Design of A Cyber Security Framework for ADS-B Based Surveillance Systems

Sahar Amin
Tyler Clark
Rennix Offutt
Kate Serenko

Department of Systems Engineering and Operations Research
George Mason University
Fairfax, VA 22030-4444
April 23, 2014
# Table of Contents

Table of Tables ........................................................................................................... 4

1.0 Context Analysis ................................................................................................. 5
  1.1 Increase in Air Transportation ................................................................. 5
  1.2 Primary and Secondary Surveillance Radar ........................................ 6
  1.3 Next Generation and Automatic Dependent Surveillance Broadcast (ADS-B) .... 7
  1.4 ADS-B Messages ..................................................................................... 8
  1.5 Threats to ADS-B ................................................................................. 9
  1.6 Scope ................................................................................................. 11

2.0 Stakeholder Analysis .......................................................................................... 12
  2.1 Primary Stakeholders ........................................................................ 12
    2.1.1 Federal Aviation Administration .............................................. 12
    2.1.2 Air Route Traffic Control Center ......................................... 12
    2.1.3 Airline Companies ................................................................... 13
    2.1.4 Crew and Pilots ...................................................................... 13
  2.2Secondary Stakeholders ........................................................................ 13
    2.2.1 ADS-B Manufacturers ............................................................ 13
    2.2.2 Congress ............................................................................... 14
    2.2.3 Customers .............................................................................. 14
    2.2.4 Labor Unions ......................................................................... 14
  2.3 Stakeholder Tensions ........................................................................... 14
    2.3.1 Congress and FAA ................................................................. 14
    2.3.2 FAA and Airline Companies ................................................ 15
    2.3.3 FAA and ARTCC ................................................................. 15

3.0 Problem and Needs Statement ........................................................................ 15
  3.1 Gap Analysis ......................................................................................... 15
  3.2 Problem Statement ............................................................................. 16
  3.3 Win-Win Analysis .............................................................................. 17
  3.4 Need Statement .................................................................................. 17

4.0 Mission Requirements ...................................................................................... 17

5.0 Design Alternatives ......................................................................................... 18
  5.1 Hashing .............................................................................................. 18
  5.2 Symmetric Encryption ..................................................................... 19
  5.3 Asymmetric Encryption .................................................................. 19

6.0 Value Hierarchy ............................................................................................... 21

7.0 Design of Experiment .................................................................................... 21
  7.1 Signal Security .................................................................................. 22
  7.2 Feasibility Analysis ........................................................................... 22
  7.3 Average Time in Flight .................................................................... 23
    7.3.1 Formulas ............................................................................... 26
    7.3.2 Results .................................................................................. 27
  7.4 Collision Risk ................................................................................... 31
    7.4.1 Results .................................................................................. 32
    7.4.2 Formulas ............................................................................... 33
Table of Figures
Figure 1: Number of People Flying Each Year in the US (11) ........................................ 5
Figure 2: United States Air Carriers Fleet (11) .................................................................. 6
Figure 3: How ADS-B Works ................................................................................................. 8
Figure 4: ADS-B Message Format ....................................................................................... 9
Figure 5: Ghost Aircraft Flooding .......................................................... Figure 6: Ground Station Flooding .......... 10
Figure 7: Threats to NextGen Airspace System & ADS-B .................................................... 11
Figure 8: Gap Analysis ........................................................................................................ 16
Figure 9: Hashing Example .................................................................................................. 19
Figure 10: Asymmetric Encryption Example ....................................................................... 20
Figure 11: Value Hierarchy ................................................................................................. 21
Figure 12: Simulation Diagram ............................................................................................ 22
Figure 13: Airspace Throughput Simulation Diagram .......................................................... 24
Figure 14: Conceptual Airspace Grid with Cell Capacities .................................................. 25
Figure 15: Airspace Grid with Attacks ................................................................................ 26
Figure 16: Flight Demographics .......................................................................................... 28
Figure 17: Flight Density per Day ....................................................................................... 29
Figure 18: Flight Times for Encryption vs. Hashing (2014) .................................................. 30
Figure 19: Flight Times for Encryption vs. Hashing (2032) .................................................. 30
Figure 20: Collision Simulation Diagram ............................................................................ 31
Figure 21: Number of Collisions in 1,000,000 Iterations .................................................... 32
Figure 22: Utilities for Each Design Alternative .................................................................. 34
Figure 23: Utility vs. Cost .................................................................................................... 35
Figure 24: Gap Analysis Revisited ..................................................................................... 36
Figure 25: Work Breakdown Structure .............................................................................. 38
Figure 26: Total Budget ...................................................................................................... 41
Figure 27: Cost and Schedule Performance Index Graph .................................................... 41
Figure 28: Project Plan ........................................................................................................ 42

Table of Tables
Table 1: Collision Simulation Results .................................................................................. 33
Table 2: Additional Costs per Minute (17) ....................................................................... 35
Table 3: Additional Costs for Extra Time Spent in Flight .................................................. 36
Table 4: Project Risks ......................................................................................................... 43
1.0 Context Analysis

1.1 Increase in Air Transportation

Since the year 2000, there has been a steady increase in the number of people flying each year. Currently, there are over 150 million people flying in the United States both domestically and internationally. By the year 2032, it is estimated that over 250 million passengers will be flying in the United States. With the increase in the number of people flying each year, there is an increased need for more airplanes to meet the demand of flying passengers. Currently, there are a total of over 6000 airplanes that make up the fleet for all United States air carriers. It is estimated that by the year 2033, there will be over 7000 airplanes that will make up the United States air carrier fleet (11). With the increase in passengers flying and the increase in the number of airplanes that will be used to carry these passengers, there will also be an increase in air traffic. More and more airplanes will be in the skies and there will be a need for a better way to track and monitor aircraft to maintain efficiency and safety in the United States airspace.

![Number of Passengers (Millions)](chart)

Figure 1: Number of People Flying Each Year in the US (11)
As air transportation and air traffic increases, so does the need for better and more efficient air traffic surveillance systems. Surveillance is defined as the close observation and monitoring of changing information and it is needed in air transportation systems to track and monitor flights in order to maximize safety and efficiency in the air space. The first type of air traffic surveillance was invented in the mid twentieth century and is known as primary surveillance radar. Primary surveillance radar was originally developed to keep track aircraft locations in the sky. The problem with primary surveillance radar was that it could only provide information about a target’s location to the Air Traffic Controller, but not the target’s identity. The need to be able to determine a target’s identity led to the creation of the secondary surveillance radar. Initially known as Identification Friend or Foe, this surveillance radar was developed during the Second World War and used to distinguish friendly aircraft from enemy aircraft. Secondary surveillance radar is attached to primary surveillance radar and works in conjunction with primary radar.
to identify and track aircraft. The problem with secondary surveillance radar is that it is expensive to maintain and does not provide coverage over oceanic areas.

1.3 Next Generation and Automatic Dependent Surveillance Broadcast (ADS-B)

With increased air travel of both passengers and goods and an increased need for airspace safety and more precise aircraft tracking, the FAA has proposed a new framework for flight tracking and monitoring that will eventually replace the current national airspace system. This new framework is called Next Generation, or NextGen. The major component in NextGen is ADS-B, or Automatic Dependent Surveillance Broadcast. ADS-B consists of two major components: ADS-B IN and ADS-B OUT. ADS-B IN allows aircraft to receive information transmitted from ground stations and other aircraft, while ADS-B OUT allows aircraft to transmit properly formatted ADS-B messages to ground stations and other aircraft. By the year 2020, ADS-B will be used alongside primary and secondary radar in areas still using radar surveillance and on its own in areas that do not use other air traffic surveillance systems. Unlike primary and secondary surveillance radar systems that are ground based, ADS-B is a satellite-based technology that uses the Global Positioning System (GPS) to determine the location of aircraft. As the location of the aircraft is determined and updated, information about location and position will be sent to both the Air Traffic Controller and the pilot in the cockpit. With ADS-B, location data for each individual aircraft is updated every second, as opposed to every 12 seconds with current radar surveillance systems. Given this information, the air traffic controller will be able to give better instructions to the pilot in the aircraft regarding landing, takeoff, or course adjustment, as well as more updates about weather conditions. In addition to providing more precise information, the implementation and maintenance of ADS-B will be significantly cheaper than that of the primary and secondary radar systems (6). Other advantages of ADS-B include surveillance coverage in areas without primary or secondary radar coverage, real
time broadcast of information, increased situational awareness for both the pilot and the air traffic controller, and the potential to decrease the separation distance between aircraft.

Figure 3: How ADS-B Works

Figure 3 shows how ADS-B surveillance systems work. ADS-B works by receiving location information from GPS and then constantly broadcasting that information to other aircraft and ground stations.

1.4 ADS-B Messages

ADS-B messages are transmitted via 1090 MHz data links. The messages are 112 bits long. The first five bits contain the downlink format, which indicates the type of message. The next three bits contain information about the capability of the Mode S transponder. The next 24 bits of data contain information about the aircraft address; these 24 bits of data are unique for each aircraft. Following the aircraft address information is the ADS-B data field, which is 56 bits long. These 56 bits of data include information about aircraft identity, position, and velocity. The final 24 bits of information include a parity check that detect and correct transmission errors in the messages (12). Currently, ADS-B messages are unencrypted and therefore unsecure.
1.5 Threats to ADS-B

With the introduction of ADS-B, the aviation industry has stepped into cyberspace. Airplane connectivity has been increased, meaning that airplanes are now exchanging more data between each other as well as between ATC centers. With the rapid exchange of time-sensitive data and no security measures to protect it, the global aviation system is “a potential target for large-scale cyber attacks” (10).

The signals that are being transmitted by ADS-B IN and OUT are public and the frequency used is well known. As a result the signals can easily be jammed or spoofed. Jamming is the forceful disruption of a signal. A jammer creates a powerful signal that interferes with the original signal and significantly reduces signal to noise ratio (SNR). As a result, the original signal cannot be properly detected (12). There are a few types of possible jamming attacks. These are “ghost aircraft flooding” and “ground station flooding.” “Ghost aircraft flooding” attack creates multiple fake aircraft on screens of the ATC center as seen in Figure 5. These fake aircrafts are travelling from a random point A to a random point B. Because of the large number of the airplanes displayed, the ATC controller can no longer differentiate between the real and fake flights.

“Ground station flooding” creates the opposite scenario. The receiver of ADS-B messages is being jammed by creating noise and results in all ADS-B messages being destroyed. In this type of attack, the ATC center now has no aircraft displayed on its screens.
Another potential type of attack is spoofing. The goal of a spoofing attack is to insert a message or a group of messages that will give the ATC center incorrect information about the current situation of flights in the air. This is achieved by inserting counterfeit messages that appear to be almost identical to the real ones, except with a slightly more powerful signal. Spoofing attacks are very difficult to detect, and as a result, they’re also very dangerous because the ATC will respond to the fake signals instead of the real signals, causing pilots to react as if they were in different locations, locations based on the false messages sent to the ATC by attackers. Spoofing attacks can create either a “false source,” “false content” or “false timing.” A “False source” attack creates signal that is identical to a real signal, but looks like coming from a different location. This creates a ghost plane or planes on ATC screen. A “False content” attack “captures” the message, changes and retransmits it. In this type of attack, the airplane location or altitude would be shown incorrectly on ATC center screen. “False timing,” also called “meaconing,” “catches” the message, alters the timing and retransmits it without changing anything else, thus sending incorrect information about speed and location to the ATC screen (13). Both “false timing” and “false content” have the same end result, an incorrect position of aircraft is being shown on the ATC screen.

GPS signals can also be spoofed. However, these types of attacks are not only difficult to implement, but they also require very costly equipment that can move as
fast the aircraft in order to be able to catch and alter GPS signals. Therefore, GPS signal spoofing will not be in the scope of our project.

The system diagram below shows vulnerability points, highlighted in red. Threats related to transmissions to from GPS to aircraft are not addressed because they are not part of our project scope.

Figure 7: Threats to NextGen Airspace System & ADS-B

This project will only be examining spoofing attacks because jamming attacks cannot be prevented, only detected.

1.6 Scope

This project considers the commercial aviation airspace over the open waters of the Gulf of Mexico, where there is no radar coverage and ADS-B signals are subject to more spoofing attacks. Furthermore, the project will only consider en route flights. The project will only be focusing on preventing spoofing attacks, as opposed to preventing and mitigating the effects of the attack.
2.0 Stakeholder Analysis

2.1 Primary Stakeholders

2.1.1 Federal Aviation Administration

The Federal Aviation Administration, or the FAA, is a government office whose primary mission is to “provide the safest, most efficient aerospace system in the world” (7). The FAA establishes the rules and regulations for the airspace of the US. The FAA created the Surveillance and Broadcast program office specifically to oversee the transition from the radar surveillance system towards ADS-B system. The FAA’s major responsibilities include “regulating civil aviation to promote safety, encouraging and developing civil aeronautics, developing and operating a system of air traffic control and navigation for both civil and military aircraft, researching and developing the National Airspace System and civil aeronautics, developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation, and also regulating U.S. commercial space transportation” (8).

2.1.1.1 Air Traffic Organization

The primary function of the Air Traffic Organization is to move air traffic safely and efficiently. The ATO is responsible for the safety of more than 50,000 flights each day and over 600 million people each year.

2.1.2 Air Route Traffic Control Center

The primary objective of the Air Route Traffic Control Center (ARTCC) is to maintain the safety and efficiency in a specified volume of airspace in high altitudes. Employees at the ARTCC use radar screens to monitor and track aircraft. With access to this type of information, employees are able to safely guide aircraft at high altitudes. Because the ARTCC is responsible for planning all of the air traffic for the United States and are responsible for the lives of the people using air transportation,
they expect the air traffic control system to be able to transmit the information quickly and reliably between the plane and the ARTCC center. Once the ADS-B system is fully implemented, the ARTCC will be directly impacted by the changes brought about because of ADS-B. With the implementation of ADS-B, employees at the ARTCC will have to learn how to use new equipment installed for ADS-B as well as learn how to use the system in order to make more efficient use of the air space.

2.1.3 Airline Companies

The main objective of the airline companies is to operate the aircraft and safely transport the passengers between their destinations, as well as earn enough profit to stimulate company growth. The owners of the airline companies will have to invest in equipping their aircraft with FAA approved equipment such as ADS-B by 2020.

2.1.4 Crew and Pilots

The crew of the aircraft, in particular captains and their first officers, are the ones who actually control the airplane. As the plane control systems are more computerized, they are mostly monitoring the instruments. They are relying on the ADS-B system and the ATC to provide them with reliable information regarding the positioning of the nearby aircraft and the necessary instructions of course adjustment.

2.2 Secondary Stakeholders

2.2.1 ADS-B Manufacturers

The primary objective of ADS-B manufacturers is to provide aircraft with reliable hardware that complies with FAA specified regulations. They need to create better technology that will provide both pilots in the aircraft and also people in the ARTCC with more information about aircraft in the sky.
2.2.2 Congress

Congress is the bicameral legislature of the United States federal government. It is comprised of the House and the Senate. The United States Congress is responsible for reviewing and approving all spending that occurs within the Federal Aviation Administration. Congress has the final say over the proposed budget for both ADS-B and NextGen.

2.2.3 Customers

Customers include passengers of commercial aircraft as well as companies using aircraft to transport their cargo. They do not explicitly use the ADS-B system, but they rely on ADS-B system, ARTCC and aircraft crew to safely get them or their cargo from one destination to another.

2.2.4 Labor Unions

Labor unions include both pilot labor unions and ARTCC/Air Traffic Control labor unions. The primary objective of the labor unions is to protect the rights of workers, strive to secure better working conditions for members, and increase workers’ incomes.

2.3 Stakeholder Tensions

2.3.1 Congress and FAA

Congress must approve any rules or regulations that are passed by the Federal Aviation Administration. This means that Congress also must approve of each rule and regulation’s associated budget. Tensions, and consequently conflicts, can arise when the FAA believes that a certain rule or regulation is imperative to air transportation safety, but Congress either does not agree to passing the rule or regulation itself or the proposed budget for it.
2.3.2 FAA and Airline Companies

Airline companies are required to comply with any rules and regulations set by the FAA. As a result, there may be a tension between airline companies and the FAA if the FAA requires the airline companies to pay for the installation of ADS-B as well as any future security software made available for ADS-B.

2.3.3 FAA and ARTCC

The ARTCC must be in compliance with all of the rules and regulations set forth by the Federal Aviation Administration. As a result, each time there is new rule or regulation passed by the FAA, the ARTCC has to make adjustments to their procedures accordingly. Tensions between the FAA and ARTCC can arise when the ARTCC believes the FAA is proposing rules and regulations at rate that is either difficult to keep up with or significantly increases the workload of the ARTCC employees.

3.0 Problem and Needs Statement

3.1 Gap Analysis

As of right now, the En Route Traffic Control Centers in the United States are responsible for overseeing approximately 40 million aircraft each year. By the year 2032, they will be responsible for handling over 60 million aircraft each year (11). In order to do this, the capacity and efficiency of the airspace must be increased so that the controllers can handle the increase in the amount of aircraft they oversee each year. These numbers have been scaled down, based on our data collection and simulation, to reflect the number of airplanes flying over the Gulf of Mexico. In our project, we would like to bridge the gap between today’s airspace capacity and that of the year 2032 by increasing the airspace capacity by 32%. This will be done by
securing ADS-B signals so that they can be used as the primary source of flight information and decrease the separation distance between aircraft.

3.2 Problem Statement

ADS-B signals are unencrypted. Consequently, the signal communications between the Air Route Traffic Control Center and aircraft are not secure. Because of this, adversaries or anyone with enough knowledge, skills, and some relatively cheap equipment or software can spoof the signals. If the signals are spoofed, they are no longer trustworthy or reliable. If the signals are unreliable, the Air Traffic Controllers cannot know the location of the aircraft with 100% certainty. Spoofed signals have the potential to reduce situational awareness, threaten flight safety, and ultimately reduce airspace capacity because airplanes will have to maintain a greater separation distance. If the airspace capacity is reduced, then the airspace efficiency is also decreased.
3.3 Win-Win Analysis

In a win-win scenario, there will be a solution to secure ADS-B signals. The solution will be cost effective so it is affordable enough for airline companies to pay for. The solution will be available by 2020, the same year that all airplanes will be required to have at least ADS-B Out installed. The solution will secure the signals and the signals will be reliable enough for ARTCC to trust and use to decrease the separation distance between aircraft. Once the separation distance is decreased, airspace capacity will be increased because there can be more aircraft in any given volume of airspace. Passengers will also benefit from the decrease in separation distance because it would result in shorter flight times and shorter delays. Finally, in a win-win scenario, airline companies would benefit from decreased separation distances because it would mean spending less money on fuel.

3.4 Need Statement

Air travel has been an increasingly popular way to travel in the US and abroad. With the increase in the number of passengers that use air transportation, the risk potential is also increasing. The number of airplanes that are in a certain airspace at any given time is increasing steadily and as a direct result the ARTCC center needs to be even more precise with their directions and timing. In order to increase airspace capacity and efficiency, there is a need for a system that prevents spoofing attacks on ADS-B signals sent from aircraft to ARTCC and between aircrafts. Mitigating spoofing attacks would result in more reliable signals and ultimately a more efficient airspace.

4.0 Mission Requirements

1.0 The system shall decrease the separation distance to 5 NM.

1.1 The system shall not increase the time spent in flight by more than 1 minute.
1.1.1 ADS-B messages shall be resistant to spoofing attacks 75% of times.
1.1.2 The system shall maintain a collision rate of 22.5 per 1,000,000 flights.

2.0 The system shall be ready to be implemented by 2020.

5.0 Design Alternatives

In order to detect and prevent spoofing attacks on ADS-B based data communication signals, the following techniques are being proposed: hashing, symmetric encryption, and asymmetric encryption. The other alternative is to maintain the status quo by doing nothing.

5.1 Hashing

The primary goal of hashing is to confirm the identity of the source of a message. This is achieved by creating a hash that is attached at the end of the message. A hash is a digest of a message created by running a hashing algorithm by the sender. This digest is verified at the receiver’s station by running the same algorithm and deriving the hash independently. The computer at the receiver’s station then compares the received digest to the independently derived digest. If both of them are identical, then the message can be considered authentic. Hashing algorithms run very quickly and only require a software upgrade. However, it will require usage of additional bits in ADS-B message that are fully used right now. A possible compromise would be to free any 8 bits that are currently being used.
5.2 Symmetric Encryption

Encryption is the conversion of plain text to cipher text by implementing various algorithms. Running an encryption algorithm on a message will scramble it and make it look illegible. However, if the receiver knows the right algorithm and key, the message can be decrypted. A key is used to encrypt and decrypt messages. The main goals of encryption are ensuring confidentiality, non-repudiation, authenticity, and integrity. Confidentiality insures that only the sender and the intended recipient can see the message. Non-repudiation is the ability of the encryption algorithm to provide proof of the message’s source. Authenticity confirms the identity of the sender. Integrity refers to the content of the message and the accuracy of the information sent in the message (15).

For symmetric encryption, each entity has a secret key and uses this key to encrypt ADS-B messages. The receiving entities also have access to these keys and use the keys to decrypt the message. Symmetric encryption relies on the strength of the key and the reliability of the key exchange process. A strong symmetric encryption will have a long key as well as a secure system for key exchanges. The implementation of symmetric encryption will require software upgrade with no additional hardware.

5.3 Asymmetric Encryption

Asymmetric encryption is very similar to symmetric. However, asymmetric encryption entitles each entity to two keys – private and public. The public key is known to everyone while the private key is only known to a particular entity. Both
keys are mathematically dependent on each other. The message that is being sent from entity A is being encoded by the private key of A, and then encoded again with the public key of receiving entity B. Then, the message is being transmitted through public space until entity B receives it. Entity B will then decode the message by using its private key first and then decode it by using A’s public key. The decrypted message is then received at B.

![Diagram of asymmetric encryption process](image)

**Figure 10: Asymmetric Encryption Example**

Asymmetric encryption does not have the security issue of key exchanges like the symmetric encryption, but this alternative still has to have a way to share all public keys between entities. This alternative will also require knowing the recipient before sending the message, similar to secondary radar, which might degrade the positive factors of ADS-B real time location data.
6.0 Value Hierarchy

Figure 11 represents the value hierarchy for this system. Design alternatives will be evaluated using this value hierarchy. Collision risk is the probability of a collision occurring in a cell under attack. Signal security is the strength of the signal. Economic implications include additional time spent in airspace, extra fuel burn, and consequently extra costs. Feasibility includes availability of technology to implement the alternatives, the time it takes to install the different alternatives, and how well the additional requirements for each alternative are met. The weights for each attribute were determined using the method of swing weights based on a ranking of the attributes by a subject matter expert.

7.0 Design of Experiment

The goal of the experiment is to verify the ability of the system to perform in adverse conditions and explore the economic and physical implications of the system. Through the simulations, we were able to calculate scores for each attribute in the value hierarchy for each alternative. Figure 12 is a diagram of the simulations used in this system.
7.1 Signal Security

The goal of the signal security analysis is to determine the relative strengths of each of the design alternatives. The reliability rate for hashing was determined through research. This rate is 50%, meaning that adding a hash to the end of an ADS-B message effectively allows the receiver to verify the sender of the message 50% of the time. Using this value, we were able to determine reliability rates for symmetric and asymmetric encryption by comparison. Symmetric encryption was determined to have a reliability rate of 85% because of security concerns about a key management system. Asymmetric encryption was determined to have a reliability rate of 99%. This is because there is a small possibility of undetected message errors that can lead to false attack detection. The undetected message error in transmissions was determined from the signal analysis. These values were then used to give each alternative a signal security score for each of the alternatives.

7.2 Feasibility Analysis

The goal of the feasibility analysis was to determine the feasibility of implementing each of the design alternatives. The feasibility of each alternative was
evaluated using execution time, availability of technology, and any additional requirements. The execution time for each alternative turned out to be negligible since ADS-B messages are very small and do not require a lot of time to be encrypted or have a hash attached. Each of the design alternatives require technology that is already available and in use. Each of the design alternatives has additional requirements. Since hashing is like an addendum to a message, it requires additional bits. At least eight extra bits are required for a hash. It could be possible to add a hash on an ADS-B message if the number of bits used in the parity check (the last 24 bits of an ADS-B message) is decreased a little bit. Another way to attach a hash would be to separate the message into several smaller messages with less information in each message. Symmetric encryption requires the implementation of encryption software as well as a secure key management system. Asymmetric encryption will require software upgrades on ARTCC and aircraft computers. The problem with this type of encryption is that it requires the use of keys that are too long for ADS-B messages. While there are additional requirements for each alternative, all of them are technically feasible and each received a score of 1 for feasibility.

7.3 Average Time in Flight

The goal of the average time in flight attribute is to see if there is a difference in average time in flight between each of the design alternatives. If there is a difference in time, the additional time and implications will be examined more closely. The airspace throughput simulation will be used to determine the throughput, capacity, and additional time in flight. The simulation is based on a conceptual grid over the Gulf of Mexico. The grid is 600 by 400 miles and represented by 600 cells, each sized 20 by 20 nautical miles. The conceptual grid is 30 cells across and 20 cells down. Inputs to this model are aircraft departure streams, aircraft velocities, attack locations, and separation distances. The aircraft departure streams were determined from real world departure data collected for the eight major Class B airspace airports around the gulf: Miami International
Airport, Tampa International Airport, Louis Armstrong New Orleans International Airport, Orlando International Airport, Cancun International Airport, William P. Hobby Airport, George Bush Intercontinental Airport, and Benito Juarez International Airport. The data for departure streams was collected for each hour of the day and used as inputs in uniform distribution. Aircraft velocity was inputted into the simulation in a triangular distribution. After running the simulation under normal conditions (i.e. no attacks and perfect avoidance), we looked at the number of aircrafts going through each cell during the whole day and determined the cells with the most traffic. Once the busiest cells were identified, we blocked off these cells and made them “attacked cells.” Attacked cells are already at full capacity, which means that any aircraft that is trying to go through those cells must reroute their paths to avoid the attacked cells. The simulation was run under normal and attack conditions for the year 2014 and the year 2032 (with a 32% increase in air traffic). For the year 2014, the separation distance was 20 NM, which is based on a one-in-one-out system. For the year 2032, the separation distance was 5NM, which is the smallest separation distance that ADS-B allows for. The outputs of this simulation were the average time in flight for all routes, the number of planes at each cell at any given time, and the total throughput of the airspace. Figure 13 represents the airspace throughput simulation.

Figure 13: Airspace Throughput Simulation Diagram
There were several assumptions for this model. The capacity of the cells accounts for altitudes ranging from 29,000 to 41,000 feet. However, we also assumed that while in flight, all aircraft maintain the same altitude. For symmetric and asymmetric encryption, we assumed that any attacks will be mitigated and aircraft can proceed through the airspace just as they would under normal conditions. For hashing, since the reliability rate was low, we assumed that if there was a spoofing attack, it is not likely that it would be mitigated or detected and therefore the aircraft would have to avoid the cells where the attack happened.

The simulation was first run under normal conditions to determine the location of the busiest cells. Figure 14 depicts the traffic through each of the cells in the airspace.

![Figure 14: Conceptual Airspace Grid with Cell Capacities](image)

The red cells have more than 300 flights that go through it each day; the yellow cells have between 100 and 300; the green cells have less than 100; the blue cells are not used at all. From this image, we were able to identify two clusters of cells and block them off for the attack scenarios.
Figure 15 shows the cluster of attacked cells in black. These cells are the busiest cells in the grid because they have most traffic as they are near multiple major airports. We assumed that flights that would have to be rerouted around the busiest areas would have the biggest impact on flight times. To examine the difference in flight times for hashing, the simulation was run with the attacked cells blocked off. This means that these cells could not be used and any flight going through these cells would have to reroute, thus adding additional time to the flight. For symmetric and asymmetric encryption in both 2014 and 2032, the simulation is run under normal conditions and has the same average flight times and throughput as the control scenario.

7.3.1 Formulas

The following formulas were used to evaluate various parts of the system.

- Dot Product - This accounts for the slope and direction of the flight path.

\[ Dot_{prod} = \frac{\vec{V}_{curr\rightarrow target} \cdot \vec{V}_{plan\rightarrow target}}{\|\vec{V}_{curr\rightarrow target}\| \cdot \|\vec{V}_{plan\rightarrow target}\|} \]
• Time to Cross One Cell – This formula is used to calculate the time spent in each cell. The distance across each cell (20 NM) is divided by the velocity of the airplane.

\[ T = \frac{D_{cell}}{V} \]

**7.3.2 Results**

After all of the simulations were run, we were able to determine the total throughput of the airspace, most popular flight routes, average time in flight for each route, and the capacity of each cell at any given time.
<table>
<thead>
<tr>
<th>Most Common Flights (Top 20%, 15-64 flights/day)</th>
<th>2014</th>
<th>2032</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miami-Los Angeles</td>
<td>938</td>
<td>1332</td>
</tr>
<tr>
<td>Houston-Miami</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-Dallas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-San Francisco</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orlando-Dallas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-Houston</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampa-Dallas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cancun-Atlanta</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-New Orleans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-Houston</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami-Mexico</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico-Miami</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico-Atlanta</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Houston-Orlando</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 16: Flight Demographics

Figure 16 shows the top 20% of the most popular routes. These flight paths have between 15 and 64 flights going through each day.
Figure 17 shows the flight density for each route per day for 2014 and 2032.

From the airspace throughput simulation, we were also able to determine the average time in flight for each of the design alternatives for the years 2014 and 2032. Figure 18 shows the average additional time spent in flight during attack scenarios in the year 2014. For the year 2014, the average time in flight under attack scenarios with hashing was 58.891 ± 3.988 minutes. For symmetric and asymmetric encryption and the control scenario, the average time spent in flight was 52.683 ± 3.668 minutes. For the year 2032, the average time spent in flight under attack scenarios with hashing was 56.844 ± 3.824 minutes. For symmetric and asymmetric encryption and the control scenario, the average time spent in flight was 52.161 ± 3.547 minutes. Each of these average time intervals was calculated using a 95% confidence interval. From the results of the airspace throughput, it was determined that there is significant difference between the time spent in flight with hashing and symmetric or asymmetric encryption.
Figure 18: Flight Times for Encryption vs. Hashing (2014)

Figure 19: Flight Times for Encryption vs. Hashing (2032)

Figure 18 shows the average additional time spent in flight during attack scenarios for the year 2014. Figure 19 shows the average additional time spent in flight during attack scenarios for the year 2032. There was a slight decrease in time
spent in flight in 2032. This is most likely because of the decreased separation distance.

### 7.4 Collision Risk

The goal of the collision simulation is to determine the probability of collision in attacked cells. In this model, it was assumed that the cell is under attack and planes going across this cell have no situational awareness. The conceptual model is one cell that is 20 by 20 NM. This cell is 12,000 feet in height with 12 flight levels given that there is a 1000 feet vertical separation distance for aircraft. The inputs to this simulation are the number of flights in the cell, random velocities, random entry points, and random exit points. At the start of this simulation, a set number of flights are randomly generated. Each flight has a random entry and exit point generated. As soon as the aircraft is randomly generated, it proceeds to fly to its exit point. If at any point, two planes get closer than 102 feet (the length of a Boeing 737) of each other and these planes are in the same flight level, a collision is registered. This simulation continues for 1,000,000 iterations. The output of this simulation is the number of iterations that had a collision out of 1,000,000 iterations. Figure 20 shows the diagram for the collision simulation.
7.4.1 Results

The collision simulation was run 30 times for each number of flights. The number of collisions per 1,000,000 iterations for each number of flights is depicted in the graph in Figure 21. We used these numbers to determine the collision risk for the system for each of the alternatives. Cells that are not under attack have a collision risk of zero. After the both the collision and airspace throughput simulations were run, we determined the number of airplanes that used the attack cell in the scenario as well as the number of airplanes in the cell at any given time. Using the number of flights in each cell and the number of collisions out of 1,000,000 we were able to determine the collision risk for each design alternative. The probabilities of collision for each cell were then summed together to get the total collision risk for the whole grid. The probability of collisions for each of the design alternatives is depicted in Table 1. The probability of collision for both types of encryption is zero because attacks are assumed to be fully mitigated.

![Figure 21: Number of Collisions in 1,000,000 Iterations](image-url)
### 7.4.2 Formulas

The following formulas were used in the collision simulation.

- Distance at time $t - x_{current} = \frac{v}{\sqrt{1+m^2}} + x_{previous}$

- Current Y Coordinate - $y_{current} = m(x_{current} - x_{previous}) + y_{previous}$

- Distance Between Two Points - $D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$

- Collision Risk - $CR = (P(\text{collision}) \times N_{cell}) \times 100\%$

### 8.0 Results and Recommendations

#### 8.1 Results

Figure 22 shows the utilities of each of the design alternatives. The utilities of each alternative was calculated using the following equation derived from the value hierarchy: $U(x) = 0.1266W_x + 0.1899W_f + 0.3038W_e + 0.3797W_c$.

Asymmetric encryption has the highest utility followed closely by symmetric
encryption. Figure 23 is the utility versus cost graph. The cost of implementation for each of the design alternatives was not readily available and as a result we were forced to make some assumptions. According to the FAA, it is estimated that about $4 billion will be spent on the implementation of ADS-B through the year 2032 (16). Using this information, we assumed that the cost of implementing ADS-B in the Gulf would be proportional to the number of flights flying over the Gulf compared to the number of total flights in the United States. We scaled down the cost to 10%. Using the new scaled down cost, we assumed that the cost to implement hashing algorithms on ADS-B signals would be between 5% and 10% of the cost of ADS-B implementation. Similarly, we assumed that the cost to implement symmetric or asymmetric encryption would be between 10% and 20%.

**Ranking for OVERALL Goal**

<table>
<thead>
<tr>
<th>Alternative</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric Encryption</td>
<td>0.834</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>0.817</td>
</tr>
<tr>
<td>Hashing</td>
<td>0.726</td>
</tr>
<tr>
<td>Maintain Status Quo</td>
<td>0.395</td>
</tr>
</tbody>
</table>

![Utility Graph](image)

*Preference Set = NEW PREFER. SET*

Figure 22: Utilities for Each Design Alternative
Figure 23: Utility vs. Cost

Using the average time in flight and the data in Table 2 from Airlines for America, we calculated the total costs for flights over the gulf as well as any additional costs due to additional time spent in flight. Table 3 depicts the total additional costs for each design alternative. These costs were calculated by multiplying the number of flights per year by the time spent in flight by the total additional cost per minute. The total costs and additional costs are depicted in Table 3.

<table>
<thead>
<tr>
<th>Calendar Year 2012</th>
<th>Direct Aircraft Operating Cost per Block Minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel</td>
<td>$39.26</td>
</tr>
<tr>
<td>Crew - Pilots/Flight Attendants</td>
<td>16.26</td>
</tr>
<tr>
<td>Maintenance</td>
<td>12.02</td>
</tr>
<tr>
<td>Aircraft Ownership</td>
<td>7.92</td>
</tr>
<tr>
<td>Other</td>
<td>2.71</td>
</tr>
<tr>
<td>Total DOCs</td>
<td>$78.17</td>
</tr>
</tbody>
</table>

Table 2: Additional Costs per Minute (17)
From the table above it can be seen that using symmetric or asymmetric encryption will incur no additional costs because there was no additional time spent in flight, according to the airspace throughput simulation. Hashing will incur significant additional costs because there will be extra time spent in flight.

After the airspace throughput simulation was run for the years 2014 and 2032, the total throughput for each year was determined. In 2014, an average of 938 flights crossed the Gulf of Mexico per day and 342,370 flights crossed per year. In 2032, an average of 1332 flights crossed the Gulf per day and 486,180 crossed it per year. Looking at the gap analysis, our system bridges the gap by 96%. It estimated that approximately 506,000 flights over the Gulf will be handled by en route traffic control centers in 2032. Our simulation estimates that the airspace will be able to handle 486,180 flights per year, resulting in a 96% gap bridge.

Table 3: Additional Costs for Extra Time Spent in Flight

<table>
<thead>
<tr>
<th>Year</th>
<th>Status Quo – Total Cost per Year</th>
<th>Encryption (Symmetric &amp; Asymmetric) - Additional Spending</th>
<th>Hashing - Additional Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>$1,409,950,237</td>
<td>+0</td>
<td>+$44,834,140-$287,488,121</td>
</tr>
<tr>
<td>2032</td>
<td>$1,982,344,674</td>
<td>+0</td>
<td>+$12,124,185-$343,841,991</td>
</tr>
</tbody>
</table>

Figure 24: Gap Analysis Revisited
8.2 Recommendations

Based on the analysis of data and the simulations, it is recommended that encryption, and in particular symmetric encryption, should be implemented on ADS-B signals because it has a high level of security strength, low probability of collision, acceptable feasibility, and least time spent in flight. This alternative has the highest utility value of the three alternatives. The security provided by asymmetric encryption will allow for increased situational awareness and will prepare the airspace for the increase in the number of flights in 2032.

9.0 Work Breakdown Structure and Budget

9.1 Work Breakdown Structure (WBS)

A work breakdown structure was created to organize all of the tasks needed to complete this project. Our work breakdown structure is divided into six major categories: Management, Research & Data, ConOps & Requirements, Simulation & Analysis, Documentation, and Reports & Presentations. Below is an image of our WBS.
Figure 25: Work Breakdown Structure
The first category, Management, includes assigning tasks and deadlines for project deliverables, contacting sponsors and setting up meetings with them, general project planning done by the manager, organization of deliverables by the manager, and any revision or rework.

The second category, Research & Data, includes conducting all of the initial research related to ADS-B, aircraft transponders, threats to ADS-B, risks, current radar surveillance systems, stakeholders, and also spoofing and jamming attacks. This category of work also includes data collection and analysis as well as meetings with sponsors.

The third category, Conops & Requirements, includes writing major parts of the Concept of Operations, such as the context analysis, stakeholder analysis, problem statement, needs statement, and requirements.

The fourth category, Simulation/Analysis, includes designing simulations for multiple scenarios, implementing the simulations, performing a tradeoff analysis of alternative solutions, testing, validation, verification, and using results of the simulation to come up with a conclusion and recommendations.

The fifth category, Documentation, includes everything from the initial kick-off deliverables due at the beginning of the Fall 2013 semester to the final conference paper and YouTube video that is due at the end of the Spring 2014 semester.

The sixth and final category of the WBS is Reports and Presentations. This category includes preparing the preliminary project plan and presentation, proposal final report, final report and final report slides.

9.2 Budget

For this project, budget will be calculated based on an hourly rate of $45/hour with an overhead cost of $54/hour for a total billing rate of $99/hour per person. As of right now, we will spend an estimated total of 1,260 hours on this project from the beginning of the Fall 2013 semester until the end of the Spring
2014 semester. The hours spent on the project rely heavily on deliverable due dates and presentation dates. The estimated weekly time spent on the project ranges from ten hours a week, on weeks such as the ones at the end of the spring semester, to sixty-five hours a week, on weeks that there are multiple deliverables and presentations due. Based on these factors, it is estimated that our project will cost $124,740.

9.3 Earned Value Management

Figure 25 shows the planned value, earned value, actual cost, and the best and worst case budgets for this project. According to this graph, we have spent more time and money than we had planned on spending originally. The earned value as of this point is slightly below the planned cost. This figure also shows the best and worst case budgets. The best case budget is a 90% budget and the worst case budget is a 110% budget. In the best case scenario, we would spend about 90% of our planned budget, while in the worst case, we would spend 110% of our planned budget. The best-case budget value is $120,285 and the worst-case budget value is $147,015. At the end of the project, we spent a total of 1392.5 hours and $137,857.50.
Figure 26: Total Budget

Figure 27 depicts our cost and schedule performance indices. According to this, we started our project slightly behind schedule but have gradually caught up to schedule by the 13th week. Our project also started under budget. We were on budget at week 4 and went over budget for the following eight weeks. At week 13, we were close to being right on budget again. Towards week 17, the project was over budget and behind schedule. This trend continued through the end of the second semester.
9.4 Project Plan

Figure 21 shows the project plan. The critical path is marked in red. The critical path consists of deliverables and the simulation.
9.5 Project Risks and Mitigation Techniques

The following table outlines all of the risks in our project by WBS category.

<table>
<thead>
<tr>
<th>WBS Category</th>
<th>Risks</th>
<th>Mitigation Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Management</td>
<td>• Tasks not assigned with correct deadlines</td>
<td>• Assign internal team deadlines several days before official deadlines</td>
</tr>
<tr>
<td></td>
<td>• Deliverables not completed by internal team deadlines</td>
<td>• Continue following up with sponsors</td>
</tr>
<tr>
<td></td>
<td>• Sponsors do not reply after being contacted</td>
<td></td>
</tr>
<tr>
<td>2.0 Research</td>
<td>• Majority of research is not completed by the middle of the Fall semester</td>
<td>• Assign research tasks to each team member so that research findings can be combined</td>
</tr>
<tr>
<td>3.0 Conops &amp; Requirements</td>
<td>• Context Analysis, Stakeholder Analysis, Problem Statement, and Requirements are not complete by Final Project Plan due date</td>
<td>• Make sure that each of these components is about 60% complete by mid-October</td>
</tr>
<tr>
<td>4.0 Simulation</td>
<td>• Not enough data for simulation</td>
<td>• Begin data collection right after Prelim Project Plan due date</td>
</tr>
<tr>
<td></td>
<td>• Data is not collected time for simulation</td>
<td>• Resize scope early in semester</td>
</tr>
<tr>
<td></td>
<td>• Simulation is too complex to be modeled within time frame of this project</td>
<td>• Seek guidance from sponsors</td>
</tr>
<tr>
<td>5.0 Documentation</td>
<td>• Documentation deliverables are not completed by deadlines</td>
<td>• Set internal team deadlines for at least five days before official deadlines</td>
</tr>
<tr>
<td>6.0 Reports &amp; Presentations</td>
<td>• Reports or presentations are not completed by deadline</td>
<td>• Set internal team deadlines for at least five days before official deadlines</td>
</tr>
</tbody>
</table>

Table 4: Project Risks
10.0 References


