CHALMERS

Security Vulnerabilities in Next Generation Air Transportation System

Master of Science Thesis in Computer Systems and Networks

ATANAS ATANASOV

RAMILLO CHENANE

Chalmers University of Technology
Department of Computer Science and Engineering
Göteborg, Sweden, June 2013

Security Vulnerabilities in Next Generation Air Transportation System

Atanas Atanasov
Ramillo Chenane

Examiner: Lena Peterson

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone: +46 (0) 31-772-10-00

Department of Computer Science and Engineering
Göteborg, Sweden 2013

Dedication

All the efforts put in this project are dedicated to God, our dear families, parents, and friends. This project starts a new chapter in our lives that will open many doors in our future success both in professional and educational career. Our family has always been there for us and their guidance has helped us become the people we are today. They will always have our love, gratitude and respect.

Acknowledgements

There are many people we would like to thank for their involvement in the preparation of this thesis. Without their support and encouragement this thesis would have never been completed. First of all, we would like to thank God for giving us the strength and ability to finish this thesis project for our Master's Degree. Second of all, we would like to express our sincere gratitude to our supervisor Lena Peterson for her continuous support, patience, and engagement to this work. Her wisdom and guidance helped us throughout our research and writing of our master thesis. We would also like to thank Professor Tomas Olovsson and Assistant Professor Magnus Almgren for their advice and educational development throughout the Computer Systems and Networks degree program and sharing their ideas and experience with us. We thank our fellow classmate at Chalmers University of Technology for their stimulated discussions, support, and all the fun we had in the past two years. Thanks to our friends in U.S., Kenya, and Macedonia who, in one way or another, contributed to making the research experience so exciting and provided interesting discoveries. Finally, we would like to extend our gratitude to our beloved families and parents who have been our closest allies while working on this thesis. They have set an early example of hard work and inspired us to become better individuals. Their faith and encouragement has given us the strength to pursue our dreams and succeed in life. We thank them for their support, love and understanding.

Abstract

The thesis highlights the importance of Next Generation Air Transportation System (NextGen) as the demand for air transportation has drastically increased over the past few years. NextGen will require a number of changes to the current aviation infrastructure in the United States in order to make it more reliable, environmental friendly, efficient, and technologically advanced. The aviation community would benefit tremendously from NextGen because pilots and Air Traffic Control (ATC) towers will collect data and information in a way not supported by the previously used radar technology.

This thesis points out the security vulnerabilities of Automatic Dependent Surveillance-Broadcast (ADS-B) protocol, which is a vital component for safety of air traffic. Through our research we have elaborated that both active and passive attacks are possible for a sophisticated attacker. Since the current proposed framework poses major security challenges thereby jeopardizing the performance of the future airspace system, we have developed a TVA matrix in order to highlight these concerns. We have studied an abundance of literature from highly ranked security publications in government, industry, and academia on NextGen and ADS-B in order to provide a holistic overview of the security risks and to allow the reader to develop an understanding of such vulnerabilities. In addition, we have proposed additional attacks and mitigation techniques, which we believe have been overlooked in the literature.

To the best of our knowledge the Threats, Vulnerabilities, and Attacks (TVA) matrix developed in this thesis provides a summary of malevolent (e.g. spoofing) data in a unique way never possible before. Even though we have focused on a particular technology, the techniques (e.g. TVA matrix, mitigation) covered here are flexible and can be applied to future technological advancements.

Table of Contents

Acronym List

Acronym	*Definition*
802.11	Wireless Local Area Network
802.15	Wireless Personal Area Network
802.16	Wireless Broadband
1090ES	1090-MHz Extended Squitter
AC	Aircraft Control
ADS-B	Automatic Dependent Surveillance–Broadcast
AIS	Airline Information Services
ARC	Aviation Rulemaking Committee
ASPIRE	Asia and Pacific Initiative to Reduce Emissions
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATO	Air Traffic Organization
CDTI	Cockpit Display of Traffic Information
CIA	Confidentiality, Integrity and Availability
CO2	Carbon Dioxide
Data Comm	Data Communications
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
EUROCAE	European Organization for Civil Aviation Equipment
EUROCONTROL	European Organization for the Safety of Air Navigation

FAA	Federal Aviation Administration
FedEx	Federal Express Cargo Carrier
FIS-B	Flight Information Service - Broadcast
GA	General Aviation
GAO	General Accounting Office
GHz	Gigahertz
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
JNU	Juneau International Airport
JPDO	Joint Planning and Development Office
LAN	Local Area Network
LFR	Low Frequency Radio Range
MEM	Memphis International Airport
METER	Aviation Routine Weather Report
MIT	Massachusetts Institute of Technology
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NATCA	National Air Traffic Controller Association
NextGen	Next Generation Air Transportation System
NOTAM	Notice to Airman
PIES	Passenger Information and Entertainment Services
PSR	Primary Surveillance Radar
RF	Radio Frequency
RFI	Radio Frequency Interference

RNP	Required Navigation Performance
SSR	Secondary Surveillance Radar
SESAR	Single European Sky Air Traffic Management Research
SWIM	System Wide Information Management
SOA	Service Oriented Architecture
TAF	Terminal Aerodrome Forecast
TCP	Transmission Control Protocol
TIS-B	Traffic Information Services - Broadcast
TKIP	Temporal Key Integrity Protocol
TOA	Time of Arrival
TT&C	Tracking, Telemetry, and Control Links
TVA	Threats, Vulnerabilities, and Attacks
VOR	Very High Frequency Omni-directional Radio Range
UAT	Universal Access Transceiver
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UPS	United Parcel Services

List of Tables

List of Figures

1

Introduction

The aviation industry has expressed serious concerns with passenger safety and aircraft exhaust emission worldwide. In addition, sustainable and flexible air transportation had played important role in the development of the technology model being studied. To provide for a better travel experience, scientists and engineers have designed a robust and reliable system, which requires widely used technologies, in order to provide real-time data to pilots and air traffic controllers.

However, every new technology that relies on data communication to share information is prone to certain vulnerabilities; NextGen is no exception. This thesis is devoted to investigating security issues associated with the adoption of NextGen and ADS-B with respect to confidentiality, integrity, and availability of data.

1.1 Background

The global air transportation system is the corner stone of the world economy. It is estimated that by 2015, the number of passengers travelling by air in the United States will exceed one billion [37]. Figure 1, illustrates the three largest markets facing serious challenges as the demand for air travel is rapidly increasing. The air traffic infrastructure that is currently in place will not be able to adequately handle the rising volume of aviation passengers in the future. Therefore, to meet future demands in aviation, a system change is required.

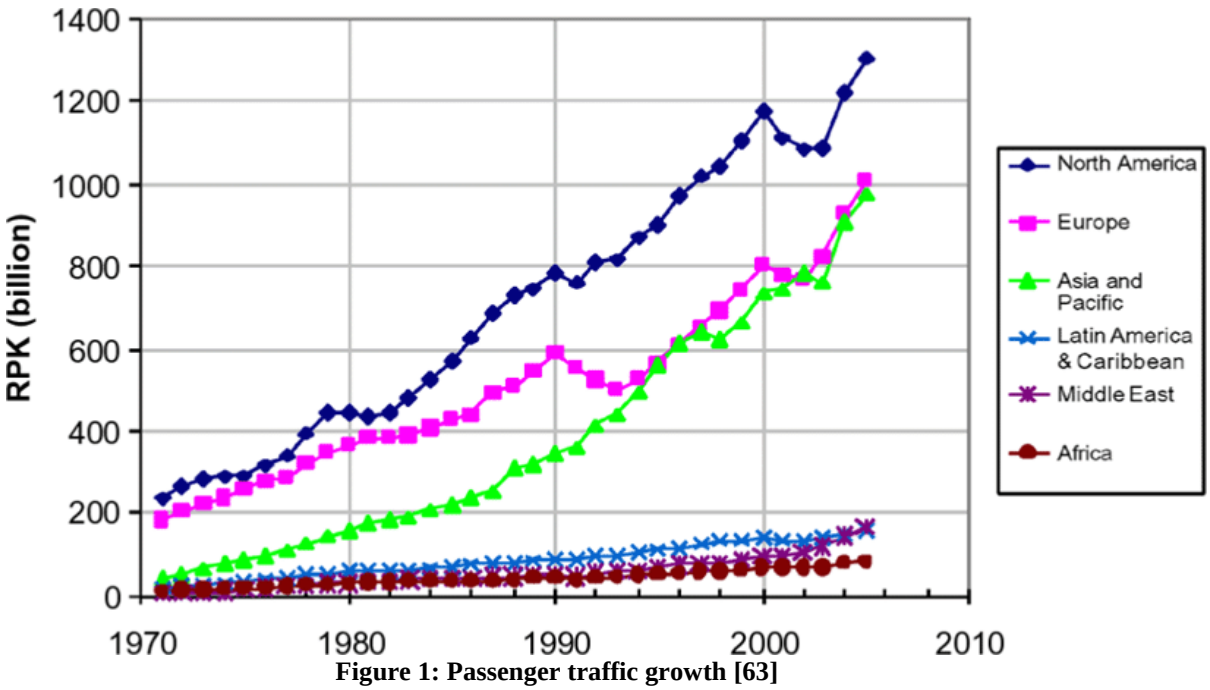

Figure 1: Passenger traffic growth [63]

The core of NextGen is a combination of programs, systems, implementation of state of the art air traffic control, and air navigation technologies introduced by the Federal Aviation Administration (FAA), in collaboration with Single European Sky Air Traffic Management Research (SESAR), led by Joint Planning and Development Office (JDPO) with the idea to change the current air space system and improve flight efficiency. NextGen is a modernization of the current radar-based air traffic control system to a sophisticated satellite-

based system. It uses a network of distributed computers to transmit digital communications allowing better travel experience and precise aircraft location. The new features offered by this technology will drastically reduce bottlenecks, accommodate growth, improve travel experience, make better use of the airports, and improve the global environment by reducing the fuel burnt [18].

From the work and research done by the Federal Aviation Administration (FAA), National Aeronautics and Space Administration (NASA), to the efforts of Joint Planning and Development Office (JPDO) and Single European Sky Air Traffic Management Research (SESAR), we have taken their findings a step further in order to provide more realistic results for the engineering community. Our goal is to investigate the security vulnerabilities associated with NextGen, with focus on ADS-B system. Lastly, we have proposed our recommendation for dealing with the security risk associated with ADS-B.

1.2 Overview

This thesis points out the security vulnerabilities of the ADS-B protocol, which is a vital safety component of NextGen. Through our research, we have investigated possible active and passive security weaknesses associated with the overall workability of the system. We aim to enhance our research by discovering security loopholes in the current system, by studying the methodology and risk in publications, done by government organizations, industry and academia. Our goal is to identify the security risks, which might halt the implementation and development of ADS-B, and provide a comprehensive summary of these risks and their impact on the system. We have focused on the data exchanged between the air and ground based systems where a sophisticated attacker can engage in malicious behavior (e.g. spoofing, jamming, etc.).

We have discussed possible solutions for dealing with these weaknesses and provided recommendations. These solutions will aid in the future development of NextGen technology. We would like the commercial and general aviation along with the FAA to make more informative and realistic decision about the adaptation of ADS-B surveillance technology.

1.3 Outline

The thesis is structured in the following way. Chapter 1 aims to provide information regarding NextGen and ADS-B necessary to understand their roles in this thesis. Chapter 2 describes the Next Generation Air Transportation System in detail, in order to give the reader a better understanding of some of the policies and issues revolving around it. Chapter 3 provides literature reviews and key elements of ADS-B, as well as security vulnerabilities. Comprehensive understanding and examples of the attacks are presented in Chapter 4 and Chapter 5 concludes this thesis and provides recommendations. To help the reader with certain terminologies in this report, we have included useful information in the Appendices.

1.4 Statement of Problems

Today most of the world air traffic control infrastructure relies on radars; these radars send out high-power interrogation signals and receive responses from a device on the airplane called a transponder. When the transponder receives the signal from the radar, it replies back with information such as four-digit aircraft identification code and altitude [48]. The ground personnel then use this information to determine the exact location of the aircraft. This approach worked well when radar was invented in the 1940's [58]. However, as skies around the world become more crowded, it is very likely that aircrafts will overwhelm the current air

traffic control system, which will lead to increases in delays, higher costs, and greater environmental impact.

To address this challenge the FAA in collaboration with universities, airline industry among others is introducing NextGen. On the other hand, ADS-B, a backbone of NextGen, poses network security weaknesses and because of these, data exchanged between aircraft and control tower could easily be spoofed and manipulated. In other words, there is no mechanism in place to protect the confidentiality, integrity, and availability of data. Adequate measures must be implemented along with appropriate security mechanisms otherwise unwanted risk may arise and jeopardize the NextGen technology. Furthermore, understanding the implications of the system is fundamental.

1.5 Thesis Limitations

Due to the complex nature of NextGen, we were limited by several factors that affected our findings. But we do not believe these limitations prevented us from effectively investigate and understand the security risks associated with NextGen and ADS-B.

It is important to note that NextGen has been implemented in stages, therefore we can only assume the attacks' effect on the current system and cannot provide a concrete proof of what could actually happen when the system is fully implemented. Moreover, as new technologies become available, the impact of these attacks can be reduced.

The second constraint is the fact that the NextGen system as a whole has many subsystems within it. This thesis however only focuses on the ADS-B subsystem operating on the 1090-MHz ES broadcast link, because of its international adaptation by air carriers. Additionally, obtaining vital quantitative data from the governmental organizations is challenging because of the restricted access to literature and documentation to the general public about specific aspects of the NextGen technology.

To enrich our research, we have reached out to experienced members in the aviation community, air safety educators, air carriers and general aviation manufacturers who were legally restricted to provide valuable information to outside contacts because of prior mutual agreement (e.g. non-disclosure) with their employer.

Finally, the lack of hands-on experience such as running laboratory tests and simulations with the system has limited the scope of this research. Obtaining the hardware components to conduct certain experiments turned out to be very expensive and building the software ourselves requires more than 20 weeks, which is beyond the time allotted to complete this thesis.

1.6 Method

To augment the NextGen and ADS-B quantitative data, we relied on several research methods. First, we have studied a comprehensive review of available legal materials relating to the NextGen and ADS-B design and development, including Federal Aviation Administration literature and documentation available to the public.

On top of frequent review of NextGen and ADS-B publications on the Internet, we have watched documentaries at National Aeronautics and Space Administration (NASA) and Federal Aviation Administration (FAA) research facilities, review material regarding equipment deployment on large and small aircrafts; we have watched flight simulation demonstrations; and aviation safety techniques to gain first-hand knowledge of the NextGen and ADS-B environment. Lastly, we have used a case study example of Juneau airport in Alaska, to review NextGen and ADS-B procedures and practices.

Additionally, we have relied on academia, non-government literature review, and extensive use of Internet-based data collection. The numerous data sources provided an affluent set of information that addressed our project objectives. Finally, we have decided not

to review source code because of challenges faced by government constraints, but instead assessed information available in our sources.

1.7 Aviation Safety

Safety is key in aviation. To address this, Safety Management Systems (SMS) are used in order to examine and monitor the real-time data in a system. This data is then further analyzed to reduce and prevent accidents [22]. "Our goal is to achieve the lowest possible accident rate and constantly improve safety" [23]. As evidence of that the Federal Aviation Administration (FAA) mission and vision statement implies that their goal is to provide the most efficient and safest aerospace system in the world and at the same time, continuously improve the safety and efficiency of aviation [19].

As stated by [50] "Aviation Safety Program (AvSP) helps examining the challenges that come with further reducing risk in a complex, dynamic operating domain like NextGen". The AvSP project analyses the entire NextGen architecture in order to predict aviation safety concerns. The goal of the program is to develop state of the art technologies, tools, and methods in order to improve safety of aircrafts using NextGen. The entire air traffic system is simulated in laboratory environment in order to provide real world scenarios [51]. The technology we will discuss in this document addresses general safety issues and focuses more on the security vulnerabilities of ADS-B.

2

The Next Generation Air Transportation System

2.1 Aviation before NextGen the U.S. Perspective

"In the decade following the Wright Brothers' first powered flight on Dec. 17, 1903, aviation captured the public imagination, but practical applications lagged".

(National Air Traffic Controller Association)

The history of U.S aviation dates back to 1903, when Orville and Wilber Wright made the first flight with their greatest invention "a self propelled airplane" [12]. Needless to say, in the period between the 1920's and 1950's aviation had reached a point where air traffic routes had to be regulated because of the increased number of aircrafts flying in the U.S. This was when the Air Commerce Act was created and different technologies were put into place to help pilots navigate the sky and increase their safety. As a result, air navigation technologies and air traffic control (ATC) such as bonfires, beacons, and radios were put in place. At first, these technologies were very simple and provided limited capabilities [7]; [45].

Bonfires provided 'out of window' navigation for pilots thus making it easier to land an aircraft at night. According to the National Air Traffic Controller Association (NATCA), bonfires were later replaced by beacon towers (e.g. rotating and flashing strobe light), which assisted pilots navigating at night over longer distances and in poor visibility [45]. It was not until the 1930's and early 1940's that radio navigation technology was introduced to aid pilots

in determining their positions more efficiently and to allow them to communicate with ground personnel. The advancement of radio navigation technology, lead to development of low frequency radio range (LFR) and very high frequency Omni-directional radio range (VOR) [1]. The combination of beacon and two-way radio communication lead Cleveland's airport to install the first radio-equipped control tower in the 1930's in the U.S. [12].

The most important technological breakthrough for the aviation industry came after World War II, thanks to the British military defense's more advanced air traffic control system, which relied solely on radar, was available to the civil aviation. Radar enabled controllers to see the location of the moving aircraft on a monitor. This feature essentially revolutionized the air traffic control [12].

The real breakthrough in the aviation industry came in 1956, when computers were introduced. The ATC was able to collect information in form of data and then display these data on a computer monitor, showing the positions, speeds, and altitudes of the aircraft [45]. It was evident that technological advancement had an impact on the aviation, however things have moved at very slow rate since radar was adapted. The air traffic control (ATC), still rely on radar and voice communication as the primary sources in order to manage the crowded airspace in the U.S. The current system is becoming slow and obsolete. To meet the challenge of air traffic growth and alleviate the risk of congestion, the FAA has invested heavily into satellite-based technology as a way to modernize the current ATC system [12].

2.2 NextGen Overview

A successful NextGen is critical for the future of global aviation system. NextGen is thorough transformation of the current antique radar-based, air traffic control (ATC) system to state of the art global positioning system (GPS) surveillance, which changes the way airplanes navigate through the sky [52] ; [35). A key idea behind NextGen is to convert most of the air-

to-ground communication from voice to data, and simultaneously transmit these data in real-time to pilots and air control towers. This kind of collaborative structure simplifies aircraft operation throughout all phases of flight and improves airport management efficiency, by offering better situational awareness for pilots and controllers [35] ; [24].

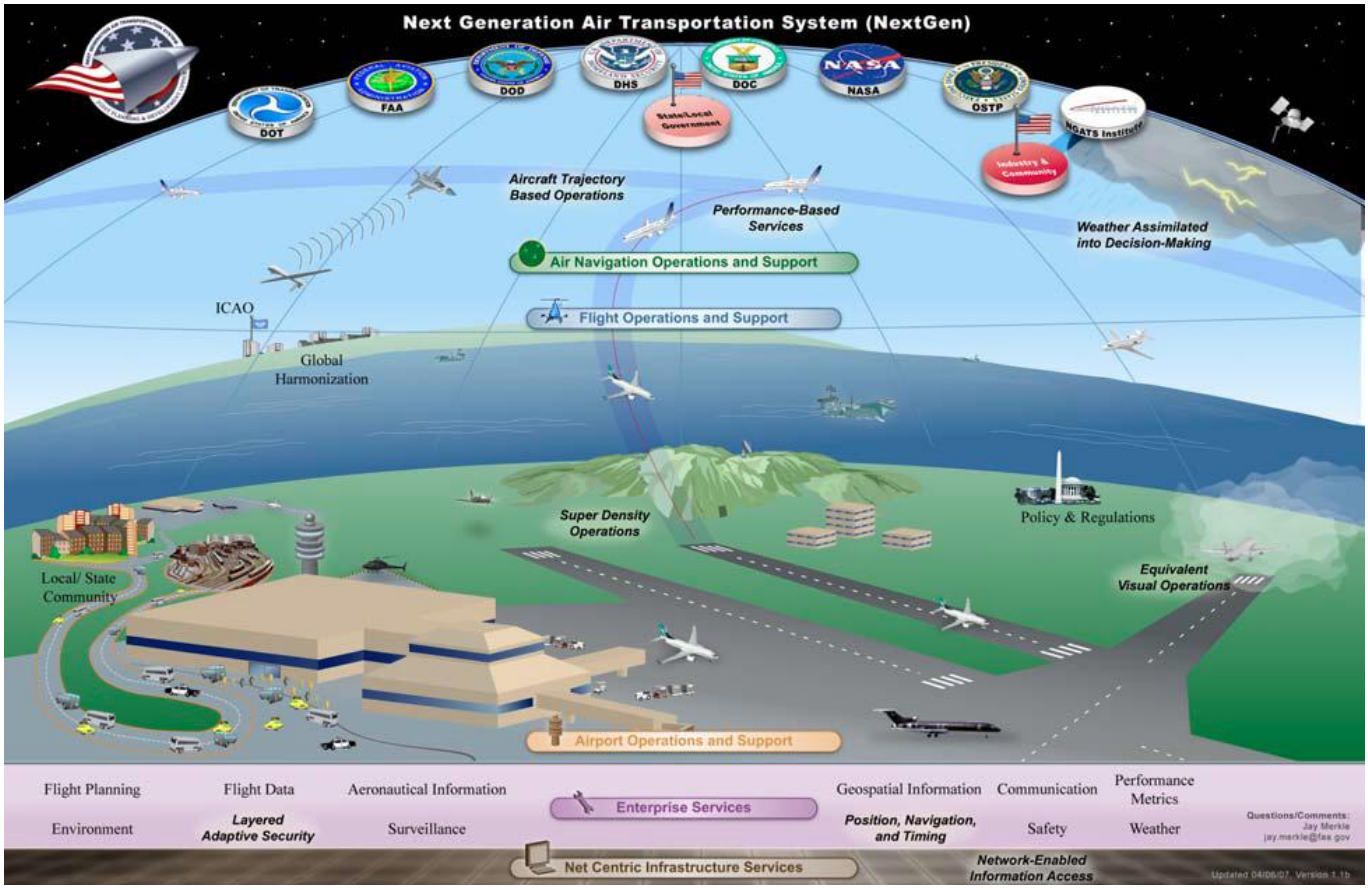

Figure 2: Next Generation Air Transportation System [37]

As illustrated in Figure 2, NextGen is envisioned to work in the following way. Communication between aircraft and the air traffic control system is strictly data based, therefore reducing the communication errors by eliminating language barriers and pilot's wrong message input. Navigation is entirely done using satellites rather than ground-based aids. Airplanes learn about each other's precise location in real-time, allowing pilots to make more informed decisions of their flight paths and their safety. ADS-B, the backbone of NextGen, relies on GPS satellite signals to accurately identify aircraft's location, speed, and altitude, and share this information with other NextGen equipped aircrafts [18]. All of this

information is available to the pilots on their display in the cockpit. ADS-B, is better than radar because it reports the location of the aircraft every second compared with every twelve seconds for radar, and improves aircraft' navigation at terrains which are very difficult to approach when simply relying on radar technology [29]. In addition, NextGen technology facilitates optimal, synchronized flow of traffic on runways and taxiways by using the Airport Surface Detection System-Model X (ASDE-X) surveillance system [25].

Trajectory Based Operation (TBO), often referred to as continuous descent arrivals (CDA), guides aircraft to smooth top-to-bottom descent in high-density airspace, therefore reducing fuel burn, noise and emission. Airspace is used more efficiently as aircraft follow four-dimensional trajectory patterns (4DT), hence avoiding potential conflicts in the sky. These trajectories are exchanged among the air traffic controller and aircraft using data-link communication (DataComm) allowing pilots to operate the most efficient routes. In oceanic operations, air traffic management provides the pilots with the most accurate trajectory as wind and other weather conditions change. A new trajectory will be calculated entirely via data communication in real time. Furthermore, TBO allows the controller to manage a larger volume of airspace containing higher densities of aircraft because the entire process is done automatically through accurate exchange of information [44]; [24].

It is important to note that NextGen is implemented in stages because it is still under development. Consequently there are some limitations to this technology as implemented today. It is expected that by 2025 air traffic around the globe will move safely, efficiently, securely, and at the same time, adapt to increase in air transportation as more and more airports around the world will become fully equipped with NextGen technology. NextGen is not an effort of a single organization but a collaborative endeavor among domestic and international governments and organizations such as the Federal Aviation Administration

(FAA), the International Civil Aviation Organization (ICAO), the Single European Sky Air Traffic Management Research (SESAR), and many others [23]; [18].

2.3 NextGen Architecture

In order for NextGen to be able to perform data communication and flow of information, a technology called System Wide Information Management (SWIM) is needed. SWIM; is an information platform that processes and shares data among authorized users from different systems. This feature of the system, increases common situation awareness and improves agility. The implementation of SWIM is based on service-oriented architecture (SOA) as illustrated in Figure 3. "*SOA enables systems on the network seeking those services to invoke them without having to change or adapt to the underlying implementation of the service.*" [59]

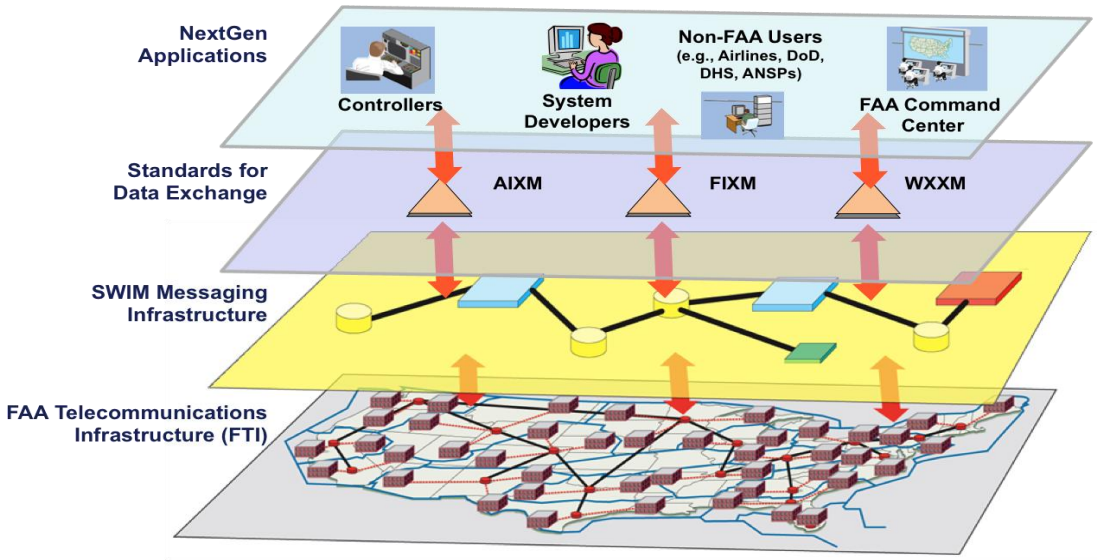

Figure 3: Service Oriented Architecture (SOA) model for NextGen [59]

SWIM is a crucial part of NextGen simply because the safety and efficiency of airspace largely depends on how well these different systems communicate with each other. Furthermore, SWIM has been deployed in stages because it is a complex technology and, according to the FAA, it will take several years before it is fully implemented [19]. A detailed

breakdown of NextGen Enterprise Architecture in regards to data-link communication between different information platforms is given by the Joint Planning and Development Office [38].

Finally, as we mentioned before, the scope of this thesis is to demonstrate the in-security in ADS-B, arising from the data messages exchanged between airplanes and air traffic control system (ATC).

2.4 NextGen Benefits

Realizing the full potential of NextGen will largely depend on users and government institutions and their decision to adapt to the technologically advanced capabilities deployed in NextGen. The FAA, along with MIT and various other organizations, have evaluated several advanced technologies like ADS-B, Data Communication, Trajectory Computation and based on their results, they drastically improve ground and air-born traffic flow, offer efficient use of the airspace by allowing more airplanes to fly closer together, reduce the emission footprint, improve flight operations by showing more direct routes for aircrafts in the event of good and bad weather [24]. Safety is preserved by having proactive data driven infrastructure and collaborative interaction of the entire NextGen system. Figure 4 illustrates the efficiency of communication and congestion at major US airports where the passenger rate is expected to rise to 1 billion by the year 2025 according to the Joint Planning and Development Office [37]. In addition, moving to a digital communication system, pilots and controllers can communicate immediately with fewer errors and monitor the aircraft movement throughout all phases of flight (e.g. takeoff, cruise, and landing) in real-time. Passengers can expect fewer delays, and the capacity of the runways can be efficiently increased [61].

Figure 4: Talking with the Sky, voice vs. data comparison model [61]

The goal of NextGen is to transition to a smarter, satellite based and digital technology in order to make air travel more convenient, predictable and environmentally friendly. The demand for the increasingly congested airspace is growing tremendously, NextGen is therefore expected to help guide and track aircrafts more precisely and on more direct routes. The efficiency of NextGen enhances safety, reduces delays, saves fuel, and reduces aircraft exhaust emissions [18]. Below are some of the benefits to be accrued from this system:

- PROVISION OF A BETTER TRAVEL EXPERIENCE

  NextGen will mean less time sitting on the ground and holding in the air. NextGen's technology and procedures are significantly reducing flight times, which in turn translate into money saved and a better overall experience for the traveling public and aviation community. NextGen also enables the exchange of real-time data about weather, the location of aircraft, vehicles, and conditions throughout the airspace. This means the right people will have the right information at the appropriate time, which in turn helps them make better decisions and improve on-time performance. NextGen is also environmentally friendly. Flying is becoming quieter, cleaner, and more fuel-efficient. Operators are beginning to use alternative fuels, new equipment and procedures, thus reducing adverse environmental impact. The presence of a more precise flight path guaranteed by NextGen also helps limit the number of people impacted by aircraft noise [18].

- PRESERVATON OF AVIATION'S ECONOMIC VITALITY

  The aviation industry plays a major role in the world's economy. NextGen's capabilities in place today are the foundation for continually improving and accommodating future air transportation needs while strengthening the economy globally and nationally with one seamless, global sky. Airports are economic engines

for the communities they serve, bringing visitors and commerce together. NextGen will provide increased access, predictability and reliability, by enhancing airport operations across the globe [18].

- NEXTGEN ENHANCES SAFETY

  The FAA's top priority is ensuring safe skies and NextGen's innovations and improvements are delivering just that. NextGen will provide air traffic managers and pilots with the tools to proactively identify and resolve weather and other hazards [18].

In the United States, Juneau International Airport (JNU) in Alaska was the first adopter of NextGen. Because mountains surround the airport, aircraft descend through a very narrow pass that is sometimes impossible to navigate, especially during low visibility [20]. A NextGen procedure that keeps aircraft on a precision path into this airport has been of significant help to Alaska Airlines as it has helped eliminate flight cancellations and weather related diversions. The airline uses GPS-based NextGen Area Navigation Required Navigation Performance (RNP) flight procedures, and this saves the airline $15 million annually due to flight completions [18]. These flight procedures are so effective that in 2011, Alaska Airlines completed 820 flights to Juneau airport that would otherwise have been delayed, diverted or completely cancelled [20].

The first U.S cargo carrier airline to experience the benefits of NextGen was FedEx Express at Memphis International Airport (MEM). *"Aviation International News online reported that the first airline trial would begin November 12, 2012 in Memphis. Air traffic controllers and flight crews will use a data communications system for pre-departure and revised departure clearances while planes are on the ground"* [49]. The publication also explains that FedEx uses data communications for over the ocean flights and for remote areas of the world as well. FedEx pilots and ground personnel benefit from NextGen by having the

system deliver data messages directly to the management computer, eliminating the need to manually enter these messages.

The Federal Aviation Administration's goal is to see NextGen's benefits in other continents as well. As a result of that, the FAA is working side by side with the Single European Sky Air Traffic Management Research (SESAR) and the Asia and Pacific Initiative to Reduce Emissions (ASPIRE) in order to develop international standards for NextGen [18]. In Europe, SESAR, which is the equivalent of NextGen, is trying to improve gate-to-gate trans-Atlantic flights between the two continents. In Asia, ASPIRE is working on an initiative called "Green Flight" where results of fuel saving and tailored arrivals have been evident thanks to NextGen [19].

Finally, the Next Generation Air Transportation System's (NextGen) progress is vital if addressing aging technologies, lowering emission, eliminating gridlocks, and increasing safety are to be preserved in the future of the global airspace [18]. More detail-oriented information on NextGen benefits can be viewed at the Federal Aviation Administration Implementation Plan and Joint Planning and Development Office publications [18] ; [39].

3

Automatic Dependent Surveillance-Broadcast

3.1 ADS-B Overview

With radar, pilots rely on air traffic controllers and a see-and-avoid strategy that literally entails looking out the window to avoid wandering in the way of—or colliding with—other aircraft on the runways. With ADS–B, pilots have a cockpit display, which looks like a full-color, topographical map on a computer screen, showing where they are, where everyone else is, and the ever-changing weather around them. "It's giving the pilot an extra set of eyes".

(Sharman - von Thaden)

To cope with the ever-growing demand of global air travel limitations, deployment of ADS-B has been initiated in the North and South America, Europe, Asia, and Australia [18]. As stated by the FAA, the ADS-B technology is a very important component of NextGen's implementation process because it aims to replace the current radar system with sophisticated global positioning system. Once an aircraft's position is determined by GPS, this information is then distributed to other aircraft in the area and ground based stations. ADS-B is responsible for the real-time distribution of this information [18].

Primary and secondary surveillance radar systems are currently used in the United States to guide pilots and track airplanes throughout the congested airspace. This type of system has its limitations with respect to human error, cost, and accuracy [2]. Primary Surveillance Radar (PSR) works by sending interrogation signals. Those signals then ricochet off of the aircraft. Secondary Surveillance Radar (SSR) on the other hand, is an improved type of radar system,

which basically replies to the interrogation signals with the help of an aircraft onboard transponder [21]. FAA estimates full deployment of ground ADS-B infrastructure by 2014, however full evolution will take roughly 20 years [18]. In addition, the ADS-B surveillance system will enhance safety, by permitting controllers to manage and monitor with greater safety margins, increase the efficiency and capacity on the runways, and provide better tracing accuracy of aircrafts.

Safety will be preserved by improving situational awareness, broadcasting the exact location of the aircraft in real-time, and by having the broadcasted information available to all users (e.g. flight and ground crews). This also applies for air traffic management of oceanic airspace, ridged mountains, and remote regions. Efficiency, will allow for aircrafts flying closer together and reducing fuel consumption. Capacity on the other hand, will improve the departure and arrival rate, allowing more aircrafts to fly concurrently; which will provide more efficient use of runways [18]. Finally, the FAA's goal is "establishing an agile air traffic system that accommodates future requirements and readily responds to shifts in demand from all users" [14].

Table 1: Radar vs. ADS-B characteristics

RADAR	ADS-B
Areal coverage limitation	No areal coverage limitation
Aircraft tracking with less accuracy	Aircraft tracking with more accuracy
Aircraft location is determined every twelve seconds	Aircraft location is determined every second
Voice communication	Digital data communication
Expensive to install	Less expensive to install

3.2 ADS-B System Functionality

At the core, the ADS-B operates by allowing aircrafts and controller to automatically transmit data information every second without pilot intervention at regular time intervals, with higher precision than radar. To determine aircraft position and velocity vector, ADS-B depends on GPS technology. Surveillance is used to determine the accurate position of the aircraft, while broadcast helps other aircraft and air traffic controllers equipped with ADS-B technology, to receive data information. On top of that, the distance between the aircraft and ground station is irrelevant for broadcast message accuracy [14].

Joint efforts by NASA and FAA allowed GPS to become the norm in the aviation industry. Because of its capabilities to locate aircraft in three dimensions, global coverage, precise location, and most importantly free service, GPS is an ideal tool for military and civilian aircraft [33]. The Global Positioning System (GPS) was developed by the U.S. Department of Defense (DOD) with the idea to provide worldwide navigation based on a constellation of twenty-four satellites orbiting the earth at very high altitude. These satellites have built-in atomic clocks and provide unbelievable precision, which enables them to act as reference points from which receivers on the ground "triangulate" their position [33]. There are more technical details describing GPS technology with regards to measurements and satellite position; however those details were left out intentionally because they were out of the scope of our research. To better understand the functionality of ADS-B, please refer to Figure 5.

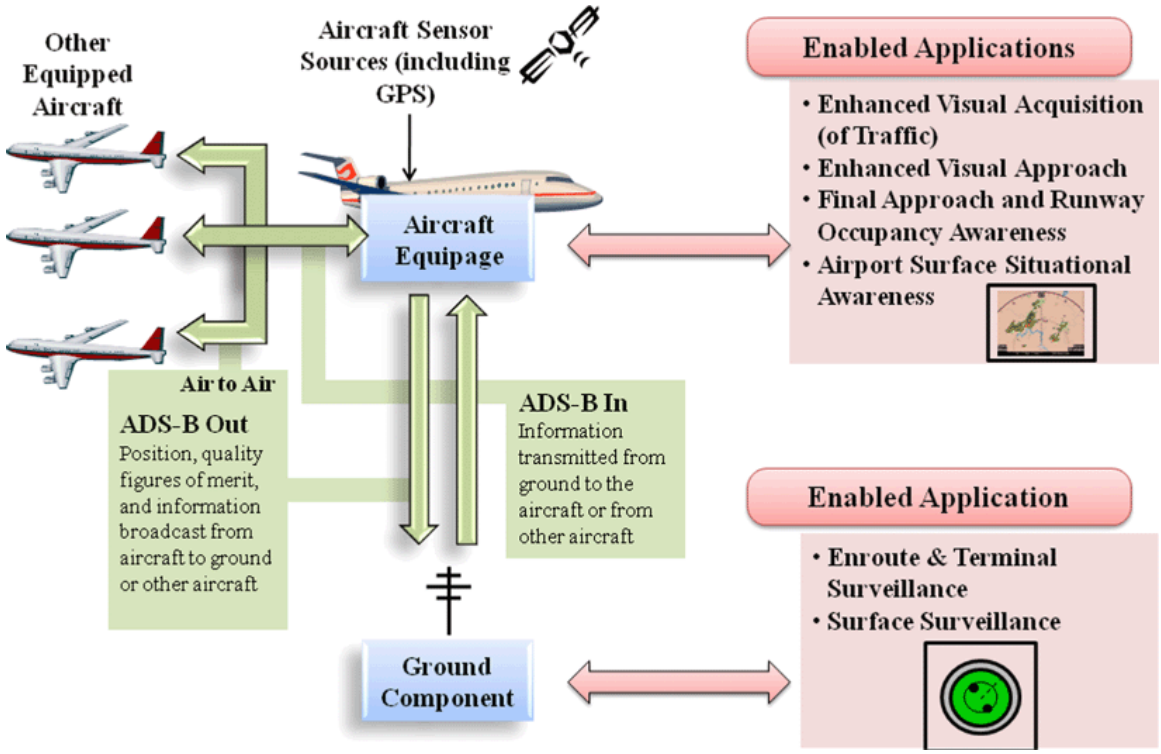

Figure 5: ADS-B Concept of Operation [4]

ADS-B provides an ADS-B IN and ADS-B OUT data-link type of service. The ADS-B OUT portion is responsible for broadcasting messages from aircraft via an onboard transmitter to the ground station and other ADS-B IN equipped aircrafts in the area. These broadcast messages contain information such as aircraft flight information, speed, heading, and other parameters and are displayed on the air traffic controller's screen. On the other hand, ADS-B IN is capable of receiving information from multiple sources, from ground station and other aircrafts and at the same time displaying the information (e.g. weather, flight restrictions) to the flight crew's cockpit [4] ; [14]. By using ADS-B IN and OUT capabilities, flight crew and ground personnel will have very accurate information about aircraft's location in the area.

The hardware required for the new ADS-B system, is fairly cheaper, smaller in size, and easier to maintain than is that for the current radar hardware. Therefore these characteristics allow for the surveillance extension of ADS-B, because the system can be deployed in larger numbers and maintained at lower cost. The aircraft requirements for ADS-B OUT call for GPS receiver, data link transmitter, and antenna. The most generic-data link transmitter is the

Mode S Extended Squitter transponder, even though Universal Access Transceiver (UAT) could also be used. The ADS-B IN uses the same hardware, as does the ADS-B OUT with the addition of a multi-function display called Cockpit Display of Traffic Information (CDTI) as illustrated in Figure 6. The ground stations will continue to use the traditional Primary Surveillance Radar (PSR) because of its compatibility with the ADS-B surveillance technology. Finally, ADS-B is all about providing surveillance in areas where radar is not possible and synchronized communication between aircrafts, and aircrafts and ground [2]; [14].

Figure 6: Cockpit Display, above and Cockpit Display of Traffic Information (CDTI), below [26]

In the U.S., the ADS-B system broadcasts digital messages on two different frequencies, 1090-MHz and 978-MHz via radio transmitter. The 1090-MHz broadcast link required for commercial aircraft flying above 18,000 feet (5,500 m) uses Mode S extended squitter (ES) transponder and it is an international standard for ADS-B OUT, approved by the International Civil Aviation Organization (ICAO). The 978-MHz broadcast link along with Universal Access Transceiver (UAT) is used by the general aviation (GA) and is required for aircrafts flying below 18,000 feet. According to the FAA, the 978-MHz frequency allows the general aviation to have a more affordable avionics package and it offers extra bandwidth, which can be used to upload weather and information services, not available on 1090 MHz [2]; [14].

Additional services offered by ADS-B are TIS-B and FIS-B. Aircraft equipped with either 1090-MHz extended squitter (ES) transponder or 978-MHz universal access transceiver (UAT) collect information data (e.g. precise location of the aircraft as illustrated in Figure 5) from internal global positioning system (GPS) receiver and then broadcast it [2]. These data are repeatedly broadcast not only to ground stations and air traffic control (ATC) but also to other aircraft in the vicinity equipped with ADS-B instruments. This process is known as Traffic Information Services – Broadcast (TIS-B) and it improves traffic awareness both airborne and on the ground by allowing the pilot to see what the controller sees, using Cockpit Display of Traffic Information (CDTI). This reduces the risk of runway collisions and enhances visual acquisition. Another ground-to-air service called; Flight Information Service – Broadcast (FIS-B) presents the pilots with meteorological information such as notice to airman (NOTAM), terminal aerodrome forecast (TAF), aviation routine weather report (METER), and it is used on 978-MHz UAT because of its higher bandwidth capacity. FIS-B enhances pilot awareness by providing real-time data of hazardous weather and airspace limitations [18]. Lastly, the evolution of ADS-B will simplify certain responsibilities such as information processing from the ground station to the flight crews' cockpit.

In section 2.4 we have seen how FedEx Express benefited from implementing NextGen. Currently, United Parcel Services (UPS) at Louisville International Airport, in Louisville, Kentucky has benefited immensely by adopting the ADS-B system. Since most of the flights take place at night, runways have tendency to become very crowded due to very short departure and arrival time, ADS-B has allowed pilots and ground stations to move aircraft more efficiently [31].

3.3 International Implementation of ADS-B

As noted by Massachusetts Institute of Technology (MIT), researchers Edward Lester and John Hansman [40], Sweden is believed to have been the first nation to explore ADS-B technology in the 1980's. It is important to mention that at the time, Sweden was advocating an additional protocol called Mode 4 data link, and were not using the 1090-MHz-ES and 978-MHz UAT data links.

Today, Australia is considered to be one of the early adopters of the ADS-B surveillance technology with 29 ADS-B sites providing full coverage of the continent. For Australia, it was an easy decision because most of the country, except the coastal areas has very poor radar coverage or no infrastructure at all [34]. Europe on the other hand, in collaboration with the EUROCONTROL CASCADE program, is enjoying the advantages of SESAR technology, which is the equivalent of ADS-B in the United States [16]. The United States has begun its initiative on ADS-B, however it will take several years before the entire country relies on GPS surveillance for full air traffic management [18]. A functional diagram of the ADS-B usage worldwide is shown in Figure 7. The yellow colored aircraft represent the real time ADS-B data, whereas the orange colored aircraft represent delayed ADS-B data. Most countries in Asia, Africa, and Latin America do not have any ADS-B coverage because radar is still the dominant technology used to aid air navigation. Finally, the Federal Aviation Administration

firmly believes that if universal ADS-B system development and global airspace consistency are to be achieved, then joint collaboration between different nations is inevitable [18].

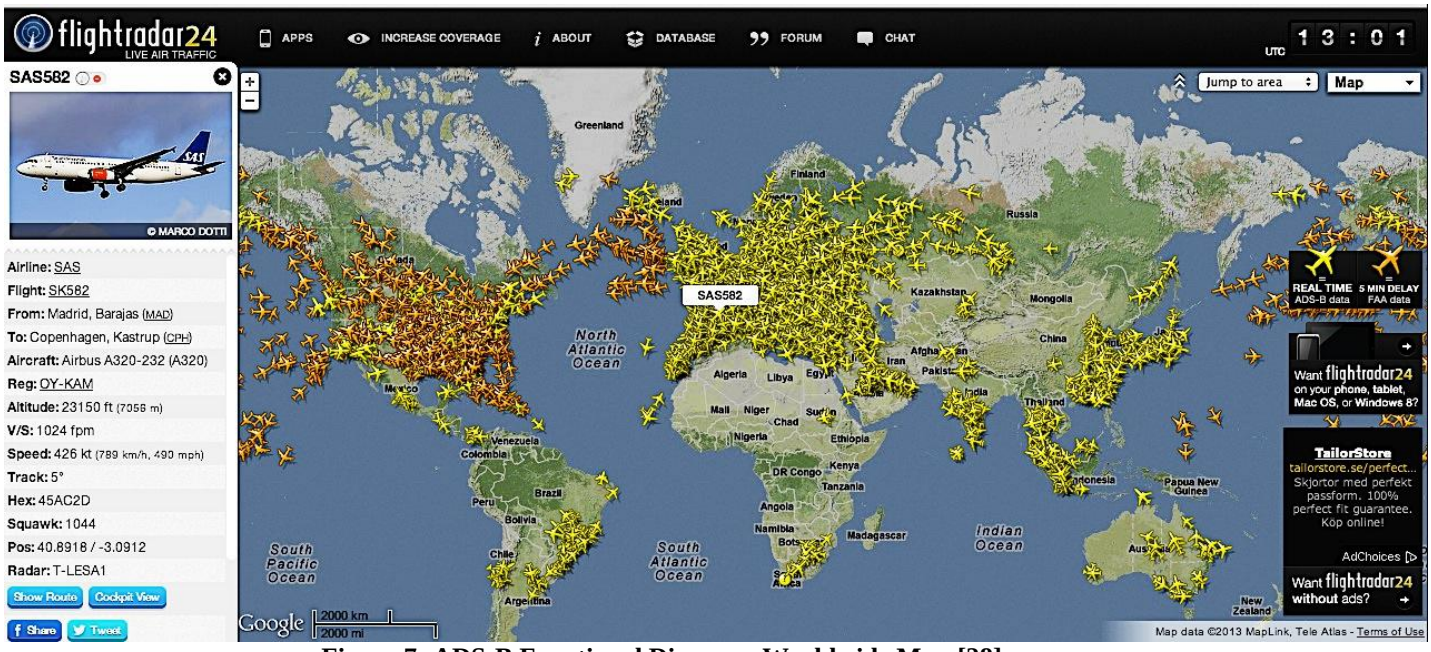

Figure 7: ADS-B Functional Diagram, Worldwide Map [28]

3.4 Known Vulnerabilities with GPS and ADS-B

3.4.1 GPS Vulnerabilities

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities;
and assess, coordinate, and deconflict all cyberspace operations…"

(The National Strategy for Cyberspace Operations, [46])

A report published by the United States General Accounting Office in 2002 [30], highlights that existing threats in GPS had led to temporary interruption of the system, putting commercial aviation at significant risk. One such interruption was noted, while ground GPS transmitter had interfered with GPS receiver of a commercial aircraft, causing the plane to temporary loose all of its GPS information [30]. A further study by the Department of

Defense (DOD) and the Department of Transportation (DOT) of vulnerability assessment [15], commented that the GPS architecture is prone to malicious disruptions. The ADS-B relies solely on GPS to determine aircraft positions in the airspace. Even though GPS does not transmit ADS-B data, there are a number of vulnerabilities within the GPS technology itself, which can impair the functionality of the entire ADS-B surveillance technology [2]. GPS is a very complex structure where vulnerabilities can occur at different levels, as data messages travel from the satellite to the aircraft and ground station (e.g. receiver) [30]. Table 2 contains more details about unintentional and intentional vulnerabilities in different parts of the commercial surveillance system.

Table 2: Unintentional and Intentional Vulnerabilities to GPS [30]

Unintentional		**Intentional**	
Type of threat	**Vulnerable satellite system components**	**Type of threat**	**Vulnerable satellite system components**
Ground-based: 1-Natural occurrences (including earthquakes and floods; adverse temperature environments) 2-Power outages	Ground stations; TT&C and data links	**Ground-based:** 7-Physical destruction 8-Sabotage	Ground stations; communications networks All systems
Space-based: 3-Space environment (solar, cosmic radiation; temperature variations) 4-Space objects (including debris)	Satellites; TT&C and data links	**Space-based (anti-satellite):** 9-Interceptors (space mines and space-to space missiles) 10-Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites Satellites; TT&C and data links
Interference-oriented: 5-Solar activity; atmospheric and solar disturbances 6-Unintentional human interference (caused by terrestrial and space-based wireless systems)	Satellites; TT&C and data links	**Interference and content-oriented:** 11-Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth) 12-Jamming	All systems and communications networks All systems

Furthermore, the GAO expresses concerns with confidentiality, integrity, and availability of data communication in satellite systems. According to their report, the FAA, the DOD, and the NASA concur with the findings and proposed that:

- *"Steps should be taken to promote appropriate revisions to existing policy and the development of new policy regarding the security of satellite systems, to ensure that federal agencies appropriately address the use of commercial satellites, including the sensitivity of information, security techniques, and enforcement mechanism* [30]*."*

- *"Techniques to protect satellite systems from unauthorized use and disruption include the use of robust hardware on satellites, physical security and logical access controls at ground stations, and encryption of the signals for tracking and controlling the satellite and of the data being sent to and from satellites* [30]*."*

With respect to security, it is evident that there are major concerns, and in addition to that, GAO had addressed the aviation community stating that, "commercial aviation uses backup satellites and redundant features to ensure availability" [30]. DOT and DOD believe that despite the vulnerabilities discovered in ADS-B and GPS, there are adequate measures (e.g. mitigation techniques) to validate any discrepancy that may occur. Finally recommending "future work will include more in depth analysis of some of the threats and gaining better understanding of how to mitigate them." [15] These issues were of particular interest to this study because "to transmit GPS data to civil aviation, the Federal Aviation Administration (FAA) objective is to rely on commercial satellites" [30].

In March 2011, an article published by the Economist reported how a truck driver who had equipped his truck with a cheap GPS jammer had caused nightmares for air traffic controllers (ATC) at Newark Liberty International Airport [60]. Apparently, every time the driver drove in close proximity to the airport, its GPS jammer caused the airport surveillance-navigation system receiver to experience sporadic delays. Professor Todd Humphreys from the University of Texas at Austin explains how his team managed to "hijack" a civilian drone in front of the Department of Homeland Security (DHS). According to their test results, they were able to feed malicious data to the drone by spoofing its GPS signal [32]. Then Professor Humphreys points out that "spoofing a GPS receiver on a UAV is just another way of hijacking a plane, it's not only about drones, it's GPS in general that is not safe" [32]. Finally, addressing the most common flaws associated with GPS is essential for successful integration of ADS-B.

3.4.2 ADS-B Vulnerabilities

Any ADS-B equipped aircraft can broadcast its position derived from the onboard equipment, over a shared data communication link [53]. The fact that information is exchanged on a common link makes the dissemination of navigation signals/frequencies (e.g. 1090-MHz and 978-MHz) susceptible to jamming. Hence, ADS-B is susceptible to injection of "phantom" aircrafts into the system [5]. The Aviation Rulemaking Committee (ARC) has expressed serious concerns that a malicious actor could exploit broadcasted messages (e.g. launch various message attacks) and create flight route conflicts in the global airspace [5]. In response to the ARC findings, various governments, industries, and academic institutions have conducted their own research and discovered that the ADS-B system lacks minimum-security mechanisms and is vulnerable to both internal and external threats as summarized in Table 3.

Table 3: Vulnerabilities to ADS-B [55]; [54]; [53]; [47]; [11]; [36]

Type of threat	Description of the threat	Vulnerability
1-1090MHz Jamming	- Temporarily disables communication between sender and receiver (DoS)	- Transmission on a common communication channel
2-Spoofing of ADS-B Signal and Message Injection/Reply	- Randomly engineering an error to generate bogus aircrafts to confuse real aircraft in the airspace and air traffic controllers	- Any two devices with ADS-B capabilities can exchange messages
3-ADS-B System Shutdown	- Disables tracking of aircraft (9-11 incident in US)	- Ability to physically access the system
4-Internal Data Manipulation and Corruption	- Hacking ground station communication network	- Lack of firewalls, antiviruses and intrusion detection systems
5-Repudiation/Liability	- When the system detects corrupted information, an entity denies having sent or received such information, leading to disrupting liability for accident or failure events in the airspace system	- Lack of an error checking mechanisms of ADS-B data
6-Message Misuse/Deletion	- Adversary can locate and track aircrafts - Messages alteration during transmission between the ground stations and the air traffic management system - Loss of real-time aircraft position on controller display - GPS jamming could block aircraft ability to use GPS	- Any two devices with ADS-B capabilities can exchange messages - Lack of a secure communication channel
7-ADS-B System Reliance on GPS	- Listen and capture cleartext data of air traffic exchanged between aircrafts and aircrafts and air traffic control	- Susceptibility to jamming
8-Eavesdropping	- Third party ability to receive, modify and re-broadcast ADS-B messages	- Lack of security in the communication channels (e.g. no encryption)
9-Delayed Signal Retransmission	- No message secrecy, limits international use	- No authentication mechanism
10-Insecure data transmission	- Aircraft position and flight number availability to the public	- Lack of encryption of data
11-Lack of confidentiality, integrity, and availability	- The unique 24-bit code aircraft identifier address is openly available to the public - Coordinating an attack on aircrafts by deriving information from aircraft ID data and current position - Using the Internet to transmit and re-transmit	- Lack of encryption of data

It is important to note that ADS-B operates using a low-power signal, it is highly dependent on GPS and wireless communications therefore it is more vulnerable than radar [41]. A malicious actor could execute passive attacks (e.g., eavesdropping) by intercepting ADS-B broadcast messages in a search for confidential information, like 24-bit aircraft ICAO address or travel plan of communicating aircraft [56]. Active attacks allow a malicious actor to inject faulty information into an ADS-B message during transmission, in order to deliberately confuse communicating parties about their locations, leading to a misinterpreted outcome caused by bogus data [54]. Even though spoofing and RF jamming of ADS-B messages is possible, ARC claims that a secondary surveillance system with lower performance is adequate enough to compensate for spoofing and data loss [5]; [54].

According to research conducted by University of New South Wales in Australia [47], the components of the ADS-B system that, are the most vulnerable, are the ones shown in Figure 8. The authors add that further analysis is needed in order for the aviation community to be able to mitigate the impact on these areas and reduce vulnerabilities.

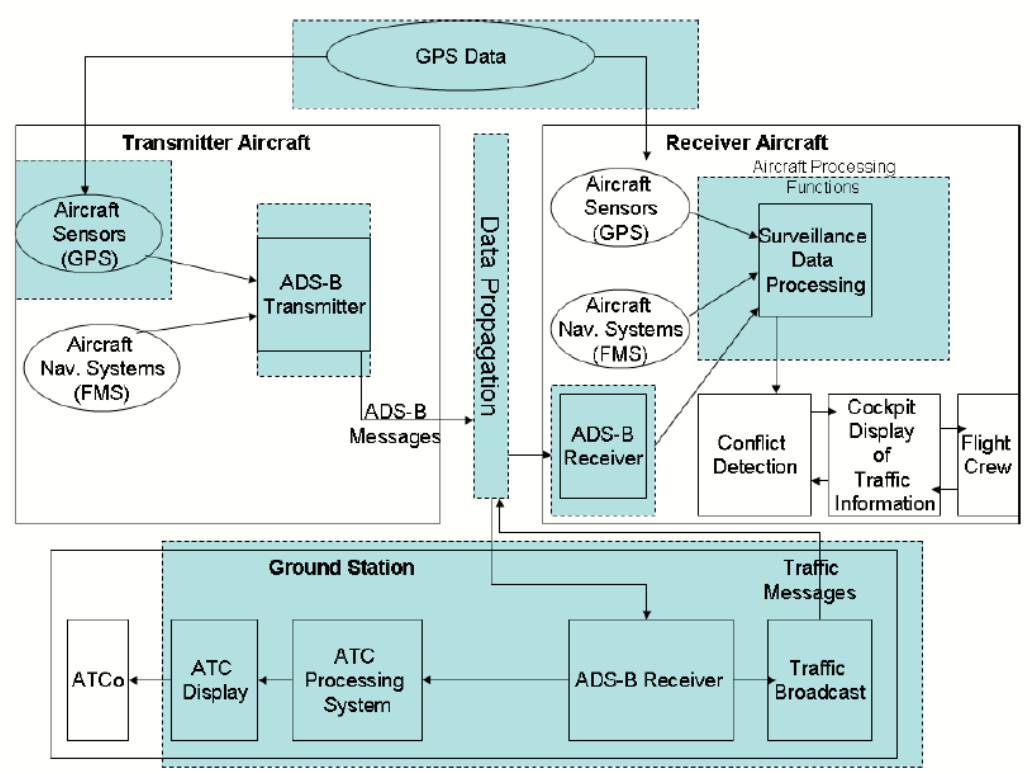

Figure 8: Overview of ADS-B most vulnerable areas [47]

A publication by Andrei Costin [11] argues that "*Despite the fact that lack of security of ADS-B technology has been widely covered by previous academic studies, and more recently by the hacking community, the fundamental architectural and design problems of ADS-B have never been addressed and fixed*". Costin has demonstrated these flaws by successfully building a cost-efficient adversary model with commercial off the shelf hardware and software components in order to spoof ADS-B signals. The demonstration of injecting "ghost airplanes" is very well documented in his publication. Finally, the ARC indicates that privacy of ADS-B equipped aircraft will be very difficult to maintain, because information such as aircraft identification, speed, and altitude will be publicly available on websites such as www.liveatc.net [5].

3.5 Summary

According to the findings demonstrated in section 3.4.1 and 3.4.2 it is evident that further technological developments with respect to security are needed, if the GPS is to be relied on as a primary air navigation service in the future. The combination of vulnerabilities can give each GPS measurement severe uncertainties, impairing the ability of the ADS-B system to determine the accurate position of aircraft. Therefore causing havoc in the global airspace. To avoid unintended consequences such as flight-route conflicts, adequate ADS-B defense techniques preserving confidentiality, integrity, and availability of flight data are required. These defense techniques (e.g. intrusion detection system, etc.) will proactively identify risks that might occur when unwanted changes to ADS-B are applied. Otherwise, the capability of ADS-B and NextGen could be jeopardized and not perform as intended.

4

Research and Results

"We should all be concerned about the future because we will have to spend the rest of our lives there."
(Charles F. Kettering)

4.1 Modern Global Aviation

Previously we discussed that voice communication is becoming a problem for the aviation industry, in order to efficiently manage crowded skies around the globe. To alleviate this issue, the United States and Europe have introduced NextGen http://www.jpdo.gov/ and Single European Sky Research http://www.eurocontrol.int/sesar technologies respectively, which allows for more efficient air traffic management (ATM) system using digital communications [53]. The idea is to transition to a network-centric infrastructure relying on various wireless interfaces (e.g. 802.11, 802.15, etc.) and implementation of Internet Protocols (e.g. TCP, UDP, etc.) for air to ground communications as illustrated in Figure 9 [53]; [6]. This kind of environment, where the Local Area Network (LAN) systems in an aircraft communicate with the ground station via distributed computer network for its operation, poses substantial privacy risks. Due to the high level of hardware and software integration and vendor specific information technology management support, the e-enabled (e.g. digital and automated) aircraft will be exposed to internal vulnerabilities. Additionally, this kind of technological transformation where information sharing with external parties (e.g airline,

airport, air navigation service provider, etc.) is also required, contributes to the growing security threats.

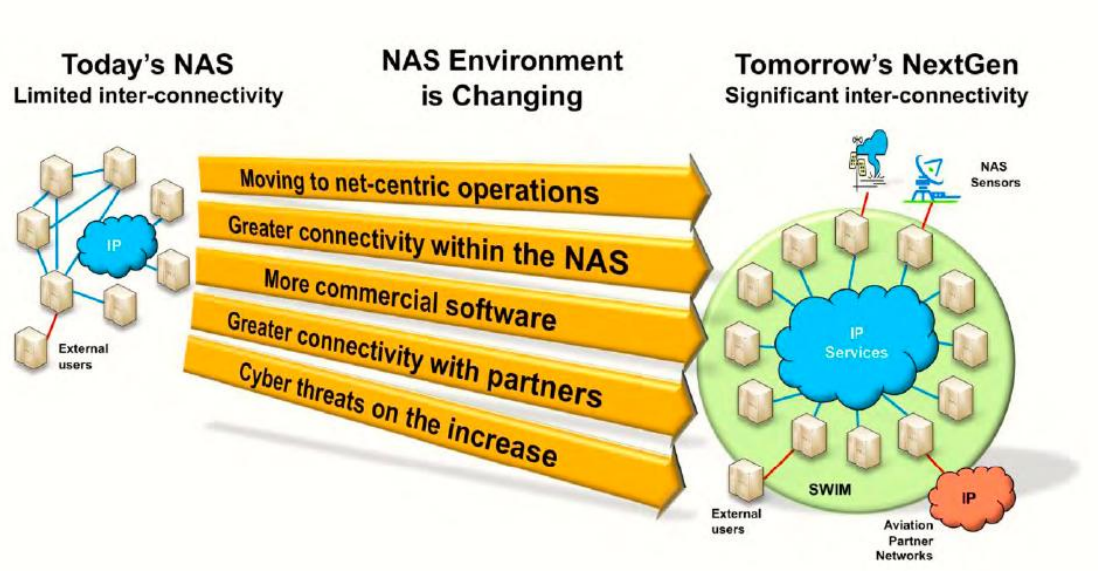

Figure 9: Increase of security risks due to transition of National Airspace System [6]

4.1.1 Wireless Aircraft Communications

The e-enabled aircraft is equipped with sophisticated wireless technologies and advanced avionics, allowing the aircraft to have broadband connectivity throughout the global airspace where information sharing between aircraft and ground stations takes place using the Internet, as illustrated in Figure 10. In addition, the logical system of the e-enabled aircraft takes full advantage of the network-centric infrastructure allowing for aircraft control (AC), airline information services (AIS), and passenger information and entertainment services (PIES) communications [53]. The AC communication portion is used by the aircraft to communicate with each other and the ground stations using various aeronautical protocols (e.g. Comsat, 1090-MHz ES, etc.). During the communication, sensitive data such as the 24-bit aircraft ICAO address are exchanged using these protocols. The airline information services (AIS) communication portion is responsible for transmitting flight logistics such as

software updates, which are vital for stable aircraft operability. The communication strictly relies on wireless and cellular networks (e.g. 802.11, 802.16). Last, the passenger information and entertainment services (PIES) communication provides passengers with live television capabilities, onboard Internet access, and various types of in-flight entertainment [53].

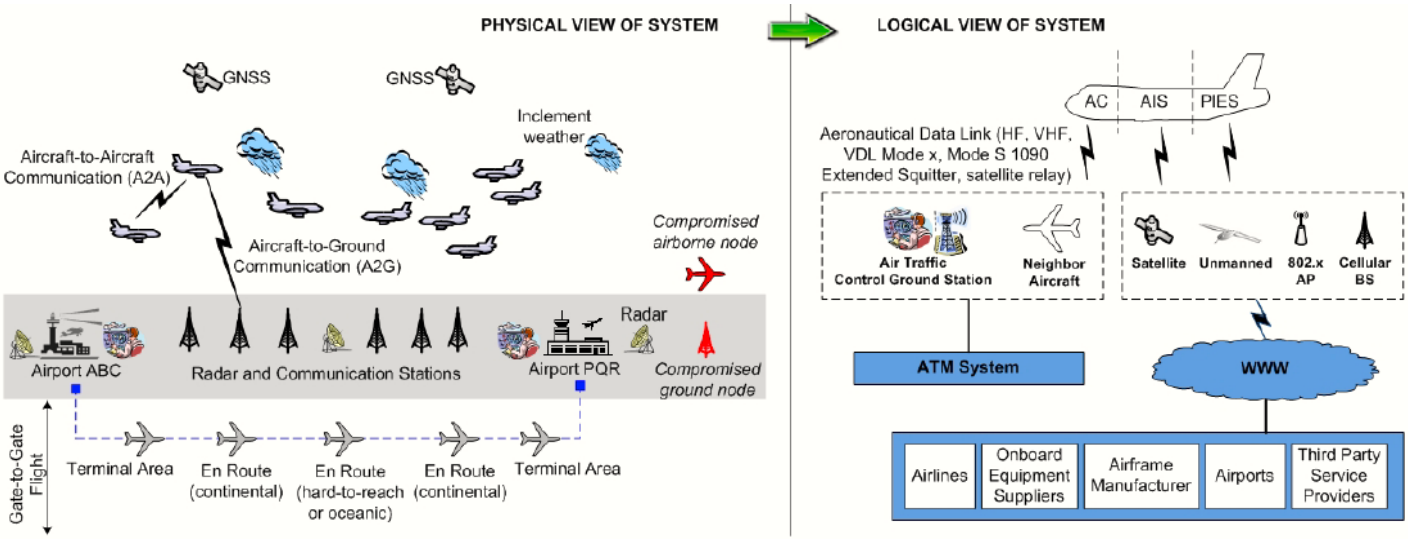

Figure 10: Global future of ATM system and e-enabled aircraft [53]

This kind of infrastructure, where critical information is exchanged using global positioning system, cloud computing, and wireless communication, sets major security challenges and exposes the data exchanged to various attacks. Such an environment creates colossal concerns for the aviation industry, putting the life of passengers and crew members in danger.

4.2 Security Assessment

The Internet has allowed the introduction of interconnected and interdependent systems to emerge in recent years, with that, large number of security challenges have been emphasized for the global aviation [53]. As a result, we have seen many articles and publications discussing denial of service attacks, spoofing attacks, viruses, zombies, and various other malicious activities. It is evident that cyber security risks are increasing and

threats against information technology systems are becoming more sophisticated. In addition, very little has been done by the engineering community to address these issues.

According to Ross Anderson [3], "*Security is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves. Security requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law*".

Complex systems require security on different levels, both physical and logical [46]. The NextGen is defined as a system-of-systems, which requires appropriate security standards at all levels, otherwise a weakness at one level of the system can halt the entire operation of NextGen [53]. Security assessment is important in data communication if confidentiality, integrity, and availability of data are to be protected. If security is omitted at any level of NextGen, an attacker can execute malicious behavior in the system [53]. The current ADS-B system openly transmits sensitive aircraft information over a shared link, allowing flight information to become available to everyone with the right ADS-B equipment. This vulnerability exposes the system to spoofing, jamming, and eavesdropping of ADS-B data [13].

Furthermore, we investigate the nature of the security attacks, their verisimilitude of occurrence, and consequences that might lead to disruption of confidentiality, integrity, availability and performance of airborne and ground data links digital systems.

4.2.1 Confidentiality

When an unauthorized recipient intercepts exchange of data between sender and receiver, the result is known as loss of confidentiality. In aviation, protecting sensitive information

from unauthorized access is crucial because of possible corruption and privacy exposure when data is transmitted on an insecure network. During our research, we have discovered that ADS-B data is transmitted on a network without encryption or any other mechanism to check for authenticity. With such a network configuration, everyone with ADS-B capabilities can gain access to this data (e.g. flight number, aircraft position, 24-bit aircraft address, etc.) and possibly make it available to the public for malicious purposes on websites like http://www.flightradar24.com/.

To protect confidentiality of wireless communications Temporal Key Integrity Protocol (TKIP) can be used among different methods. The idea here is to ensure that data communication between the sender and receiver is encrypted using a 128-bit long secret key combined with 48-bit initialization vector (IV), therefore only the authenticated parties can access the information.

4.2.2 Integrity

When an unauthorized individual modifies data either intentionally or unintentionally during transmission, is defined as loss of integrity. Integrity is particularly important for air traffic control because messages exchanged between the ground station and aircraft can be altered or even deleted, resulting in disappearance of aircraft from the display and transmission of false messages. In other words, the pilot and controller will receive modified data leading them to make incorrect decisions, and in some cases, they might not receive any information at all. In ADS-B, messages are broadcasted and no acknowledgement is received once these broadcasts have reached their destination. In such an environment, an adversary can spoof and modify message traffic, thereby violating one of the fundamental properties (e.g. pillars) of network security.

To ensure integrity of a message in wireless communications, a CRC32 checksum

mechanism can be used to detect damaged messages. In addition, before communication takes place between two stations synchronize (SYN), synchronize-acknowledge (SYN-ACK), and acknowledge (ACK) messages are exchanged. This method guarantees that the recipient receives unmodified data by reassembling it in the correct order.

4.2.3 Availability

Availability is probably regarded as the most important attribute in service-oriented architecture where sharing and processing of information takes place among different systems. The idea is that if part of the system is down, it could affect the other systems depending on it. Recently, an American Airline network system experienced intermittent outages, which caused interrupted services such as airline schedules, flight information, and even lead to grounding all flights. Such an example is defined as loss of availability.

The ADS-B is part of NextGen, therefore, relies on a network connection to perform information sharing. ADS-B accomplishes this by periodically (e.g. every second) broadcasting messages with aircraft and ground stations in the vicinity, therefore ensuring availability and avoiding authentication. Jamming can lead to loss of data, therefore disrupting the availability of ADS-B broadcasts. To ensure the availability of data in wireless communication, devices normally require authentication. One way to achieve authentication is by using digital signatures where public and private keys are exchanged in order to ensure that the data being transmitted comes from trusted sources and is authentic.

4.3 Known Attacks on GPS and ADS-B

To investigate, identify, and understand attacks on ADS-B system we have designed the novel Threats, Vulnerabilities and Attacks or TVA Matrix. We have developed this matrix based on reviewing case studies and studying an abundance of literature. By using TVA, we

can determine the impact of each attack and the effect it will have on the overall global airspace. Furthermore, the information provided in the matrix can be used to improve the most vulnerable areas of the system. The level of attacks can be classified as low, medium, or high. Attacks on the low level, can be executed fairly easily by the malicious actor with very little knowledge of the system architecture causing minimal harm to the system. Medium attacks, can be executed where certain level of knowledge of the system is required, in order to disrupt system operability. Attacks on the high level can be executed if the adversary has thorough knowledge of the system, enabling the adversary to produce a catastrophic outcome.

In Section 3.2 we have discussed that Automatic Dependent Surveillance-Broadcast (ADS-B) disseminates digital messages on two different frequencies, 1090-MHz and 978-MHz. Our research was designed to focus on attacks only on the ADS-B 1090-MHz broadcast link, which is 112-bits long and contains 56-bits of ADS-B information as illustrated in Figure 11.

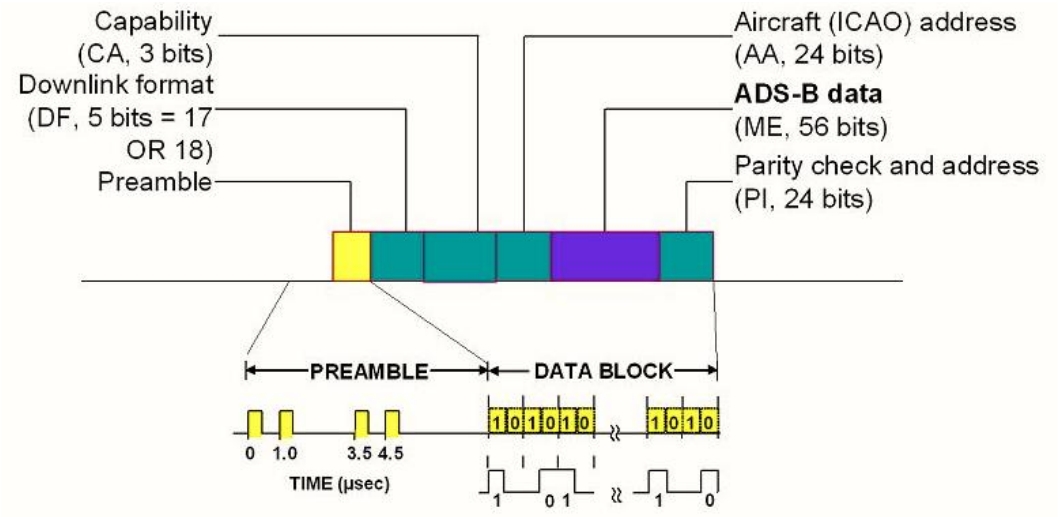

Figure 11: 1090-MHz Message Format [17]

Aside from attacks on 1090-MHz broadcast link, we will assume that the malicious actor with adequate set of skills can execute both internal and external attacks on the distributed computer network (e.g. NextGen) affecting aircraft and ground stations. We take the

vulnerabilities of GPS and ADS-B discussed in section 3.4, one step further by providing a detailed description of the attacks dealing with data corruption, spoofing, and jamming. The TVA matrix provides short descriptions of threats, vulnerabilities, and attacks in both sections 4.3.1 and 4.3.2 with the idea to aid the reader.

4.3.1 GPS Attacks

GTVA1. Jamming: A jamming attack is a denial-of-service attack (DOS) against positioning systems due to weak signal transmission from the satellite. This attack allows an adversary to interfere with the message/signal transmission by the navigation system, leading to reduced probability of successful message reception by the receiver. The consequence is that it prevents the receiver (e.g. pilot, controller) from determining a correct position of the aircraft. This GTVA is ranked as low [42]; [8]; [10].

GTVA2. Signal-Synthesis: This attack generates and sends out incorrect navigation messages/signals with the idea to mislead the receiver (e.g. pilot, controller) by showing different position on its display, than the actual position of the aircraft. To accomplish this, an adversary can use power amplifier and an antenna in order to broadcast false navigation signals. This GTVA is ranked as low [8].

GTVA3. Wormhole: This attack is similar to the Signal-Synthesis one, with the exception that the adversary intercepts and passes the messages/signals through various tunneled routes. The idea is to gather signals to a spoofed location and relay the signals from there to the actual destination. Since wireless transmissions travel at different speeds and routes, the tunneled route might be preferred option for the receiver based on the distance and speed of delivering the messages/signals. In which case, the pilot will accept the false messages/signals and make incorrect decision about its aircraft position reading. This GTVA is ranked as medium [8]; [10].

GTVA4. Selective-delay: Because radio frequency-based positioning systems, calculates their position by time of arrival (TOA) of the navigation signals, a malicious actor can execute a selective-delay attack. An adversary delays each navigation signal in a way such that the receiver calculates a false position, allowing the adversary to spoof the receiver for the entire coverage area of the signals. This GTVA is ranked as medium [8].

GTVA5. Counterfeit correction message: An attack that intercepts and directly forges correction messages. By working with forged correction messages, a pilot will calculate a false position. Furthermore, an adversary may execute an attack on the reference stations, causing them to generate false correction messages. This GTVA is ranked as high [8].

GTVA6. Shifting the tracking point: Having the signal arrive on time is known as tracking point in global positioning systems literature. An adversary can manipulate a tracking point by adding a replacement signal on top of the original pulse, leading the receiver to identify a wrong tracking point. This GTVA is ranked as high [42].

GTVA7. Tamper the receiver: Software and hardware updates can be executed on the receiver, if an adversary gains physical access to it. This tampering could lead to the receiver displaying falsely calculated positions. This GTVA is ranked as medium [8].

GTVA8. Collusion: A group of adversaries work together in cooperative manner to inject false communication into the system thus overpowering the legitimate communication. The idea is to make the targeted receiver unable to send and receive messages/signals. In addition, the targeted receiver might be reported as being malicious. This GTVA is ranked as high [10].

4.3.2 ADS-B Attacks

TVA1. ADS-B Message Corruption: An attack where remote manipulation of GPS readings can lead to false position data on aircrafts display. With such corrupted information,

an adversary may delay flights and even produce false traffic information. This TVA is ranked as medium [53].

TVA2. ADS-B Message Misuse: Through passive eavesdropping an adversary can identify, locate and track aircrafts with very high accuracy. This kind of attack is called side channel attack and can expose an aircraft's fuel level to the malicious actor by capturing exchanged data between aircrafts and ground stations. Furthermore, real time movement of the aircraft could also be reviled from gaining access to the public database. This TVA is ranked as low [53].

TVA3. ADS-B Message Delay: An attack where deliberately jamming is executed on the aircraft wireless communications in order to disrupt ADS-B services in certain locations, therefore leading to loss of aircraft visualization. This TVA is ranked as low [53].

TVA4. Corruption of Information Assets: The adversary may attempt to interfere with communications in order to interrupt proper operation of the system, creating false alarms and allowing for late detection to occur in the system, leading to flight delays [53].

TVA5. False Alarm: In this attack an adversary deliberately injects incorrect settings into the aircraft configuration system software. This tampering can cause the aircraft configuration to appear faulty therefore leading to unauthorized flight delays. This TVA is ranked as medium [57].

TVA6. Aircraft Reconnaissance: In this attack an adversary intercepts, recognizes and interprets ADS-B messages. Thus, an adversary can locate certain aircraft in the global airspace. This TVA is ranked as low [43].

TVA7. Ground Station Flood Denial: Focusing on the ground station an adversary can jam the ADS-B data link (e.g. the 1090-MHz ES) using a cheap jamming device. This way an adversary may interrupt only transmission of ADS-B signals intended for the ground station, but not all broadcast signals. This TVA is ranked as low [43].

TVA8. Ground Station Target Ghost Inject: An adversary can replace the original parameters of an ADS-B signal and insert malicious strings, designed to attack a ground station, therefore creating confusion by injecting "phantom aircrafts" on the display screen used by the controller to monitor air traffic. This TVA is ranked as medium to high [43].

TVA9. Aircraft Flood Denial: This attack allows an adversary to establish close proximity to aircraft location in real-time. In such case an adversary will use sophisticated jamming device to disrupt landing, takeoff and taxing operation of the aircraft. This TVA is ranked as medium [43].

TVA10. Aircraft Target Ghost Inject: This attack is similar to the Ground Station Target Ghost Inject, except that the goal of the adversary is to inject "phantom aircraft" into the aircraft cockpit display. This TVA is ranked medium to high [43].

TVA11. Ground Station Multiple Ghost Inject: By executing this attack an adversary can replace the original parameters of an ADS-B signal and insert malicious strings, designed to attack a ground station. The difference between this attack and TVA8 is that, this attack allows an adversary to insert several "phantom aircrafts" at once leading to traffic congestion in the air traffic management display of the controller. This TVA is ranked as medium to high [43].

TVA12. In-Aircraft Network Malware: This attack targets the wireless electronics carried by passengers onboard. An adversary can use the internal aircraft network to gain access to passenger devices that could potentially access aircraft system interfaces, thereby misusing the operability of such interfaces. This TVA is ranked as medium [57].

TVA13. Flame Malware: This attack uses a worm capable of stealing data information and disguising itself from antivirus and tracking tools. An adversary can use this worm to gather information about the network architecture and collect sensitive avionics data. This TVA is ranked as low [6].

TVA14. Software Incompatibility: This attack allows an adversary to intercept the distribution of software. It gives the adversary the chance to manipulate software updates intended for aircraft systems operation. This TVA is ranked as medium [57].

Furthermore, the aviation industry security has been jeopardized in the past by allowing the malicious actor to execute the additional attacks summarized in table 4:

Table 4: History of cyber security threats in aviation, modified from [9]

- In 2009, an FAA server was compromised allowing an adversary to steal 48,000 employee Social Security numbers - In 2008, 800 cyber incident alerts had been registered at ATC facilities and over 150 incidents remained unsolved - In 2007, a virus loaded into Thai Airways Electronic Flight Bag, spread to other electronic flight bags in addition to disabling the electronic flight bag	- In 2006, a virus spread to FAA's air traffic control systems caused portion of the air traffic control systems to shutdown in Alaska - In 1997, a skilled hacker broke into a Bell Atlantic computer system, causing FAA radio tower and runway lights transmitter to shutdown

Since we have investigated possible attacks on ADS-B, we felt it will be good to also emphasize some mitigation techniques for some of these attacks proposed by engineers and academia. The major limitation in this section however is the fact that most of the publications do not provide mitigation techniques for the specific attacks we have analyzed herein, but rather they use a general approach where attacks are grouped together and a mitigation technique for such a group is proposed. We are not experts in this field and therefore we feel it would not be right for us to try to connect a specific mitigation technique proposed by others to a specific attack, since we may do it wrongly, hence the reason for taking a general approach. These mitigation techniques therefore include the following:

M1. For proper ADS-B position verification, Costin proposes use of multilateration and radar [11]. Multilateration is basically a technology developed specifically for the military to

enhance accuracy in tracking aircraft. It involves measuring the Time Difference of Arrival (TDOA) for aircraft by many ground stations located strategically. These stations send interrogation signals and listen for replies. The replies will arrive at different times to the many different stations due to difference in distance between the aircraft and the ground stations. From this timing information, the precise aircraft position can be accurately determined and communicated to other aircraft. A ground station and other aircraft can therefore correctly verify the position of any aircraft hence preventing an attacker from lying about the position of any aircraft to other aircraft or to the control tower. This solution though expensive due to the many ground stations required, and was specifically for the military; it is feasible and has been successfully implemented in some parts of the world. A good case is at Narita International airport in Japan, where multilateration was adopted to ensure safe and smooth operations at the airport, by providing accurate and highly reliable surveillance information to aircraft controllers [62].

M2. To ensure message verification, engineers and researchers, from both the engineering community and academia, are exploring whether or not it is possible to employ cryptography [11]. One of the major challenges with this technique is incompatibility, since there's no standard cryptographic infrastructure being used worldwide. The other challenge is the lack of public key infrastructure in some parts of the world, especially in the developing world.

M3. To protect against misuse of ADS-B data, the engineering community has proposed a solution being referred to as privacy mode, which works by prompting an aircraft to generate a random identifier as a pseudonym. However, this method cannot make aircraft fully untraceable, due to the short periods between exchanged messages in ADS-B and the fact that strong spatial and temporary correlation between aircraft locations exists because of the underlying predictable mobility of aircrafts. Researchers also suggest that symmetric key

based solutions, may be an efficient way for ensuring integrity, authenticity and confidentiality of data, while at the same time, proposing message authentication codes or keyed hashes to be used for message signing [11].

M4. Feng Ziliang and co-authors [27], proposed a data authentication solution for an ADS-B system based on X.509 certificate. They argue that there are two possible ways of manipulating ADS-B data: one way is to manipulate valid data and send it on time to the intended source while the second option is to perform a replay attack where an attacker records valid ADS-B data in advance and resends the data later. They therefore propose a solution for data authentication that uses timestamp data from the GPS to protect against data replay attacks. Second their solution demands that the original ADS-B out payload and the timestamp data should be signed by an algorithm referred to as Elliptic Curve Data Signature Algorithm (ECDSA) with the elliptic curve cipher (ECC) private key. The signature data is encapsulated in a new data type called ADS-B out, which will be defined to accommodate new signature data. The new data will be sent together with original payload data through the ADS-B communication channel. The signature is mainly for ensuring that the message received is the original message that was sent out from the source. To better understand how this works, kindly refer to the publication [27]. The feasibility of this solution cannot really be proved since it is yet to be tested on a real aircraft. The laboratory tests carried out by the authors however proved that the solution is valid and suitable for the verification of ADS-B out data [27].

4.3.3 Additional Attacks

Based on the results discovered in section 4.3.1 and 4.3.2 of the proposed system architecture, additional attacks and mitigation techniques are described below. Furthermore,

the shift from radar-based technology to NextGen means a shift from voice to data. Therefore, this shift implies the presence of a wireless network since aircraft have to exchange information among themselves, or exchange information with the ground aircraft control towers. With this assumption, it is therefore our feeling that the engineering community that has so far evaluated security risks on NextGen and ADS-B technology has overlooked some security threats stemming from the fact that there's data transmission through an open channel. Furthermore, NextGen is still a work in progress, therefore these threats may be mitigated by the time the whole system is ready for implementation worldwide.

A1. Distributed Denial of Service (DDOS): In the ADS-B protocol, aircraft broadcast plain-text information to each other. Any device installed with an ADS-B component will receive the broadcast information, including an adversary with ADS-B component [11]. Malevolent data may therefore be broadcasted to aircraft by a malicious attacker, which upon their execution, the aircraft joins a botnet or a group of zombies, which the attacker can then use to shutdown the surveillance network, and spread the malware to other aircraft with the intent of shutting the surveillance network down, hence completely disabling it.

A2. Man-in-the-Middle: This attack allows an adversary to establish a communication link between communicating parties on the network. In such case, the communication between two parties will not take place over a private connection and will be controlled by the adversary. A genuine aircraft may unknowingly connect directly to a malicious aircraft, which may lead to access of sensitive information by the attacker, which can later be used for the attacker's own benefits.

A3. Message Replay: This attack allows an adversary to rebroadcast previous messages on the communications network leading to system reset. Aircraft and/or the surveillance network maybe flooded with more messages than what their capacity can hold by many fake aircraft.

A4. Message Redirection: Here an adversary can redirect ADS-B messages on the communication link. By doing this, an adversary can inform the communicating parties of the best path to reach a destination. An adversary can intercept a message from the pilot and engage in legitimate communication, making the pilot believe it is communicating with the ground station.

A5. Impersonation: This attack allows an adversary to masquerade as a legitimate user and execute malicious actions on the distributed network architecture. An adversary can then deliberately turn off the ADS-B functionality of an aircraft, making the aircraft disappear from the controller's monitor and monitors of other ADS-B equipped aircraft.

A6. Trapdoor: An adversary can gain backdoor access to the system components due to a security hole overlooked at the time of design, development, and implementation of the system architecture. An adversary can use this privilege to modify the software and hardware code or insert worms to mimic legitimate flow of data communication on the network.

A7. Zero Day: This attack basically exploits any security vulnerability exactly on the day the vulnerability is discovered. There are literally zero days between the discovery time and the first attack. This is risky especially if an attacker discovers it first and there's no time to protect against it. Since this system is still a work in progress, we believe it is susceptible to zero-day attacks since no one is certain of the final implementation, which should be in place by 2025. Any attacker can therefore discover vulnerability and exploit it to attack the system before the concerned authorities know about it.

MA1. To ensure that there is no malware that can be used to either recruit aircrafts as agents, handlers or zombies, one can use closed multicast groups with ingress filtering so that any incoming traffic from the other members in the group is filtered. This is because one member of the group may have been compromised and therefore being used to spread the malware to the others in the group.

MA2. To prevent a malicious aircraft from gaining access to the information being exchanged by genuine aircraft, closed multicast groups could be a good mitigation technique. It works because the malicious aircraft will not be in the multicast group.

MA3. Message replay attacks can be prevented through time stamping. For instance, aircraft exchanging messages or aircrafts communicating with a control tower periodically broadcast the time on their clocks. The receiving aircraft or control tower should only accept messages for which the timestamp is within a reasonable range.

MA4. Use of closed multicast groups could be a good way to prevent against message redirection attacks. Aircraft are grouped together and only members of this group can exchange ADS-B messages with each other. This technique therefore prevents a non-member from accessing information or communicating with any of the members of this closed group.

MA5. A possible mitigation technique is to use strong passwords that cannot be easily guessed nor are susceptible to brute force attacks, to prevent unauthorized access to the system. Closed multicast groups could also be another way to prevent such attacks, whereby only members in the group can exchange messages with each other. Other members in the group will only receive a broadcast from any member belonging to the same group.

MA6. The best way to prevent against exploitation of the trapdoor, by would-be attackers, is to either ensure all existing backdoors are well documented, have strong passwords, or that no backdoor exists in the system at all. The documentation is important if they exist because system designers need to access the backend from time to time, and backdoors provide the avenue through which they can access the system.

MA7. The best way to protect against zero day attacks is to deploy intrusion detection systems. This is because at the time of the attack, only the attacker has prior knowledge about this attack; such a system would detect any attempts to attack the system for necessary protection mechanisms to be put in place.

4.4 Summary

The first part of the summary provides a holistic approach of threats, vulnerabilities and attacks associated with the NextGen with respect to ADS-B and GPS. The adversary knowledge level of the system architecture has been categorized as low, medium, and high, as we indicated at the beginning of this chapter. Furthermore, we have included an analysis on how a specific TVA affects confidentiality, integrity, and availability of messages exchanged. Lastly, some TVA's affect all three pillars of CIA, while others only two or one as illustrated in Table 5.

Table 5: Summary of the TVA matrix

Threats, Vulnerabilities, and Attacks (TVA)		Description	Rating	Confidentiality	Integrity	Availability
GPS Attacks	GTVA1	Jamming	Low			X
	GTVA2	Signal-synthesis	Low		X	
	GTVA3	Wormhole	Medium		X	
	GTVA4	Selective-delay	Medium		X	
	GTVA5	Counterfeit correction message	High	X	X	
	GTVA6	Shifting track point	High		X	
	GTVA7	Tampering the receiver	Medium		X	
	GTVA8	Collusion	High		X	X
ADS-B Attacks	TVA1	Message Corruption	Medium	X	X	X
	TVA2	Message Misuse	Low	X	X	
	TVA3	Message-Delay	Low			X
	TVA4	Corruption of Information Assets			X	
	TVA5	False Alarm	Medium		X	X
	TVA6	Aircraft Reconnaissance	Low	X		
	TVA7	Ground Station Flood Denial	Low			X
	TVA8	Ground Station Target Ghost Inject	Medium to High	X	X	
	TVA9	Aircraft Flood Denial	Medium		X	
	TVA10	Aircraft Target Ghost Inject	Medium to High		X	
	TVA11	Ground Station Multiple Ghost Inject	Medium to High		X	
	TVA12	In-Aircraft Network Malware	Medium	X	X	
	TVA13	Flame Malware	Low	X		
	TVA14	Software Incompatibility	Medium	X	X	

The second part provides a summary of additional attacks we identify in section 4.3.3. These attacks are only related to the Next Generation Air Transportation System and ADS-B system architecture. The effects of these attacks on the confidentiality, integrity, and availability have been highlighted in Table 6.

Table 6: Summary of additional attacks

Attacks (A)		**Description**	**Security Property Affected**
Attacks	A1	Distributed Denial of Service (DDOS/DOS)	Availability
	A2	Man in the Middle	Confidentiality and Integrity
	A3	Message Replay	Confidentiality and Integrity
	A4	Message Redirection	Integrity
	A5	Impersonation	Confidentiality and Integrity
	A6	Trapdoor	Confidentiality, Integrity and Availability
	A7	Zero Day	Confidentiality, Integrity and Availability

5

Conclusion and Recommendations

5.1 Conclusion

The NextGen and ADS-B are essential in achieving a robust and well-organized air transportation system by providing real-time data to pilots and controllers. We cannot assume that NextGen will have suitable security measures in place at the time of deployment. In this thesis, we have identified and described possible security threats and vulnerabilities for NextGen and ADS-B aviation technology. For this purpose, we have developed a TVA matrix to provide a holistic summary of major attacks associated with these vulnerabilities, which arise from the network characteristics of implementing ADS-B. We have assessed these attacks by studying an abundance of literature. The TVA matrix provides descriptions of how these attacks could affect the functionality of NextGen if adequate security measures are not implemented. Our findings have identified additional attacks, which we believe have been overlooked by the engineering community. Additionally, we have discussed the importance of NextGen and the way it will transform the future air traffic management infrastructure, address passenger and airport capacity increase by introducing new technologies and procedures. We hope that the TVA matrix in this thesis can establish a common set of criteria that can ensure future experimentation on attacks associated with NextGen and ADS-B. Even though these attacks are not new, as time elapses these attacks can become more sophisticated and harder to

protect against. By using the TVA matrix, more people can efficiently gain a better understanding of the vulnerabilities associated with the NextGen and ADS-B systems. To our knowledge, this matrix is the first of its kind to provide a synopsis of security attacks on NextGen and ADS-B.

We have discussed and proposed mitigation techniques for the TVA matrix and for the additional attacks respectively. However, we feel some of these techniques are feasible and therefore can be implemented while others cannot, due to different constraints such as cost and infrastructure complexity. The intrusion detection system, closed multicast groups, and time-stamping can be adopted because of their cost efficiency and minimal infrastructure modification. On the other hand, limited number of techniques proposed for the TVA matrix may not be feasible. This is because they are neither cost-efficient nor supported by the existing infrastructure. Such example is M2 and M3, which require data encryption, therefore limiting the scope of international operability because there is no common public key infrastructure accepted worldwide.

Not all countries will benefit from NextGen equally; this is mainly because of government restrictions and lack of available funds. In addition, funding constraints have already caused deficiencies in the implementation process of NextGen. The government laws and policies will significantly delay the implementation process as well. Even though our research focused on U.S., the same principles regarding policy making and political debate will have a tremendous impact on the implementation decision in other countries.

Understanding the security risks and their capabilities can provide valuable information to the research community and other projects. According to Plato, *"the beginning is the most important part of the work."* Hence, addressing adequate security measures during the early stages of implementation of Next Generation Air Transportation System is vital.

5.2 Summary of Contributions

- We have invented a TVA matrix, which addresses possible attacks on ADS-B and GPS systems.
- The main contribution of this thesis is the TVA matrix table, which provided a summary of weaknesses associated with the NextGen technology with regards to confidentiality, integrity, and availability of data messages.
- We have suggested additional attacks and mitigation techniques, which could be executed on the current infrastructure of the system being studied.
- We support the idea that summary of attacks (e.g. TVA matrix table) are effective for aiding further design and development of newer technologies.

5.3 Recommendations for Future Research

In this thesis, we propose a good starting point in addressing and developing security measures for NextGen. More aggressive approaches to tackling security risks are strongly suggested because they will minimize the risk of vulnerabilities and threats. Providing training material to educate and empower the developers of NextGen and stay up to date with common threats related to cloud computing would be a great step forward. Close collaboration between various institutions could lead to developing new technologies capable of mitigating attacks on the NextGen infrastructure.

We recommend that an authentication mechanism be introduced on NextGen. Having an authentication method in place could reduce the complexity of detecting malicious actors. The use of a combination of secret keys and secret numbers will allow the communication between aircraft to aircraft and aircraft to ground to be authenticated. This means that the receiver can associate the messages being transmitted to a genuine source. By using the secret key on the communication devices, a form of validation is possible between those devices, if a device

does not possess a secret key can not engage in transmission of messages. In addition, a pilot will be required to enter a secret number, a combination of the secret key and secret number will then be validated and compared to information stored at a remote database, prior to sending or receiving a message.

Second, we propose that by use of digital certificates, message validation is possible therefore reducing the risk of malicious activities on the aircraft infrastructure. Digital certificates should be implemented at different phases of operation, when the aircraft is parked on the ground or when it is airborne. In addition, they can be embedded in an individual device of the aircraft network or one common digital certificate can be used for the entire network. Defining common criteria to implement and manage digital certificates on an aircraft can be of a great benefit to the airline industry allowing the lifecycle process of the digital certificate to be closely and carefully inspected and maintained.

The third proposal is improving in-flight security whereby moving forward, the modern aircraft will have an built-in complex network system, therefore threats need to be addressed adequately.

We also propose research programs whereby government institutions should be more involved by providing funds and creating programs for graduate students to pursue careers in engineering, while acquiring the necessary skills to enhance security of communication and information infrastructure.

Our last proposal is introduction of a Security program. The FAA should consider improving its security policy to ensure integrity of assets and address concerns related with the use of network centric architecture. NextGen relies on number of interconnected systems therefore some of the weaknesses discussed here could affect the intended operability of other sub-systems. Firewalls and Intrusion Detection Systems must be supported.

The information provided in this thesis can be used to solve similar problems in other

industries, deploying NextGen type of infrastructure. Additionally, further research is needed in order to develop security standards capable of mitigating the vulnerabilities and threats discussed herein.

Bibliography

[1] AAAE, “Air Traffic Control, Airspace and Navigational Aids,” 2005.

[2] FAA, “Federal Aviation Administration,” 2011. [Online]. Available: http://www.faa.gov/nextgen/implementation/programs/adsb/. [Accessed February 2013].

[3] J.R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2 ed., Wiley Publishing, Inc, 2008.

[4] ARC, “Recommendations to Define a Strategy for Incorporating ADS-B In Technologies into the National Airspace System,” 2011.

[5] ARC, “Recommendations on Federal Aviation Administration Notice No. 7-15, Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Notice of Proposed Rulemaking,” 2008.

[6] J. Veoni, J. Miller and R.Bigio, “Enterprise Information Systems Security for NextGEN,” in *2012 Cyber Proceedings: Right Topic.Right Time. ATCA’s 2012 Aviation Cyber Security Day*, 2012.

[7] A4A, Airline Handbook Chapter 1: Brief History of Aviation, 2013.

[8] S. Lo, D. D. Lorenzo, D. Qiu, C. Paar, P. Enge and George T. Becker, “Efficient authentication mechanisms for navigation systems- a radio-navigation case study,” 2009.

[9] C. Riley and D.R. Cerchio, “Aircraft Systems Cyber Security,” in *Institute of Electrical and Electronics Engineers, Digital Avionics Systems Conference*, 2011.

[10] J. J.Haas, Y.C. Hu and J.T. Chiang, “Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration,” in *Proceedings of the second ACM conference on wireless network security*, 2009.

[11] A. Francillon and A. Costin, “Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices,” Sophia-Antipolis, 2012.

[12] Deloitte, “Transforming the Air Transportation System,” 2011.

[13] FAA, “FAA Faces Significant Risks in Implementing the Automatic Dependent Surveillance-Broadcast Program and Realizing Benefits,” 2010.

[14] FAA, “Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Final Rule,” 2010.

[15] J. A. V. NTSC, “vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System,” 2001.

[16] EUROCONTROL, “EUROCONTROL,” 2013. [Online]. Available: http://www.eurocontrol.int/surveillance/cascade. [Accessed April 2013].

[17] EUROCONTROL, “ATMTraining Zone,” March 2013. [Online]. Available: https://trainingzone.eurocontrol.int/ATMTraining/PreCourse/SUR/ADS/Taste%20the%20Course/32501.10.32657.85.28722/Default.html. [Accessed April 2013].

[18] FAA, “NextGen Implementation Plan,” 2012.

[19] FAA, “FAA Flight Plan,” 2009.

[20] FAA, “NextGen Saves the Day in Juneau,” 2013.

[21] FAA, “Airport Surveillance Radar,” May 2009. [Online]. Available: http://www.faa.gov/air_traffic/technology/asr-11/. [Accessed April 2013].

[22] FAA, “Federal Aviation Administration Safety Management System Manual,” 2004.

[23] FAA, “Destination 2025,” 2011.

[24] FAA, “National Airspace System Capital Investment Plan FY 2013-2017,” 2012.

[25] FAA, “Fact Sheet - Next Generation Air Transportation System,” 2010.

[26] Fabrice, “ADS-B For General Aviation, ADS-B Explained,” March 2010. [Online]. Available: http://ads-bforga.blogspot.se/2010/03/ads-b-explained_15.html. [Accessed February 2013].
[27] P. Weijun, W. Yang and F. Ziliang, “A Data Authentication Solution of ADS-B System Based on X.509 Certificate,” in *27th International Congress of the Aeronautical Sciences*, 2010.
[28] flightradar24, “flightradar24,” March 2013. [Online]. Available: http://www.flightradar24.com/. [Accessed March 2013].
[29] GAO, “Next Generation Air Transportation: Collaborative Efforts with European Union Generally Mirror Effective Practices, but Near-Term Challenges Could Delay Implementation,” 2011.
[30] GAO, “Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed,” 2002.
[31] D. Hughes, “FAA Approves UPS ADS-B Operations,” 2008.
[32] T. Humphreys, “Statement on the Vulnerability of civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing,” 2012.
[33] J. Hurn, GPS, A Guide to the Next Utility, Trimble Navigation Ltd, 1989, p. 76.
[34] ICAO, “The Tenth Meeting of Automatic Dependent Surveillance-Broadcast (ADS-B) Study and Implementation Task Force,” Singapore, 2011.
[35] ICAO, “ICAO Environmental Report, Aviation and Climate Change,” 2010.
[36] ICAO, “Guidance Material: Security Issues Associated with ADS-B,” 2008.
[37] JPDO, “Concept of Operations for the Next Generation Air Transportation System,” 2007.
[38] JPDO, “Enterprise Architecture V2.0 for the Next Generation Air Transportation System,” 2007.
[39] JPDO, “Targeted NextGen Capabilities for 2025,” 2011.
[40] E. A. Lester and R. J. Hansman,“Benefits and Incentives for ADS-B Equipage in the National Airspace System,” 2007.
[41] K. Pan and W. Li, “Integrated Aviation Security for Defense-in-Depth of Next Generation Air Transportation System,” 2011.
[42] B. B. Peterson, P. K. Enge and S. C. Lo, “Assessing the Security of a Navigation System: A Case Study using Enhanced Loran,” 2009.
[43] D. L. McCallie, “Exploring Potential ADS-B Vulnerabilities in the FAA's NextGen Air Transportation System,” 2011.
[44] E. Mueller, D. Thipphavong, R. Paielli, J.H. Cheng, C. Lee, S. Sahlman, J. Walton and D. McNally, “A Near-Term Concept for Trajectory-Based operations with Air/Ground Data Link Communication,” in *27th International Congress of the Aeronautical Sciences*, 2010.
[45] NATCA, “A History of Air Traffic Control,” 2013.
[46] NIST, “Recommended Security Controls for Federal Information Systems and Organizations”.
[47] H. Abbass, S. Alam and L. Purton, “Identification of ADS-B System Vulnerabilities and Threats,” in *Australasian Transport REsearch Forum 2010 Proceedings*, Canberra, 2010.
[48] L. A. Reingold, “How Things Work: Aircraft Identification,” 2006.
[49] W. Risher., “FedEX becomes the first U.S airline to launch NextGen trial,” 2012.
[50] K. Rugg, “Aviation Safety Program,” 2013.
[51] V.D.L. Santos, “Aviation Systems Division: Modeling and Simulation,” 2011.
[52] V.D.L. Santos, “Air Traffic Management Research,” 2012.
[53] K. Sampigethaya and R. Poovendran,“Security and Privacy of Future Aircraft Wireless Communications with Offboard Systems,” 2011.
[54] K. Sampigethaya and R. Poovendran,“Visualization and Assesment of ADS-B Security for Green ATM,” in *Digital Avionics System Conference*, 2010.
[55] K. Sampigethaya and R. Poovendran, “A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance,” 2009.
[56] K. Sampigethaya and R. Poovendran, “Privacy of Future Air Traffic Management Broadcast,”

in *Digital Avionics System Conference*, 2009.
[57] K. Sampigethaya and R. Poovendran, “Secure Operation, Control and Maintenance of Future e-Enabled Airplanes,” 2008.
[58] C. H. Sharman, “Feds Push Satellite Technology to Make Skies and Runways Friendlier,” *Scientific American,* 11 November 2008.
[59] FAA, “System Wide Information Management, Program Overview,” 2011.
[60] “No Jam Tomorrow,” *The Economist,* March 2011.
[61] A. Turner, “Digital Decisions,” *Air Traffic Management .net,* 30 April 2012.
[62] T. Koga, E. Ueda, I. Yamada, Y. Kakubari, S. Nihei and Hiromi Miyazaki, “Evaluation Results of Multilateration at Narita International Airport”.
[63] A. L. Mozdzanowska, R.E. Weibel and R.J. Hansman, "Feedback Model of Air Transportation System change: Implementation Challenges for Aviation Information Systems," Institute of Electrical and Electronics Engineers, 2008.

Appendix B

Glossary of Terms

ADS-B Message – Information broadcast by the aircraft and vehicle containing set of parameters. In addition the message contains error protection information to reduce the risk of undetected errors in the decoding of the message by the receiving system

ADS-B In – A feature of the ADS-B system, which displays real-time ADS-B aircraft, feeds on a onboard cockpit display

ADS-B Out – A feature of the ADS-B system, which periodically broadcast very accurate aircraft position and traffic information

Adverse Actions – Actions performed by a malicious actor on a system resource

Attack – Intentional and unintentional violation of the security policy of a system

Attacker/s – An individual or group executing attack on a system property

Authentication – A procedure requiring password at login, to verify user's claimed identity

Bandwidth – The range of frequencies in a signal

Broadband – Use of signals over different frequencies for transmission of information

Coupling – Level of interdependence between software modules

Cryptography – A process of protecting information by using encryption (cipher text) and decryption (plain text) of messages

Cyber Security – Protection and recovery of onboard and ground systems from malicious intent

DHS – Responsible for enforcing security and safety of the United States from terrorist attacks and other disasters

Digital Signature – The result of a cryptographic transformation of data, which can be attached to transmitted messages to verify the authenticity of the sender

DOD – The Department of Defense, the larges organization of the U.S. federal government, which is responsible for providing national defense for protecting the United States

DOT – The Department of Transportation, a division of the U.S. federal government, which oversees the national transportation systems and infrastructure in the United States

Electronic Flight Bag – An electronic system mainly used in the cockpit, to display aviation data such as performance and fuel level

Encryption – Achieving data security by using asymmetric and symmetric key in order to protect data from unauthorized access

eEnabled Aircraft – An aircraft required to communicate with the ground station via distributed computer network for its operation

External Threat – A malicious actor not associated with an organization, trying to gain unauthorized access to the system

FAA – The Federal Aviation Administration, a division of the U.S. Department of Transportation, which oversees and regulates all aspects of civil aviation in the United States

Frequency band – A particular range of frequencies

Frequency spectrum – The distribution of signal amplitudes as a function of frequency

GPS Data Message – A part of the GPS signal, which contains information such as satellite location and clock data

ICAO 24 Bit Code – A uniquely assigned aircraft address usually in hexadecimal format

Interference – Unwanted signals in a receiver

Internal Threat – An individual authenticated and authorized by the system, which can execute malicious action

Ionosphere – A group of charged particles roughly 80 to 120 miles above the earth's surface

Jamming – Intentional interference to forcibly obstruct communication

Local Area Network – A data network allowing shared communication between computers in small geographical area

Malware – Malicious software designed to disrupt a system, with the idea to compromise the confidentiality, integrity, and availability of the data

NASA – The National Aeronautics and Space Administration, independent federal agency responsible for the development and implementation of the United States space program

NextGen – Transformation of the United States National Airspace System from a ground-based system of air traffic control to a satellite-based system of air traffic management

Noise – Unintentional interference

Radar – An abbreviation of Radio Detection and Ranging. By using electro-magnetic waves transmitted into the air, it can detect location, altitude, distance, speed and movement of moving and non-moving targets

Radio Frequency – Electromagnetic wave that oscillates between the audio and infrared in the electromagnetic spectrum

Satellite – Artificial craftsmanship built by mankind, launched into space orbiting the Earth used for scientific research and communications

Satellite Constellation – Satellite arrangement in space

Security – Preserves the information of a system from malicious intent. Therefore allowing for proper operation of the system elements

System-of-Systems – Combination of physical and logical view of multiple complex information systems, which involves connectivity and interaction among the systems

Threat – A situation, either intentional or accidental, that may affect the functionality of a system

Time of arrival – A travel time of the navigation signal between receiver and transmitter. The distance between the receiver and the transmitter is determined based on the time it took the signal to reach the receiver. Proper synchronization between the receiver and the transmitter is necessary to compute the accurate travel time

Transmission Control Protocol/Internet Protocol – TCP/IP is the de facto standard for transmitting data over networks. TCP is responsible for correct delivery of data from client to server. IP exchanges packet of data from node to node

User Datagram Protocol – A connectionless protocol responsible for sending and receiving datagrams over IP network

Vulnerability – A weakness in the system that can be exploited to violate the system's intended behavior

Wireless Local Area Network – A (802.11) wireless data network using radio signals for short distance communication

Wireless Personal Area Network – A (802.15) personal wireless data network for interconnected devices in a workplace