1) that T_{Flight} is the flight time to the location. Once the UAV reaches the target location, the time it takes for the UAV network to tune to right frequency using cognitive radio is $T_{Sensing}$ and to orient itself as well as establish a connection to the existing network and begin routing communication is represented by T_{Setup} . The cell frequency has to be replaced by the UAV

network by following the non-overlapping frequency allocation scheme to avoid inter-cell interference. This response time can be used to determine which database center to request UAVs from when there multiple disaster response locations. The obvious choice would be to send UAVs from the closer response center with the exception being if the nearest response center has not sufficient UAVs or has already sent out all of its available UAVs. In this case, the next closest response center would need to be chosen.

Sometimes a daisy chain of UAVs needs to be created to form a link to the nearest communication tower. Such a scenario could occur if a remote tower becomes destroyed and there is secondary tower for the area. A line of UAVs could be used to effectively route information to the nearest tower. Consider N number of UAVs, the max linear coverage distance can be defined by eq. (4.3) T_r is the max linear coverage distance of the UAV network. T_1 is the transmission radius of the first UAV in the chain and T_N is the transmission radius of the N^{th} UAV. Each intermediate UAV can have their own transmission radius and so it is important to consider the minimum transmission range between any two UAVs. The equation states that the total linear transmission coverage is given by the transmission radius of the *first* UAV plus transmission radius of the N^{th} UAV plus the sum of the minimum transmission range of each of the intermediary UAV hops. In this way, the number of UAVs needed to form a chain from one area to another and the needed transmission ranges of each can be found.

$$T_r = T_1 + T_N + \sum_{i=1}^{N-1} \min\{T_i, T_{i+1}\} \quad (4.3)$$

It should also be noted that different frequencies will affect the maximum achievable transmission range attainable by the UAVs. It is shown in eq. 4.4 and in Fig. 4.4 as the frequency increases, the maximum possible transmission range will decrease. The typical operating frequency for modern cell phones range from 900 MHz to 2100 MHz. The graph provided shows that increasing the operating frequency results in a decreased maximum

transmission range.

$$d_{max} = \frac{c}{4\pi f} \sqrt{\frac{P_t}{P_r}} \quad (4.4)$$

When multiple UAVs replace destroyed cell tower(s), there will be multi-hop communications to fill the gap. The channel capacity (bps/Hz) [48] per UAV is given as

$$C = \frac{B}{K} \left(\frac{R_D}{R} \right)^{-1} \log_2(1 + \gamma_k) \quad (4.5)$$

where B is the channel bandwidth in hertz, K is the number of sub-channels for UAVs, R_D denotes the reuse distance (between nearest co-channels in the networks), R denotes the distance between two nodes, and γ_k is the signal-to-interference-plus-noise ratio (SINR).

The SINR is given as

$$\gamma_k = \frac{P_t \cdot R^{-\alpha}}{B \cdot N_0} K^{\alpha+1} = \sigma_s^2 / \sigma_n^2$$

where P_t is the transmit power, α path loss exponent, σ_s^2 is the variance of the received signal (when it is independent and identically distributed or i.i.d.) with zero mean, and $N_0 = \sigma_n^2$ is the noise variance (that corrupts the received signal assumed to be the Additive White Gaussian Noise (AWGN) and i.i.d.).

Given multiple UAVs in a network, the worst case propagation delay can be calculated. The absolute worst case propagation delay will occur when a message needs to be sent from one side of the network to the other that hops in between all UAVs in the network. P_d is the worst case propagation delay, N is the number of UAV hops, T_d is the propagation delay between the k th UAV and the $k + 1$ th UAV. The sum of all of the propagation delay hops will give you the worst case propagation delay of the network.

$$P_d = \sum_{k=1}^{N-1} T_d(k, k + 1) \quad (4.6)$$

Consider that the total of P_J packets of B_{p_j} bits/packet are transmitted through UAV

networks. Then the throughput for N -hop UAV network is given by

$$\theta = \frac{B_{p_j} \cdot P_j}{P_d} \frac{B}{\sum_{\forall i} (P_j + K - 1 + i) p_i} \quad (4.7)$$

where p_i is the probability of packet transmission for a given duration. This probability depends on average packet error rate p which is $p = 1 - (1 - p_b)_{p_j}^B$ for average bit-error-rate (BER). The p_b , for quadrature phase shift keying (QPSK) and Gaussian approximation of interference, is

$$p_b = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{\gamma_k}{2}} \right) \quad (4.8)$$

where $\operatorname{erfc}(\cdot)$ is the complementary error function.

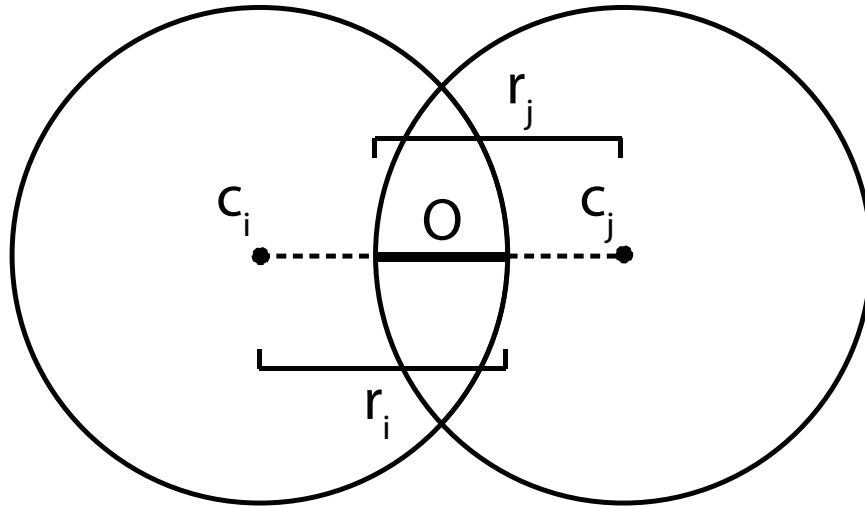


Figure 4.3: Overlap of two UAVs' transmission ranges.

Since there is a reuse distance in cellular UAV network, the system throughput is

$$\Theta = \theta \left(\frac{R_D}{R} \right)^{-1} \quad (4.9)$$

Each communication tower will have a set transmission range that needs to be covered by one or more UAVs if the tower is destroyed. The most optimal packing configuration that covers all of the area with limited overlap between UAVs will result in roughly 20.9% overlap [49]. Since signal quality tends to dissipate toward the edge of the transmission

range, the overlap is acceptable. The radius of each UAV transmission range is defined as r and $\|c_i - c_j\|_2$ as the 2-norm distance from one UAV to another. The overlap of the two transmission areas can be defined as the subtraction of the radii and the 2-norm distance as shown in Fig. 4.3.

$$O = r_i + r_j - \|c_i - c_j\|_2 \geq 0 \quad (4.10)$$

The goal is to reduce the overlap distance and find optimal number of UAVs needed to connect the disconnected network. If the total coverage area of the communication tower is defined as A_t and the coverage area of the UAVs as A_u , then the minimum number of UAVs needed to cover the area would be defined as a fraction of A_t over A_u multiplied by the packing density, $\rho_p = \frac{O}{r_i+r_j}$. It is known that the percent of overlap for an optimal packing configuration is roughly 20.9%, so the packing density should be one plus the overlap percentage or 120.9%.

$$N = \frac{A_t}{A_u} \rho_p \quad (4.11)$$

4.4 Performance Evaluation and Results

To corroborate theoretical analysis, first the number of UAVs (that are needed to connect the destroyed area with the rest of the network) for a given cell of a given transmission range of 1000 meters is plotted as shown in Fig. 4.5. The equation given in (4.11) shows that the total coverage area divided by the UAV coverage area and then multiplied by the optimal packing density gives us the number of UAVs needed. This will allow the response center to decide how many UAVs to send to a designated area to reconnect the destroyed area to the backhaul network.

From Fig. 4.5, as expected, it is observed that total number of UAVs decreases with their increasing transmission range. When a UAV is capable to cover entire destroyed cell area, then only one UAV is needed. However, to cover a given destroyed cell of 1 km, 2

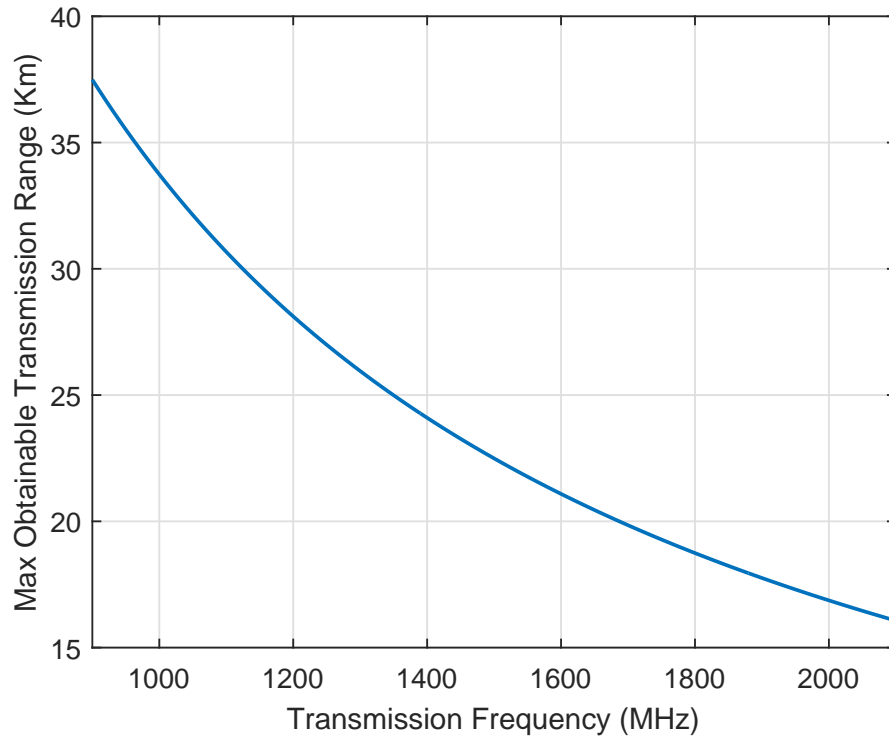


Figure 4.4: Assume a transmission power, P_t , of 2 watts and a threshold received power, P_r , of -90dBm (10^{-12} watts). The frequency range listed is from 900 MHz to 2100 MHz which is the typical cell phone operating frequencies. Note that increasing the transmission frequency results in a decreased max obtainable transmission range.

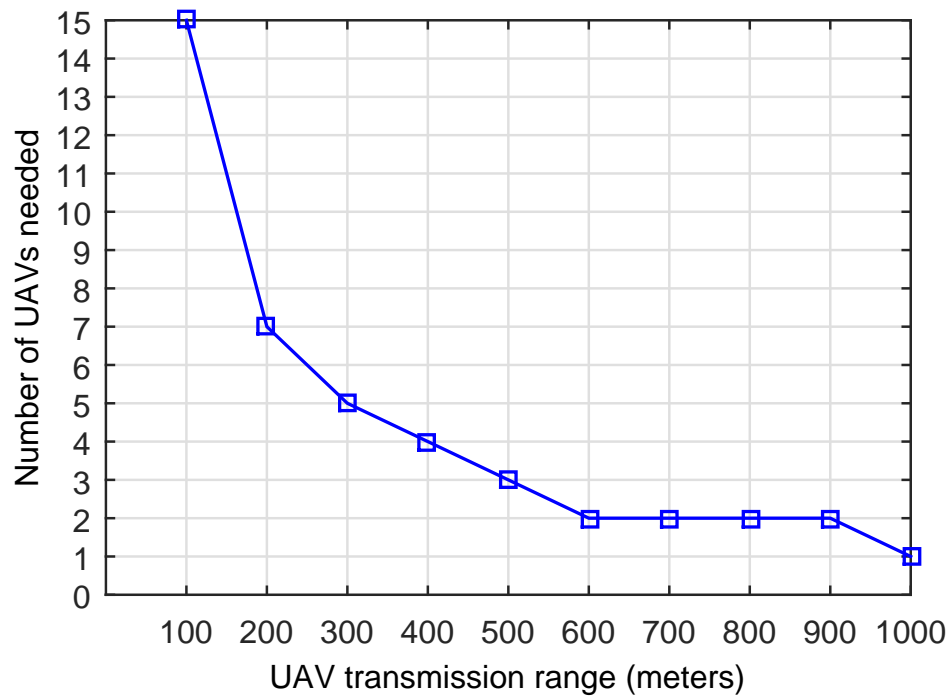


Figure 4.5: Given 1 km transmission range of a original cell tower, the amount of UAVs needed are shown based on their respective transmission range.

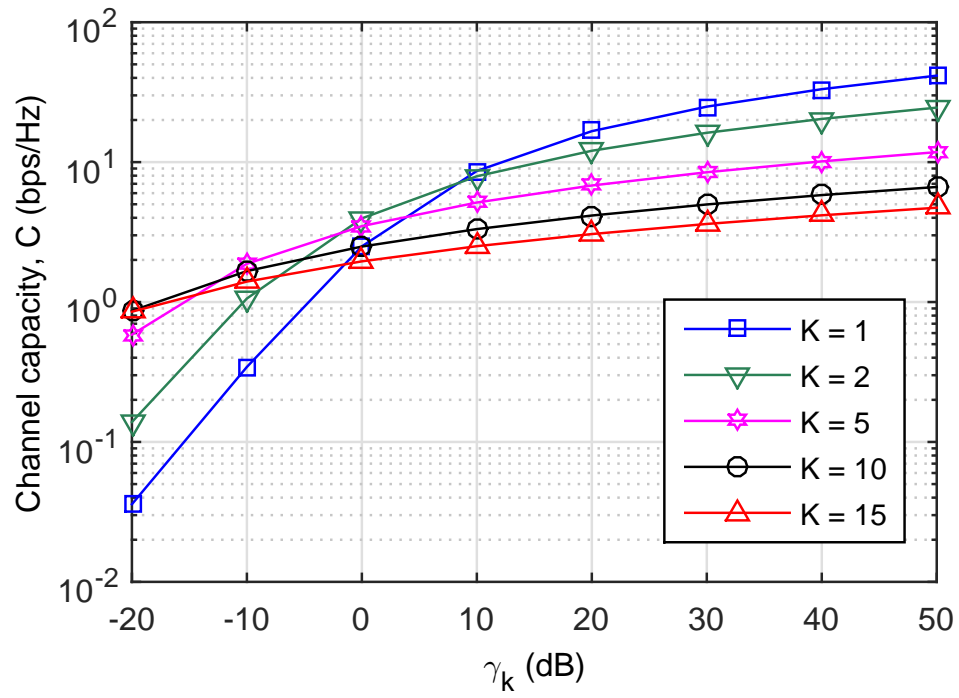


Figure 4.6: Channel Capacity vs. Signal to Interference plus Noise Ratio (SINR) γ_k for $\frac{R_D}{R} = 4$, path loss exponent $\alpha = 2$ and different K values.

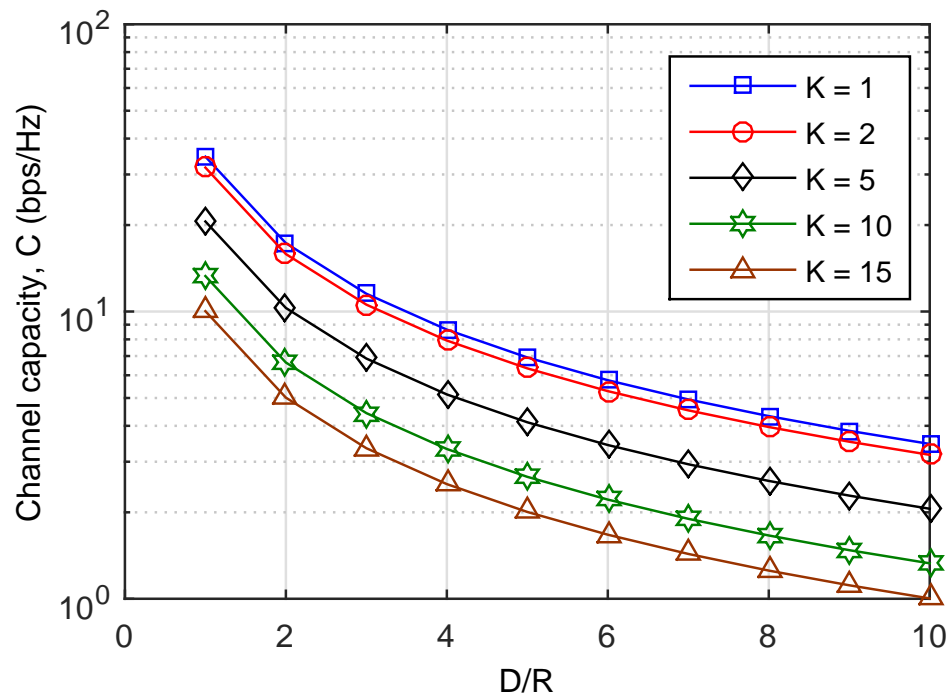


Figure 4.7: Channel Capacity vs. the ratio $\frac{R_D}{R}$ for Signal to Interference plus Noise Ratio (SINR) $\gamma_k = 10dB$, path loss exponent $\alpha = 4$ and different K values.

UAVs are needed when they have their transmission range from 600 m to 900 m.

Next, the variation of channel capacity versus the different SINR values for $\frac{R_D}{R} = 4$, path loss exponent $\alpha = 2$ and different K values is plotted as shown in Fig. 4.6. From Fig. 4.6, it is observed that as K increases (which maximizes the frequency reuse distance) the channel capacity decreases for high SINR. For higher K , the channel capacity is higher as multiple UAVs are close by from users with high transmit power (hence the SINR) compared to 1 hop network with large distance where it is difficult to receive enough power (resulting in weak SINR).

Similarly, the variation of channel capacity versus the different $\frac{R_D}{R}$ values for SINR $\gamma_k = 10dB$, path loss exponent $\alpha = 4$ and different K values was plotted as shown in Fig. 4.7. From Fig. 4.7, it was observed that the multi-hop UAV network achieves larger channel capacity than 1-hop network. The reason is that the received SINR increases with number of UAVs or K since the distance between the transmitter and receiver becomes shorter and received power becomes stronger.

4.5 Chapter Summary

In this chapter, an UAV-assisted wireless network to connect the disconnected network which is destroyed by natural or man-made disasters was designed and analyzed. In the proposed work, cloud based distributed database centers monitor the overall network and provide feedback to the emergency response centers when needed. When a communication tower is determined to be inoperable, emergency response centers deploy UAVs to establish the network on the fly by implementing suitable UAV packing to find the optimal number of UAVs and by providing geolocation to route the UAVs to the target location to recover communications in the affected area. The numerical results suggested that there are significant improvement in channel capacity and throughput after deploying UAV network to reconnect the destroyed network even in low SINR region. The optimal number of needed

UAVs for a given communication tower based on the coverage area of both the tower and the UAVs is also shown. It was noted that a tradeoff must be made between coverage area and propagation delay when deploying UAV networks for public safety communications. Future work includes looking into the number of users that can be covered by each UAV and how to handle if multiple UAVs are needed to cover the same area to provide sufficient wireless users.

CHAPTER 5
ROUTING SECURITY IN UAV-SUPPORTED MOBILE
NETWORKS FOR DISASTER RESPONSE
COMMUNICATION

During a disaster situation, communication between emergency responders is critical for relaying important information and sustaining an efficient rescue operation. Often during these disaster situations, communication infrastructure becomes damaged and made unusable. Without communication infrastructure responders are unable to transmit important information back to their headquarters. One possible solution is to make use of UAVs to act as mobile base stations that are capable of temporarily restoring vital communication to users. UAVs can be equipped with sensors and other important equipment that allow them to navigate autonomously to a disaster location and begin routing communication traffic. Such UAVs could provide communication between emergency responders as well as provide limited public communication channels as well. In this chapter, the different types of routing protocols that can be used in mobile ad hoc networks as well the different types of attacks that can occur will be discussed. Proposed solutions to preventing these attacks are presented with a focus on security of the overall network.

5.1 Introduction

Disasters can strike at any time, causing damage to an area. When a disaster occurs, emergency responders are called to this damaged area to quickly bring relief and restore order. These emergency responders require communication and coordination to best respond to an emergency situation. Since emergency responders are typically mobile, wireless connections are used to establish this communication and assist with coordination.

For cellular communication, a wireless connection to the public telephone network is established through the local cell tower. During a disaster, these towers can become

damaged and made unusable. If this occurs, wireless communications that rely on these towers and on the public telephone network will not work. Without access to the public telephone network, emergency responders are limited to local communication (if peer-to-peer communication is available). In order to solve this issue, UAV Ad hoc networks can be used to restore communication with the public telephone network [50, 51, 52]. UAVs can form a mesh network (peer-to-peer) in the affected area and span to the nearest cell tower communication range. Once set up, the UAVs can act as mobile base stations and start routing traffic to and from the cell tower. The use of these UAV mobile base stations would allow for emergency responders to continue using public cellphone network for communication even if the local cell towers are damaged or destroyed. UAVs are a temporary solution to restoring communication due to the fact that the power source is limited. A more permanent network must be set up as soon as possible. The UAV network would be used to restore communication quickly while a more permanent network can be moved into place.

Emergency responders are typically thought of in three departments: Fire and Rescue, Emergency Medical Services, and Police. Each of these departments maintain their own communication channels and protocols, which means that coordination between the different emergency departments is difficult. The Federal Communications Commission (FCC) and Congress have recently passed the Spectrum Act [4], which paves the path for designing a combined communication network specifically for use by emergency responders. This new combined communication network would allow for all emergency responders, no matter the department, to communicate and coordinate effectively. The Spectrum Act reserves the 700MHz frequency band for communication among these responders. In addition to reserving the 700MHz frequency band for emergency responders, the Spectrum Act also creates the First Responder Network Authority (FirstNet). FirstNet is tasked with creating a nationwide Public Safety broadband communication network that to link communication

for all emergency responders. This nationwide network would allow for more than just voice to be sent over the coordinated network. Multimedia messages such as video, pictures and other data would be able to be sent and received. The ability to send broadband data other than just voice would better prepare responders for emergency situations before they arrive at an affected area. The proposed UAV Ad hoc network should be able to integrate in with a broadband network and send the same necessary data.

The previous work mentioned had focused on the structure and communication range metrics associated within a UAV ad hoc network. For this chapter the security challenges related to UAV ad hoc networks as well as how to prevent most types of attacks will be investigated. The rest of the chapter is organized as follows: Section 5.2 discusses the necessary constraints in UAV ad hoc networks. Section 5.3 will go into detail about the system model and how UAV Ad hoc networks can be used to restore communication during disaster scenarios. In Section 5.4 the different communication protocols available for ad hoc networks are considered. Section 5.5 focuses on the available security techniques for ad hoc networks as well as the advantages and disadvantages of each. The research challenges are discussed in Section 5.6. The chapter concludes in Section 5.7 and wraps up with future works.

5.2 UAV Ad hoc Network Constraints

There are a number of factors that must be considered when dealing with UAV ad hoc networks as compared with traditional ad hoc networks. As shown in [53], these different features are node connectivity, node density, energy constraints, node mobility, and delay constraints. Each of these factors affect a UAV ad hoc network differently than would be considered in traditional ad hoc networks due to the mobile and aerial nature of UAVs.

- **Node Connectivity:** For UAV ad hoc networks, it cannot be considered that the

connection between two nodes will be constant or consistent. Depending on the mobility of each node and the interference at its location, the connection between two nodes can be degraded or even severed. If this occurs, the connection must be reestablished either through single or multi-hop communication. If a node leaves the network, then protocols must detect this quickly and update any routing schemes to reflect this change.

- **Node Density:** As compared to traditional ad hoc networks, the node density of UAV ad hoc networks is much less. Each UAV is able to have a much greater coverage area due to its three-dimensional nature and ability to quickly change positions. Since UAVs are aerial vehicles, they are able to configure themselves in a much more efficient way so as to cover the greatest possible area. As long as communication exists between each of the nodes within the network, UAV networks are capable of maintaining low node density.
- **Energy Constraints:** UAV ad hoc networks rely on the UAV itself for power. Usually a single battery provides power for both the movement and control of the UAV as well as the communication equipment. Due to this shared power source, the life time of a UAV node is limited. When the power of one node becomes drained, the network must reconfigure itself to adapt to the loss of a node.
- **Node Mobility:** Each node within this type of network is a UAV. This means that the node is capable of quickly moving from one place to another. While other types of ad hoc networks, such as vehicular ad hoc networks, share this same feature, they do so while assuming a two-dimensional plane. For UAV ad hoc networks, the nodes are capable of moving in three-dimensional space. This extra movement means that it is more common for nodes to quickly leave and enter the network. Communication between nodes must be quick so that data is not sent to a node that is leaving the

network.

- **Delay Constraints:** Building on the last constraint, nodes must be able to send data quickly in order to prevent having to resend data if a node leaves the network. Another reason data must be sent and received quickly is due to the fact that UAV ad hoc networks also talk to neighbor nodes to regularly update positional data. If neighbor nodes did not update position data frequently, nodes could collide.

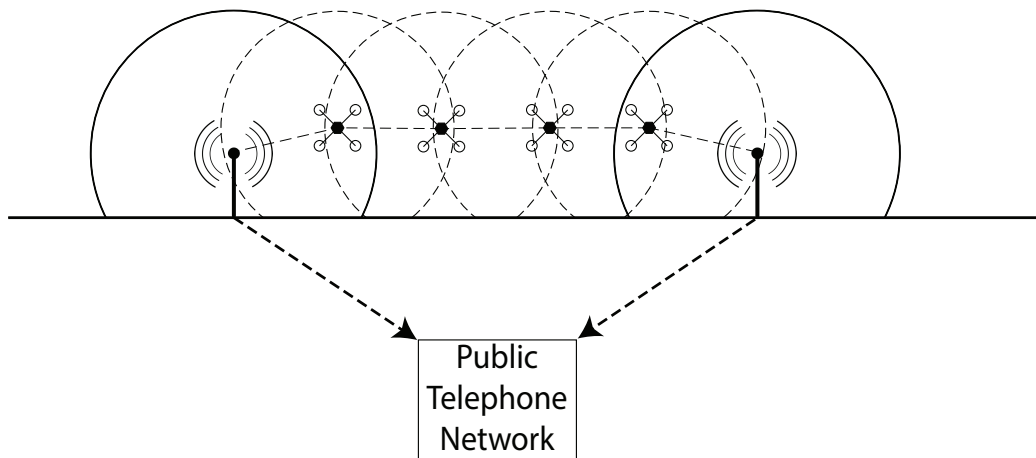


Figure 5.1: Unmanned Aerial Vehicle (UAV) ad hoc network connecting and routing communication between two disjoint cell towers. Such a network can connect users and devices cutoff from the Public Telephone Network due to a damaged or destroyed cell towers.

5.3 System Model

UAVs are flying vehicles that are either controlled remotely or controlled autonomously; for this chapter, the UAVs will be considered to be controlled autonomously. Autonomous flight is achievable through the use of various sensors and equipment on the UAV itself; these sensors and equipment includes GPS, magnetometer, gyroscope, and accelerometer

all controlled and managed by a microcontroller. The microcontroller reads data from each of the sensors and adjusts its current position, velocity and direction in order to maintain a stable flight path. The UAV network would be given a location to fly to and it would automatically determine the best path and avoid obstacles en route to the location. Once at the location, multiple UAVs would form an ad hoc network and begin routing communication data through to the nearest cell tower.

When a network is able to be formed between multiple devices without the use of a preexisting infrastructure, this is called an ad hoc network. UAVs are able to form these ad hoc networks between themselves to extend their effective range or to cover more area. If equipped with the necessary equipment, a UAV ad hoc network could route cell phone communication over large distances (depending on the size of the UAV network). The network would form a connection between the nearest cell tower and the desired location allowing all cell phone communication in the area to be routed through the connected tower. This can be very useful during disaster situations as communication infrastructure can become damaged or destroyed.

5.3.1 Scenario

Consider a disaster scenario (such as an earthquake or tornado) where damage to the local cell tower has occurred. This cell tower is no longer able to send or receive information from mobile users. As emergency responders arrive at the location, they are unable to connect with their headquarters or dispatcher to request equipment or other necessities; hospitals can not be contacted to determine if they have space for more patients. A solution is needed to restore mobile communication quickly after a cell tower becomes unusable in order to restore communication. Traditional systems are able to bring in a temporary system (such as a generator and mobile base station) but it takes time, especially if damage to the driving infrastructure occurred. The proposed system discussed earlier would be able to restore

communication as soon as possible. UAVs benefit from the ability to fly to the location. Flying to a location means that UAVs can avoid obstacles and terrestrial damage that might have occurred. This aerial ability also means that a direction path from the takeoff location to the destination can be followed. The following subsections will discuss the system in detail.

5.3.2 UAV Mobile Base Stations

Each UAV acts as a mobile base station. By forming an ad hoc networks with other UAV base stations, the range of coverage can be extended to virtually any area. This area covered by these UAVs would route traffic through the UAV network to the closest working cell tower. From there, the communication is routed to the public telephone network and on to the requested destination. Since UAVs are battery powered, the individual nodes within the network can only exist temporarily before they must be replaced or recharged. One such solution to this is to rotate out depleted nodes with fresh UAVs. A more practical solution is to deploy a more permanent system (such as a static ground based network) that can be directly connected to the public telephone network). Airborne vehicles are able to reach a location much quicker than ground-based counterparts and therefore are beneficial for immediate response. The ideal system would deploy both UAV and ground nodes with ground nodes being a more permanent communication system (until the cell tower can be repaired). The UAV network would aim to restore communication as quickly as possible so as to minimize damage to life and property while the ground network would take over as soon as it is able.

5.3.3 Deployment Centers

Using certain criteria and metrics, deployment centers would be positioned throughout an area. Each deployment center is responsible for it's own sub-area. Inside these centers

are housed multiple UAVs that can act as mobile base stations. The UAVs are housed and maintained until they are needed. When a disaster occurs and damages part of the communication network, a signal is sent to the deployment center and activates the necessary number of UAVs. This number is based on the number of communication devices predicted to be in the area as well as the total area needed to be covered. These UAVs then fly out to the disaster affected area and form mesh networks to restore communication and reconnect it with the existing communication network. Since UAVs are battery operated, they are only a temporary fix for the destroyed communication infrastructure. The advantage of this system is that they are much quicker than the more permanent land based counterparts. Deployment centers house the UAVs until they are needed. Updates to the UAVs and maintenance are also done. Charging of batteries, etc. Deployment centers are strategically placed based on certain metrics. When a disaster is detected, UAVs would be deployed to the area to restore communication. Different metrics can be seen in [51]. After a more permanent communication system is set up, the UAVs would return to the deployment center to await further instruction and recharge.

5.4 Routing Protocols for Mobile Ad Hoc Networks

There are many types of ad hoc routing protocols used for mobile networks. In this chapter the focus will be on Proactive, Reactive, and hybrid protocols. The benefits, challenges and uses of each type of protocol will be listed. Proactive and Reactive protocols each have benefits and challenges that are opposite of each other while hybrid protocols take the benefits of both networks. UAV networks must have a trade off with these protocols. UAVs require that data sent through the network have a low end-to-end delay in order to counter any changes in the node architecture that can occur. At the same time, power and bandwidth are limited for this type of network. A protocol for a UAV network must be chosen such that it works best for the required task. Proactive protocols work best for

maximizing connectivity and minimizing propagation delay while reactive protocols work best for minimizing energy consumption and bandwidth usage.

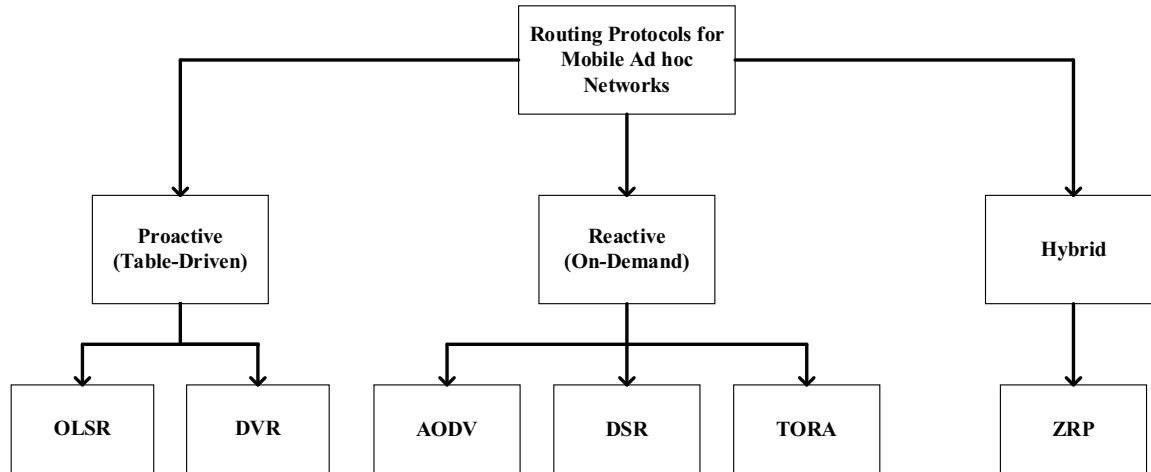


Figure 5.2: The groupings of different types of Mobile Ad hoc Networks

5.4.1 Proactive Routing

Proactive Routing protocols frequently update their routing tables to have the most up to date information about routes to any node on the network. These types of protocols will be able to always know the quickest path to any node but are not able to react to restructuring of the network. These networks also have a lot of overhead traffic as the routing tables must be constantly updated if they wish to maintain the best path to any node within the network. For UAV networks, the quickest path to any node must be known in order to maintain connectivity with the network. The protocol used must be able to react and know if any node leaves or enters the network.

- **Optimized Link State Routing (OLSR):** Optimized Link State Routing or OLSR is a proactive routing protocol used in mobile ad hoc networks. In this type of

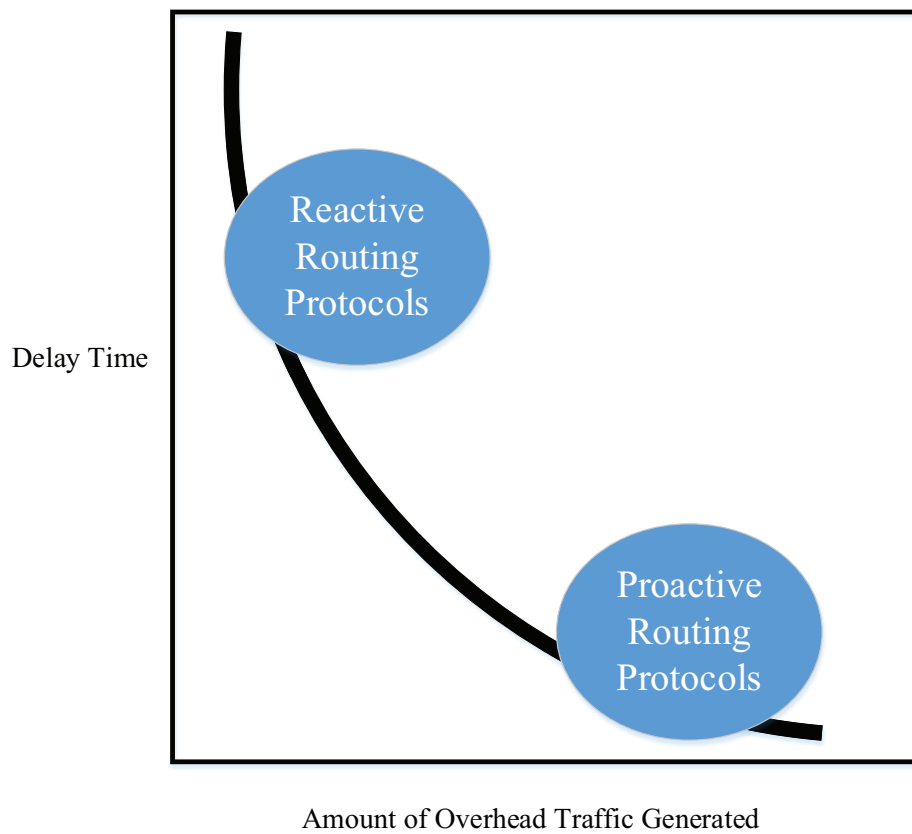


Figure 5.3: Increasing the amount of overhead traffic (the control signals and other path information) results in the delay time associated with sending a message from one point of the network to the other to decrease.

routing, each node within the network creates a set of neighbor nodes to use as multi-point relays. These relays are used to forward control traffic to other nodes within the network. Since only the multi-point relays forward control traffic, this reduces (optimizes) the amount of control traffic that gets sent within the network. The key benefit of OLSR over other types of routing protocols is that it reduces the traffic associated with proactive routing protocols while still maintaining the most up-to-date routing paths to any node within the network.

- **Distance Vector Routing (DVR):** Distance Vector Routing is another type of routing protocol where each node does within the network does not know the fastest path to any other node within the network. Instead, these nodes keep a table of the distance and direction to all of its neighbor nodes. When a message needs to be sent over multiple nodes, the initial node sends it to the closest neighbor node in the correct direction. This next nodes in the path do the same thing until the destination is reached. Since only the distance and direction to each neighbor node is needed, this further reduces the amount of control traffic that is sent in this type of protocol (as compared to OLSR).

5.4.2 Reactive Routing

In Reactive Routing, the path to any node within the network is not known until it is needed. The path is discovered by flooding the network with queries to determine a suitable path. Since paths are only discovered based on when they are needed. This type of protocol typically takes longer to send messages than proactive routing protocols. This disadvantage is countered with the fact that very little overhead is needed for reactive routing protocols. For UAV networks, computing power and bandwidth is limited as multiple nodes exist in any network. In this way, reactive protocols save on both bandwidth and energy efficiency.

- **Ad hoc On-Demand Distance Vector (AODV):** Ad hoc On-Demand Distance Vector routing uses three different types of messages when determining a route: Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs). Route Requests are initially sent to flood the network and wait for a reply to determine a viable route. If a Route Reply is received, the network knows that the destination can be reached through that particular route. Route Errors notify the network if a break in the active route occurs. These messages only need to be used when a direct link (single hop link) cannot be established between two nodes. This type of routing is used in Zigbee networks.
- **Dynamic Source Routing (DSR):** This protocol is similar to AODV, but uses source routing instead of routing tables. In source routing, the path through the network is sent from the source of the message. This is different from a routing table in which each node updates the best path from one node to another. Source routing follows only the path specified by the source. This type of routing prevents attacks by making it more difficult to reroute the message during transmission. There are two major phases for this protocol, Route Discovery and Route Maintenance. Route Replies are sent when a message reaches its destination.
- **Temporally Ordered Routing Algorithm (TORA):** Temporally Ordered Routing Algorithm is a flat, non-hierarchical routing algorithm. It consists of three major phases: Route Creation, Route Maintenance, and Route Erasure. A route is initially created in Route Creation. This route is monitored and maintained in Route Maintenance. When a route is finished and no longer needed, it is forgotten in Route Erasure. Based off of these phases a Directed Acyclic Graph at the destination is formed. This graph is used to represent the route from any point to the destination.

5.4.3 Hybrid Routing

Hybrid routing protocols are able to benefit from both previous types of protocols. This subsection will focus solely on the Zone Routing Protocol and show how it takes the best of both proactive and reactive protocols.

- **Zone Routing Protocol (ZRP):** This type of routing is designed to speed up delivery and reduce overhead by selecting the most efficient type of protocol to use at any point in the route from one node to another. Establishes zones based on needs and availability. Different zones are created within the network that run different types of routing protocols based on location and need. If one part of the network benefits greatly from a reactive protocol while another benefits from a proactive protocol, those two zones can run the necessary routing protocol and still work with each other.

5.5 Security in UAV Ad hoc Networks

Security in ad hoc networks is difficult due to the fact that each node is considered both a router and a client. Each node must decide if it trusts the other nodes in the network. As nodes join or leave a network or as nodes move within the network, the network topology changes and route are shifted. This makes securing the network a challenge. For UAV networks, the nodes are even more mobile. UAVs move in and out of the network much more quickly than traditional ad hoc networks. There are other features that also cause UAV ad hoc networks to be vulnerable to attacks as well and can be found more in depth in [54, 55]

5.5.1 Confidentiality, Integrity, Availability Triad

Security for any network can be broken into three different areas: Confidentiality, Integrity and Availability. This is called the C.I.A. triad. For UAV networks, the same approach can

be applied as it is required that the data being sent between nodes needs to be as secure as possible. For multi-hop communication it is important that intermediate hops are not able to read the data being forwarded. Attackers can gain access to the network if this triad is not followed. Each part of this triad is explained below with examples pertaining to UAV ad hoc networks. Further information on the types of attacks regarding each of these can be found in [56].

- **Confidentiality:** In security, confidentiality means that unauthorized users should not have access to important or sensitive data. At the same time, authorized users should be able to access this data. In UAV ad hoc networks, this means that attackers should not have access to data being transmitted. Since data is sent wirelessly, attackers will be able to pick up data being transmitted if they are within range. In order to combat this wireless challenge, data should be encrypted in such a way that even if attackers are able to collect the data, they are unable to decrypt it.
- **Integrity:** The integrity of data should be maintained. For example if data is sent between two nodes, attackers should not be able to modify the data without the legitimate users being aware. Encryption of the data should be set up such that any modification to the data being transmitted would be instantly recognized at the receiving node.
- **Availability:** Availability of the data and network should be near consistent. Attacks focusing on causing disruption to the network should be resolved quickly as to minimize down time of the network. This is especially important for UAV ad hoc network as any disruption to the network could cause a catastrophic failure.

5.5.2 Routing Attacks

There are many different types of attacks that can occur in an ad hoc network. A few selected attacks are listed below with more in-depth discussion located in [57, 58, 59, 60, 61, 62]

- **Wormhole Attacks:** Wormhole attacks work by creating a link between two nodes within an ad hoc network. This link can occur between two nodes that are not typically close to each other (in other words, more than a single hop away). The wormhole receives data from the source node and passes it onto the destination. Since the destination receives data through the wormhole, it assumes that the source is now one hop away. The routing table is updated and will now see the source as a neighbor node. An attacker can do two things with this wormhole: denial of service and eavesdropping. By routing the information from source to destination, an attacker is able to also see all the information being sent. If the attacker also has the cryptographic keys of the network, then they would be able to read the encrypted data as well. The second type of disruption that a wormhole attack can generate is a denial-of-service attack. By switching the wormhole on and off periodically, the routing tables in the network would need to be updated. The overhead traffic caused by the updating of the routing tables would slow the network tremendously.
- **Blackhole Attacks:** In this type of attacks a malicious node enters the network. By sending out routing information to neighbor nodes and pretending to have the best routing path to any node, the attacker node is able to trick all neighbor nodes to route information to itself. Once the data is received, the attacker node drops packets instead of forwarding them to the appropriate destination node. This type of attack prevents data from being sent through the network as all of it is instead routed to the attacker node.
- **Rushing Attacks:** A Rushing Attack works similar to a wormhole attack. Two

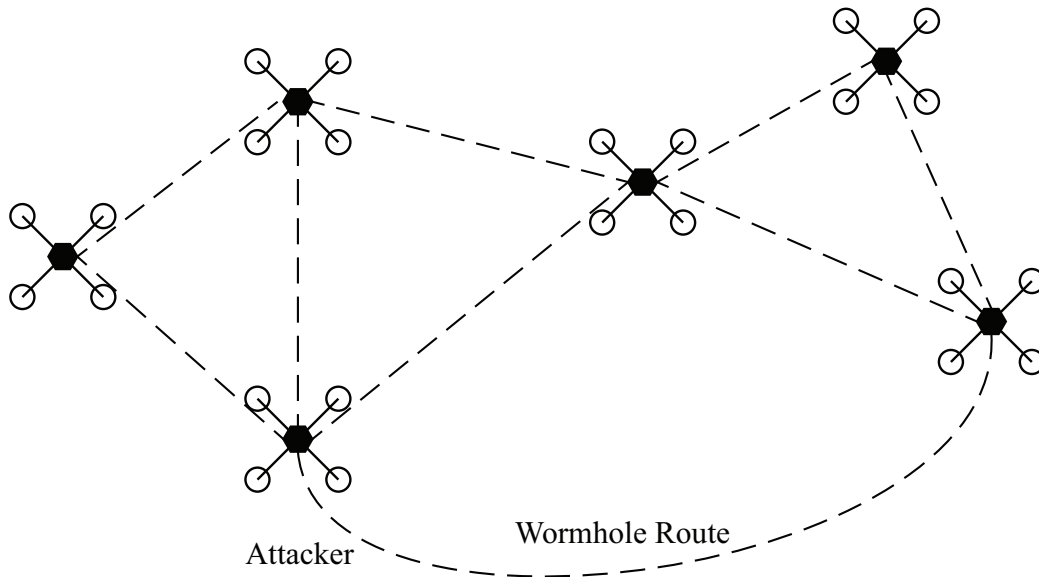


Figure 5.4: A wormhole attack where an attacker node routes data to another part of the network while eavesdropping on the information. This attacker node can be turned on and off to cause havoc with the routing table in the network.

attacker nodes work together and enter an ad hoc network. These nodes form are assumed to have a dedicated path between each other and span from one part of the network to the another. Since a dedicated path exists between the two attacker nodes, this path is assumed to be fastest and is used over other multi-hop paths. Data sent through the attacker nodes can then be read and forwarded or the data can be dropped (preventing the network from communicating).

- **Link Spoofing Attacks:** In Link spoofing, an attacker broadcasts to the rest of the network that it has a one-hop connection to non-neighbor nodes. This means that neighbor nodes attempting to reach that distant node through the fake link will send data to the attacker node to forward on the data. The attacker node can then drop the data to disrupt data flow within the network or it can forward the data after reading or modifying it.

- **Node Spoofing Attacks:** When an attacker node pretends to be another legitimate node, it is called a spoofing attack. An attacker gains information about a specific node within the network and takes on its credentials. The attacker is then able to enter the network with the stolen credentials. When a message is trying to be sent to the legitimate node, it will instead be sent to the attacker node, allowing the attacker to read the data.
- **Flooding Attacks:** Attacker nodes can attempt to send junk data into the network to waste bandwidth. The attacker sends the junk data into the network and tries to keep it moving between nodes for as long as it can. The more junk data that is sent through the network, the more bandwidth that is wasted and unable to be used for legitimate messages.
- **Replay Attacks:** In replay attacks, legitimate data is detected by the attacker node and is retransmitted over and over to use up bandwidth. Since the data is legitimate, it is difficult to determine if the original source node is sending the message again or if the resent data is an attack.
- **Byzantine Attacks:** By injecting multiple attacker nodes into the network, an attacker can cause havoc by individually telling the attacker nodes to do a number of different smaller attacks. These attacker nodes can randomly drop packets or route packets through longer paths. The goal of this type of attack is to disrupt packet flow and efficiency throughout the network.

5.5.3 UAV Ad hoc Networks Security Solutions

All of these different types of attacks can be present in UAV ad hoc networks since the same routing protocols are used as traditional ad hoc networks. UAVs are aerial vehicles and it should be easy to spot an attacker flying within the network but attackers can spoof

their location data and hide somewhere on the ground while broadcasting. In order to prevent certain types of attacks, various papers have suggested using different techniques [63]. For things like flooding attacks, where nodes are bombarded with packets from an attacker node, legitimate nodes should monitor the transmission rate of each neighbor node. If the transmission rate increases above a certain threshold, then the node is blacklisted and all communication from it is ignored. For attacks that use spoofing, nodes should use cryptography with GPS and time stamp information. Each time a message is sent, the location of the node as well as the time is sent with it. Attackers are still able to spoof the location data, but it would be very difficult to update the location data in real time since UAV ad hoc networks are extremely mobile and constantly moving. This same type of approach can be used for wormhole and Byzantine attackers. By knowing the location of each node within the network based off of GPS readings, it would be difficult for attackers to spoof a realistic location while still convincing the network to route data through the attacker node due to the mobility of a UAV ad hoc network.

5.6 Research Challenges

UAV ad hoc networks can provide a fast and effective temporary communication network for scenarios where access to the wireless cell tower is not available. While the scenario presented in this chapter focused on communication in disaster situations, the UAVs can be made to multitask. When equipped with camera and other critical sensors, the UAVs can work together with emergency responders to allow responders to have a better overview of a disaster area. Search and rescue operations can be carried out with the UAVs all while still acting as mobile base stations. As the UAVs fly over an area, using equipped cameras a virtual map can be created and be made accessible to responders. Further research in this area can be very beneficial to this type of network.

5.7 Chapter Summary

An overview of different routing techniques that can be used in mobile ad hoc networks were presented. Security challenges were address concerning UAV ad hoc networks as well as possible solutions to prevent most types of network attacks. These types of techniques can be applied to the proposed UAV communication network and the network be used in disaster situations where the local cell tower is damaged or destroyed. Research challenges were discussed with respect to future work that can be done in this field of research, mostly focusing on how to efficiently use UAV mobile base stations. UAV ad hoc networks can be deployed much quicker than traditional, ground-based ad hoc networks and can act as a temporary communication link between users and the public telephone network. This UAV network is able to rapidly restore communication to areas where the cell tower is unusable while still providing a stable communication platform for emergency responders.

CHAPTER 6

DISCUSSION, CONCLUSION, AND FUTURE WORK

The adaptivity algorithm described in chapter 2 was shown to increase the probability of a successful connection between nodes for the simulation time in Figure 2.2. Specifically, there is an abrupt loss in communication that happens at the 400 second mark that simulates a change in the network architecture (such as a single UAV leaving the network). The designed algorithm is able to adapt to this change in the network and only suffers a minor loss in probability of connectivity while the static network has a large loss in probability of connectivity. The adaptivity algorithm presented in this chapter shows a large improvement over a static scenario for UAV ad hoc networks.

The effects of an increased transmission time and an increased number of UAVs are shown in chapter 3. Two of those figures (3.3 and 3.4) show the effect of an increasing number of UAVs on transmission range and propagation delay. As the number of UAVs increase in a network, the worst case propagation delay will increase since the number of hops will increase. A similar effect can be seen for transmission range; an increase in the number of UAVs leads to an increase in the overall transmission range (the distance a message can be sent) of the network. Other results for this chapter include figures (3.2 and 3.6) which show the effect of an increased transmission time on the needed data rate and goodput per unit energy. Both of these show similar results since an increase in available transmission time means that less information or energy needs to be expended per second. Increasing the total transmission time will result in less data rate and less goodput per energy needed.

The main feature of chapter 4 is on the change in channel capacity when increasing signal to interference plus noise ratio (SINR) and increasing the reuse distance. By increasing the SINR, the channel capacity increases to a certain threshold (channel capacity cannot increase past the Shannon-Hartley limit). In a cellular communication system, the reuse

distance ratio is defined by the distance between nodes divided by the reuse distance. By increasing the reuse distance, the channel capacity will decrease due to the fact that your reuse cells start to overlap each other causing interference (thereby decreasing SINR).

An integrated UAV ad hoc network for emergency response communication was designed, analyzed, and evaluated. Results detailing the performance of the network were presented with specific focus on data rate, channel capacity, propagation delay and transmission range. The work presented supports the ground work for future research in this area.

Restoring communication as quickly as possible and informing emergency responders of an emergency situation is of utmost importance for minimizing loss of life and property. The system presented integrates in with existing cellular technologies while having the advantage of unmanned flight which reduces the travel time to the destination. As such, this system will restore communication in areas where the telephone network is damaged and inoperable while autonomously controlling itself.

6.1 Future Work

The work presented in this thesis has focused on analyzing performance dealing with an UAV ad hoc network for emergency response communication. As FirstNet is rolled out across the United States, it would be beneficial to consider integration of this UAV network with the FirstNet channels and equipment to allow for integrated support of the system.

Another area of research is in the cost analysis of such a system. It is expected that such a system will yield a decrease in loss of life as the system will restore communication faster than ground-based communication response systems. This decrease in loss of life can be compared with the cost of such a system.

The battery life of each UAV also needs to be considered. The system is only viable as long as the UAVs are able to stay airborne and route communication data. Since batteries

are inherently transient, a solution is required to keep the system function for long periods of time. One suggestion is to cycle out UAVs as their batteries drain.

Assuming that some all-terrain robots can be developed to act as mobile base stations, the analysis done in this thesis can also be applied to such a system. An all-terrain vehicles would be unaffected by certain levels of obstructions and therefore would have similar response times to UAV implementations.

REFERENCES

- [1] ©[2015] IEEE. Reprinted, with permission, from [D.B. Rawat, R. Grodi, C. Bajracharya, “Enhancing connectivity for communication and control in unmanned aerial vehicle networks,” in *2015 IEEE Radio and Wireless Week (IEEE RWW 2015)*, pp. 200-202, 2015].
- [2] ©[2015] IEEE. Reprinted, with permission, from [R. Grodi, D.B. Rawat, C. Bajracharya, “Performance evaluation of unmanned aerial vehicle ad hoc networks,” in *Southeastcon 2015*, pp. 1-4, 2015].
- [3] ©[2015] IEEE. Reprinted, with permission, from [R. Grodi, D.B. Rawat, “Uav-assisted broadband network for emergency and public safety communications,” in *Signal and Information Processing (GlobalSIP), 2015 IEEE Global Conference on.*, pp. 10-14, 2015].
- [4] (2015) 700 mhz public safety spectrum. [Online]. Available: <https://www.fcc.gov/encyclopedia/700-mhz-spectrum>
- [5] A. C. Watts, V. G. Ambrosia, and E. A. Hinkley, “Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use,” *Remote Sensing*, vol. 4, no. 6, pp. 1671–1692, 2012.
- [6] (2016, Feb) Amazon prime air. [Online]. Available: <http://amzn.to/1cXMamo>
- [7] E. Yanmaz, “Connectivity versus area coverage in unmanned aerial vehicle networks,” in *2012 IEEE International Conference on Communications (ICC 2012)*, June 2012, pp. 719–723.
- [8] A. I. Alshbatat and L. Dong, “Performance analysis of mobile ad hoc unmanned aerial vehicle communication networks with directional antennas,” *Int’l Journal of Aerospace Engineering*, vol. 2010, 2011.
- [9] W. L. Teacy, J. Nie, S. McClean, and G. Parr, “Maintaining connectivity in UAV swarm sensing,” in *2010 IEEE GLOBECOM Workshops*, December 2010, pp. 1771–1776.
- [10] Z. Han, A. L. Swindlehurst, and K. R. Liu, “Smart deployment/movement of unmanned air vehicle to improve connectivity in MANET,” in *IEEE WCNC 2006*, 2006, pp. 252–257.

- [11] Z. Xu, J. Huo, Y. Wang, J. Yuan, X. Shan, and Z. Feng, "Analyzing two connectivities in UAV-ground mobile ad hoc networks," in *2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2011, pp. 158–162.
- [12] J. Schleich, A. Panchapakesan, G. Danoy, and P. Bouvry, "UAV fleet area coverage with network connectivity constraint," in *11th ACM international symposium on Mobility management and wireless access*, 2013, pp. 131–138.
- [13] T. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall PTR New Jersey, 2002.
- [14] D. B. Rawat, D. C. Popescu, G. Yan, and S. Olariu, "Enhancing VANET performance by joint adaptation of transmission power and contention window size," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1528–1535, 2011.
- [15] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, 2012.
- [16] D. M. Marshall, R. K. Barnhart, S. B. Hottman, E. Shappee, and M. T. Most, *Introduction to unmanned aircraft systems*. CRC Press, 2011.
- [17] R. Austin, *Unmanned aircraft systems: UAVs design, development and deployment*. John Wiley & Sons, 2011, vol. 54.
- [18] D. B. Rawat, M. Song, and S. Shetty, "Resource Allocation for Cognitive Radio Enabled Vehicular Network Users," in *Dynamic Spectrum Access for Wireless Networks*. Springer International Publishing, 2015, pp. 57–65.
- [19] B. B. Bista and D. B. Rawat, "A Robust Energy Efficient Epidemic Routing Protocol for Delay Tolerant Networks," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*, 2015, pp. 290–296.
- [20] K. M. Rabbi, D. B. Rawat, M. A. Ahad, and T. Amin, "Analysis of multi-hop opportunistic communications in cognitive radio network," in *IEEE SoutheastCon 2015*, 2015, pp. 1–8.
- [21] D. B. Rawat, M. Song, and S. Shetty, *Dynamic Spectrum Access for Wireless Networks*. Springer, 2015.

- [22] J. L. Mauri, K. Z. Ghafoor, D. B. Rawat, and J. M. A. Perez, *Cognitive Networks: Applications and Deployments*. CRC Press, 2014.
- [23] D. B. Rawat, B. B. Bista, G. Yan, and S. Olariu, "Vehicle-to-Vehicle Connectivity and Communication Framework for Vehicular Ad-Hoc Networks," in *2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS'14)*, 2014, pp. 44–49.
- [24] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust On the Security of Wireless Vehicular Ad-hoc Networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.
- [25] G. Yan, S. El-Tawab, and D. Rawat, "Reliable routing protocols in VANETs," *IGI Global*, 2009.
- [26] G. Yan, D. B. Rawat, and B. B. Bista, "The Mobility-based Reliable Routing in VANET," *7 th International workshop on Wireless Adhoc and Sensor Networking*, vol. 1, no. 1, 2010.
- [27] E. W. Frew and T. X. Brown, "Networking issues for small unmanned aircraft systems," *Journal of Intelligent and Robotic Systems*, vol. 54, no. 1-3, pp. 21–37, 2009.
- [28] D. B. Rawat, R. Grodi, and C. Bajracharya, "Enhancing connectivity for communication and control in unmanned aerial vehicle networks," in *2015 IEEE Radio and Wireless Week (IEEE RWW 2015)*, January 25 – 28 2015.
- [29] C. Mbarushimana and A. Shahrabi, "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks," in *21st International Conference on Advanced Information Networking and Applications Workshops 2007*, vol. 2, 2007, pp. 679–684.
- [30] D. L. Gu, G. Pei, H. Ly, M. Gerla, B. Zhang, and X. Hong, "Uav aided intelligent routing for ad-hoc wireless network in single-area theater," in *IEEE Wireless Communications and Networking Conference 2000 (WCNC 2000)*, vol. 3, 2000, pp. 1220–1225.
- [31] Y. Li, J. Harms, and R. Holte, "Impact of lossy links on performance of multihop wireless networks," in *2005 14th International Conference on Computer Communications and Networks*, 2005, pp. 303–308.

- [32] C.-M. Cheng, P.-H. Hsiao, H. Kung, and D. Vlah, "Maximizing throughput of uav-relaying networks with the load-carry-and-deliver paradigm," in *IEEE Wireless Communications and Networking Conference 2007 (WCNC 2007)*, 2007, pp. 4417–4424.
- [33] P. C. Ng and S. C. Liew, "Throughput analysis of ieee802. 11 multi-hop ad hoc networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 15, no. 2, pp. 309–322, 2007.
- [34] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser, "An analysis of the optimum node density for ad hoc mobile networks," in *2001 IEEE International Conference on Communications (ICC 2001)*, vol. 3, 2001, pp. 857–861.
- [35] R. Hallahan and J. M. Peha, "Enabling public safety priority use of commercial wireless networks," *Homeland Security Affairs*, vol. 9, p. 13, 2013.
- [36] J. M. Peha, "How america's fragmented approach to public safety wastes money and spectrum," *Telecommunications Policy*, vol. 31, no. 10, pp. 605–618, 2007.
- [37] ———, "A public-private approach to public safety communications," *Issues in Science and Technology*, vol. 29, no. 4, p. 37, 2013.
- [38] J. A. Manner, S. Newman, and J. M. Peha, "The fcc plan for a public safety broadband wireless network," in *38th telecommunications policy research conference*. Retrieved from {http://tprcweb.com/images/stories/2010%20papers/Peha_2010.pdf}, 2010.
- [39] A. Gorcin and H. Arslan, "Public safety and emergency case communications: Opportunities from the aspect of cognitive radio," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2008)*, 2008, pp. 1–10.
- [40] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.
- [41] B. Le, F. A. Rodriguez, Q. Chen, B. P. Li, F. Ge, M. ElNainay, T. W. Rondeau, and C. W. Bostian, "A public safety cognitive radio node," in *2007 SDR forum technical conference (SDRF 2007)*, 2007.
- [42] M. Chen, S. Mao, Y. Zhang, and V. C. Leung, *Big data: related technologies, challenges and future prospects*. Springer, 2014.

- [43] T. Jiang, H. Wang, and Y. Zhang, "Modeling channel allocation for multimedia transmission over infrastructure based cognitive radio networks," *IEEE Systems Journal*, vol. 5, no. 3, pp. 417–426, 2011.
- [44] M. Portmann and A. A. Pirzada, "Wireless mesh networks for public safety and crisis management applications," *IEEE Internet Computing*, vol. 12, no. 1, pp. 18–25, 2008.
- [45] G. Iapichino, C. Bonnet, O. del Rio Herrero, C. Baudoin, and I. Buret, "A mobile ad-hoc satellite and wireless mesh networking approach for public safety communications," in *2008 10th International Workshop on Signal Processing for Space Communications (SPSC 2008)*, 2008, pp. 1–6.
- [46] H. Coxeter, "Division of mathematics: The problem of packing a number of equal nonoverlapping circles on a sphere*," *Transactions of the New York Academy of Sciences*, vol. 24, no. 3 Series II, pp. 320–331, 1962.
- [47] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
- [48] B. Sklar, *Digital communications*. Prentice Hall NJ, 2001, vol. 2.
- [49] R. Kershner, "The number of circles covering a set," *American Journal of Mathematics*, pp. 665–671, 1939.
- [50] A. Merwaday and I. Guvenc, "Uav assisted heterogeneous networks for public safety communications," in *2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2015, pp. 329–334.
- [51] R. Grodi and D. B. Rawat, "Uav-assisted broadband network for emergency and public safety communications," in *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2015.
- [52] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 619–641, 2014.
- [53] J.-A. Maxa, B. Mahmoud, M. Slim, and N. Larrieu, "Secure routing protocol design for uav ad hoc networks," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, 2015, pp. 4A5–1.

- [54] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," *Infotech@ Aerospace*, 2012.
- [55] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.
- [56] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, 2012, pp. 585–590.
- [57] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.
- [58] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in *2005 IEEE Wireless Communications and Networking Conference*, vol. 2, 2005, pp. 1193–1199.
- [59] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless communications*, vol. 14, no. 5, pp. 85–91, 2007.
- [60] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE communications surveys*, vol. 7, no. 4, pp. 2–28, 2005.
- [61] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *2002 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, 2002, pp. 403–410.
- [62] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70–75, 2002.
- [63] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," *International Journal of Computer Applications*, vol. 9, no. 12, pp. 11–15, 2010.