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

Sahar Amin, Tyler Clark, Rennix Offutt, and Kate Serenko
George Mason University, samin9, tclark11, roffutt, eserenko@gmu.edu

***Abstract* - The need for increased surveillance due to increase in flight volume in remote or oceanic regions outside the range of traditional radar coverage has been fulfilled by the advent of space-based Automatic Dependent Surveillance – Broadcast (ADS-B) Surveillance systems. ADS-B systems have the capability of providing air traffic controllers with highly accurate real-time flight data. ADS-B is dependent on digital communications between aircraft and ground stations of the air route traffic control center (ARTCC); however these communications are not secured. Anyone with the appropriate capabilities and equipment can interrogate the signal and transmit their own false data; this is known as spoofing. The possibility of this type of attacks decreases the situational awareness of United States airspace. The purpose of this project is to design a secure transmission framework that prevents ADS-B signals from being spoofed. Three alternative methods of securing ADS-B signals are evaluated: hashing, symmetric encryption, and asymmetric encryption. Security strength of the design alternatives is determined from research. Feasibility criteria are determined by comparative analysis of alternatives. Economic implications and possible collision risk is determined from simulations that model the United State airspace over the Gulf of Mexico and part of the airspace under attack respectively. The ultimate goal of the project is to show that if ADS-B signals can be secured, the situational awareness can improve and the ARTCC can use information from this surveillance system to decrease the separation between aircraft and ultimately maximize the use of the United States airspace.** *(Abstract)*

I. Introduction

Since the year 1978, there has been a steady increase in the demand for air transportation each year. As of right now, there are over 150 million people flying in the United States both domestically and internationally [1]. The Bureau of Transportation Statistics estimates that by the year 2032, over 250 million passengers will be flying in the United States [1]. 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 [2]. 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.

A. Primary and Secondary Surveillance Radar

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. There are three types of surveillance used for air traffic control. Primary surveillance radar provides information about a target's distance and azimuth to the Air Traffic Controller, but not the target's identity. Secondary surveillance radar is attached to primary surveillance radar and is able to interrogate a transponder of an aircraft, determining its altitude, latitude/longitude, and flight number. Both primary and secondary surveillance radar are expensive to maintain and have limited coverage radius.

B. NextGen and Automatic Dependent Surveillance Broadcast (ADS-B)

For more precise aircraft tracking the FAA has proposed a new framework 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. 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. 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 is sent to both the air traffic controller and the pilot in the cockpit. This data is transmitted at a rate of once per second, which is an improvement to the 12 second delay of the current system. In addition to providing more frequent and precise information, the implementation and maintenance of ADS-B will be significantly less expensive than that of the primary and secondary radar systems [3]. 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.

C. ADS-B Messages

ADS-B messages are 112 bits long and transmitted via 1090 MHz data links. 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 [4]. Currently, ADS-B messages are unencrypted.

D. Threats to ADS-B

With the introduction of ADS-B, the aviation industry has stepped into cyberspace. With the rapid exchange of time-sensitive data and limited security measures to protect it, the global aviation system is "a potential target for large-scale cyber-attack" [5].

ADS-B signals are public over a known frequency. As a result the signals are vulnerable to spoofing and jamming.

Jamming is the forceful disruption of a signal. While we acknowledge that jamming exists, we will not be finding solutions for these types of attacks because, unlike spoofing, they cannot be prevented, only detected.

Spoofing attacks, on the other hand, are very difficult to detect. The goal of spoofing is to falsify the information transmitted in a message. Two major types of spoofing attacks are "false source" and "false content." A "false source" attack creates signal that is identical to a real signal, but looks like it is coming from a different location. This creates a ghost plane or planes on ARTCC or aircraft screen. A "false content" attack "captures" the message, changes and retransmits it. In this type of attack, the airplane location or altitude are shown incorrectly on ARTCC or aircraft display. For the scope of our project, we will be looking only at spoofing attacks.

E. 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.

II. Stakeholders

A. Primary Stakeholders

- *Federal Aviation Administration* (FAA) - The FAA is a United States Federal Government office whose primary mission is to "provide the safest, most efficient aerospace system in the world" [6], by establishing the rules and regulations for domestic and bordering airspace of the US. The FAA created the Surveillance and Broadcast program office specifically to oversee the transition from the radar surveillance system to the ADS-B system.
- *Air Route Traffic Control Center* (ARTCC) - The primary objective of the 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 aircraft and to safely guide aircraft at high altitudes. Once the ADS-B system is fully implemented, the ARTCC will be directly impacted. ARTCC employees 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.
- *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.
- *Crew and Pilots* - The crew of the aircraft, in particular pilots, are the ones who actually control the airplane. They are relying on the ADS-B system and the ARTCC to provide them with reliable information regarding the positioning of the nearby aircraft and the necessary instructions of course adjustment.

B. Secondary Stakeholders

- *ADS-B Manufacturers* - The primary objective of ADS-B manufacturers is to provide aircraft with reliable hardware that complies with FAA specified regulations. .
- *The Congress* - 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.
- *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.
- *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.

C. Stakeholder Tensions

- *Congress and FAA* - Congress must approve any rules or regulations as well as the associated budgets that are passed by the Federal Aviation Administration. Tensions 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.

- *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.
- *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 a 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 a rate that is difficult to keep up with and significantly increases the workload of the ARTCC employees.

III. 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 [2]. 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. In our project, we would like to bridge the gap between today's airspace throughput and that of the year 2032 by increasing the throughput 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 as a result, the separation distance between aircraft can be decreased.

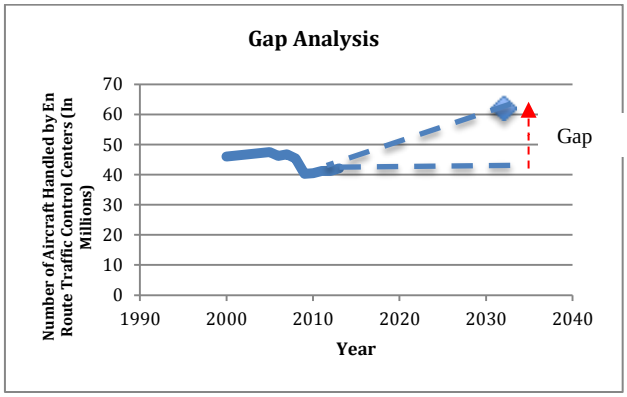

FIGURE 1
GAP ANALYSIS

IV. Problem Statement and Need Statement

ADS-B signals are unencrypted and the signal communications between the Air Route Traffic Control Center and aircraft are not secure. As a result, the signals can be spoofed by adversaries or anyone with enough knowledge, skills, and appropriate equipment or software. Spoofed signals are no longer reliable, and they have the potential to reduce situational awareness, threaten flight safety, and ultimately reduce airspace throughput because airplanes will have to maintain a greater separation distance.

In order to increase airspace throughput 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.

V. Mission Requirements

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

1.1 The system shall not increase fuel burn by more than X.

1.1.1 ADS-B messages shall be resistant to spoofing attacks Y% 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.

VI. 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 and asymmetric encryption. The other alternative is to maintain the status quo by doing nothing.

A. 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.

B. 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 [7].

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.

C. 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.

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.

VII. VALUE HIERARCHY

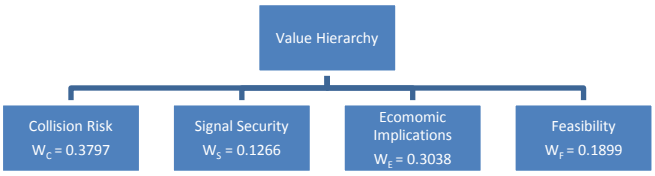

FIGURE 2
VALUE HIERARCHY

Figure 2 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.

VIII. DESIGN OF EXPERIMENT

There are three simulations for this project. There is a signal simulation, an airspace simulation and a collision simulation.

The signal simulation was created first. This simulation has unencrypted ADS-B messages and the design alternatives as inputs. This simulation will be used to determine the reliability and security of the proposed design alternatives.

The reliability factor that will be derived from signal simulation will then be used as an input to the airspace simulation. The other inputs for this simulation will be separation distances between the aircraft, the departure stream, arrival capacities and the speed of the aircraft. The output of the entire simulation will be the changes in airspace capacity that is dependent on separation distance and the reliability of our design alternatives.

The collision simulation uses the number of violations from the airspace simulation to calculate the number of collisions per one million flights.

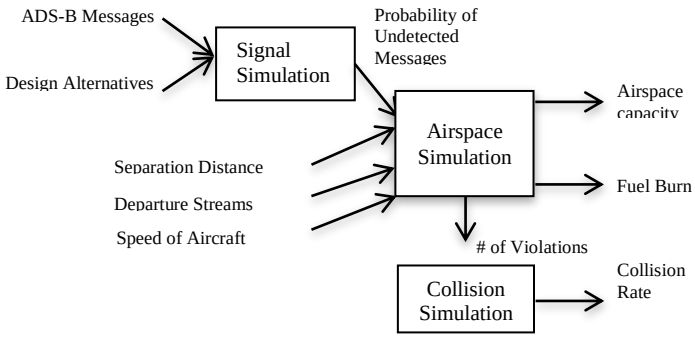

FIGURE 3
SIMULATION BLOCK DIAGRAM

A. Signal Simulation

The signal simulation is processed in RedHawkSDR, which is a software defined radio program designed to simulate real world signals. The signal simulation inputs can be seen in Figure 3. The design alternatives are coded in C++ and python. The signal starts with an encoder/decoder block which is for the receiver and transmitter. After the ADS-B message is synchronized, it is converted from a string to a binary value. The next step is the Cycle Redundancy Check which consists of identifying up to 8 bits of corrupted/missing data. The next step introduces the design alternatives, hashing, symmetric and asymmetric encryption.

The final signal block is the Reed Solomon's block. This final step of the signal process is where all the missing/corrupt bits that were detected by the CRC are replaced from the four burst message. This step ensures all data is salvaged. The output of this simulation shows the undetected message error probability.

B. Airspace Simulation

The airspace simulation is modeled in MATLAB. The economic goal of this simulation is to determine how spoofing attacks impact fuel burn. This simulation abides by FAA rules and regulations, which means both ADS-B In and Out will both be used for communication. In this model, only en route flights over oceanic areas with no ADS-B coverage are being simulated.

The conceptual model will look like a grid. Each grid cell will have a capacity calculated based on the volume and separation distances. The grid is approximately 400 NM by 600 NM, which makes it a 20 by 30 grid, with each individual cell being 20 NM by 20 NM. Entry and exit points to the grid are modeled after major airports around the Gulf of Mexico. The capacity of each airport is modeled after the departure rates of each airport.

The control scenario has no spoofing attacks and all conditions are normal. When an attack occurs, the separation distance will automatically be increased to the standard 20NM as a safety precaution. This decreases the capacity of an attacked cell, which means that if the number of planes in the cell is greater than the current capacity, then any extra planes must immediately move to the closest cell of highest preference level.

The inputs for this simulation are shown in Figure 3. Start and end points for flights are randomly generated and flight paths between these points are straight lines. Once the plane enters the starting cell, it makes a decision about where to go next based on the dot product. The dot product is calculated using the coordinates of the airplane's current cell, target cell, and planned path. At each cell, the dot product is calculated for each of the adjacent cells. The cell with the smallest dot product is chosen as the next cell in the path. This continues until the aircraft reaches its end point. For avoidance, a conflict resolution algorithm is implemented. Given that the radius of ADS-B is 60 NM, an aircraft in a cell can see other planes in the two adjacent cells. After the next cell in the planned path is determined from the dot product, the algorithm checks for any "conflicts" or cells that are over capacity. If there is a conflict or a cell that is over capacity, the algorithm determines which plane has a slower speed and calculates a new route for the slower aircraft. This algorithm continues until all conflicts are resolved. If there is conflict that cannot be resolved, the aircraft will continue on its original planned path, but a violation will be registered. In this simulation, attacks are implemented by decreasing the capacity of air cells. Hashing is simulated by detecting a spoofed signal and notifying the aircraft about the attack. The cell in which the spoofing attack occurs will experience a drop in capacity and cannot be entered. Both symmetric and asymmetric encryptions are simulated in the same way. Encryption mitigates all of the spoofing attacks.

The outputs of this simulation are the number of violations registered, the total throughput of the air space with and without cyber-attacks and mitigation techniques, the total flight time for planned and adjusted paths, and the time in flight for planned and adjusted paths.

The simulation runs flights for Orlando International Airport, Louis Armstrong New Orleans International Airport, William P. Hobby Airport, George Bush Intercontinental Airport, Miami International Airport, Tampa International Airport, Cancun International Airport, and Benito Juarez International Airport between the hours of 12 AM and 12 PM. After the flights were run, the throughputs for each of the grid cells were determined and as ranked high (>200), medium (100-200), and low (<100) throughputs. The six cells with the highest throughputs were blocked off in the attack scenarios. The average time in flight for control and attack scenarios is depicted in the figure below. Overall, the average time spent in flight during an attack scenario increased by 2 minutes.

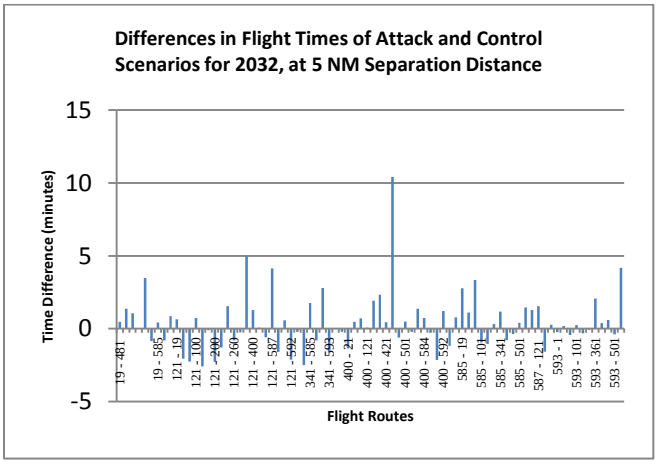

FIGURE 4
DIFFERENCE IN AVERAGE FLIGHT TIMES BY FLIGHT ROUTES

C. Formulas for Airspace Simulation

The following formulas will be used to evaluate various parts of our system.

Dot Product – Accounts for the slope and direction of the flight path.

$$Dot_{prod} = \overrightarrow{V_{curr \to target}} \cdot \overrightarrow{V_{plan \to target}}). \quad (1)$$

Time to Cross One Cell - The time spent in each cell will be calculated by dividing the distance across the cell (20 NM) by the velocity of the airplane.

$$T = \frac{D_{cell}}{V}. \quad (2)$$

Fuel Burn – The amount of fuel consumed by an aircraft in flight.

$$Fuel\ Burn = Fuel_{min}(t_{withAttack} - t_{control}). \quad (3)$$

Collision Risk - Collision risk will be determined by multiplying the probability of collision by the number of violations. This value will then be multiplied by 100% to get a percentage for collision risk. The lower this number gets the better safety our system has.

$$CR = (P(collision) * N_v) * 100\%. \quad (4)$$

D. Collision Simulation

The goal of the collision simulation is to find the probability of collisions in any given cell with varying number of flights assuming that the aircraft do not have situational awareness.

The input in this simulation is the speed and altitude of the aircrafts. Based on the number of flights (x), random starting points are generated along the edges of a single air space cell that is 20 NM by 20 NM by 12,000 feet in height. The same number (x) end points are randomly generated. The 20 NM by 20 NM width was determined from the current separation distance rules which state that in areas without radar coverage, airplanes must maintain a 20 NM separation distance. 12,000 feet is the height of commercial class B airspace.

In addition to maintaining a 20 NM horizontal separation distance, airplanes are also required to maintain a 1,000 feet vertical separation distance. With the current separation rules, the capacity for this air space cell is 12 aircrafts.

With ADS-B signals, the horizontal separation distance can be decreased to 5 NM, while maintaining the same 1,000 feet vertical separation distance. In this case the capacity of the air cell is increased to 48 aircrafts.

For each aircraft, a random velocity and altitude are determined from the triangular distributions of aircraft velocities and altitudes, respectively. The slope of the flight path and the velocity of the aircraft are used together to determine the position of an aircraft at any given time. With each move across the cell, the simulation checks the distances between all planes. If the distance is less than 100 feet (the length of a Boeing 737) and the airplanes are in the same 1,000 feet level, a collision registered.

This simulation runs in sets of one million iterations. In each iteration, every single plane makes a complete path from its starting point to its final destination. The output of this simulation is the number of iterations that had a collision registered. The probability of a collision during attack scenarios was determined by multiplying the throughput of the six cells with the highest throughputs by the collision rate for the appropriate number of flights. The total probability of a collision during an attack scenario is 0.002369. The results for the collision simulation are shown in Figure 5.

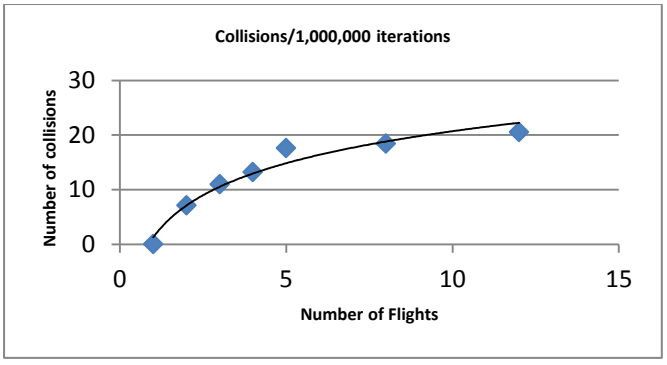

FIGURE 5

COLLISION SIMULATION RESULTS

E. Formulas for Collision Simulation

The following formulas are used in the collision simulation.

Distance at time t

$$x_{current} = \frac{v}{\sqrt{1+m^2}} + x_{previous} \quad (5)$$

Current Y Coordinate

$$y_{current} = m\left(x_{xurrent} - x_{previous}\right) + y_{previous} \quad (6)$$

Distance between Two Points

$$D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (7)$$

IX. Conclusion

Based on the analysis of data and the three simulations, it is recommended that encryption, and in particular symmetric encryption, should be implemented on ADS-B signals because it has the highest security strength, lowest probability of collision, acceptable feasibility, and least economic implications.

Acknowledgment

The authors would like to give special acknowledgement to the individuals who contributed to the completion of this project: Paulo Costa, PhD, Massimiliano Albanese, PhD, Duminda Wijesekera, PhD, representing GMU; Michael Scher, Integrity Applications.

References

[1] *Bureau of Transportation Statistics*, 2012

[2] FAA. "FAA Aerospace Forecast: Fiscal Years 2012-2032." *FAA Aerospace Forecast: Fiscal Years 2012-2032* (2012): 1-115. Print.

[3] McCallie, Donald. Department of the Air Force University. Air Force. Exploring Potential ADS-B Vulnerabilities in the FAA's NextGen Air Transportation System. Print. <http://apps.fcc.gov/ecfs/document/view.action?id=7021694523>.

[4] Jerry T. Chiang and Yih-Chun Hu. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. *IEEE/ACM Transactions on Networks*.

[5] AIAA Decision Paper. "A Framework for Aviation Cybersecurity." *The Connectivity Challenge: Protecting Critical Assets in a Networked World* (2013): n. pag. Print.

[6] "Air Traffic." - *NextGen Briefing*. Federal Aviation Administration, 21 Sept. 2009. Web. 9 Sept. 2013

[7] Skalski-Pay, Jennifer, *Applied Encryption: Ensuring Integrity of Tactical Data* ,SANS Institute InfoSec Reading Room, 2003