UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Camilo Andres Pantoja Viveros

Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts

Master's Thesis (30 ECTS)

Supervisors: Prof. Olaf Manuel Maennel
Associated Prof. Raimundas Matulevicius

Tartu 2016

Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts

Abstract:

The present paper has a profound literature review of the relation between cyber security, aviation and the vulnerabilities prone by the increasing use of information systems in aviation realm. Civil aviation is in the process of evolution of the air traffic management system through the introduction of new technologies. Therefore, the modernization of aeronautical communications are creating network security issues in aviation that have not been mitigated yet. The purpose of this thesis is to make a systematic qualitative analysis of the cyber-attacks against Automatic Dependent Surveillance Broadcast. With this analysis, the paper combines the knowledge of two fields which are meant to deal together with the security issues in aviation. The thesis focuses on the exploitation of the vulnerabilities of ADS-B and presents an analysis taking into account the perspective of cyber security and aviation experts. The threats to ADS-B are depicted, classified and evaluated by aviation experts, making use of interviews in order to determine the possible impact, and the actions that would follow in case a cyber-attack occurs. The results of the interviews show that some attacks do not really represent a real problem for the operators of the system and that other attacks may create enough confusion due to their complexity. The experience is a determinant factor for the operators of ADS-B, because based on that a set of mitigations was proposed by aviation experts that can help to cope in a cyber-attack situation. This analysis can be used as a reference guide to understand the impact of cyber security threats in aviation and the need of the research and aviation communities to broaden the knowledge and to increase the level of expertise in order to face the challenges posed by network security issues. The thesis is in English and contains 58 pages of text, 5 chapters, 17 figures, 15 tables.

Keywords:

Aviation, Automatic Dependent Surveillance Broadcast, Cyber Security, Cyber Attacks

CERCS: P170 Computer science, numerical analysis, systems, control.

ADS-B süsteemile suunatud küberrünnakute analüüs lennundusekspertide seisukohast

Lühikokkuvõte:

Käesolev töö loob põhjaliku ülevaate lennunduses valitsevatest küberjulgeoleku ohtudest. Tsiviillennunduse lennuliiklusteenindus ja õhuseire on üleminekufaasis valmistudes kasutusele võtma uue põlvkonna tehnoloogiaid, mis tulevikus asendavad praeguse radaripõhise lennukite jälgimissüsteemi uue satelliitpõhise süsteemiga. Lennunduse sideteenuste moderniseerimine loob aluse uuetele turvalisusega seotud ohtudele, mille võimalikke negatiivseid tagajärgi ei ole suudetud veel maandada. Magistritöö eesmärk on koostada kvalitatiivne süstemaatiline analüüs võimalikest küberrünnakutest uue satelliitpõhise automaatse sõltuva seire üldsaade (Automatic dependent surveillance-broadcast –ADS-B) vastu. Analüüs ühendab teadmised küberturvalisuse ja lennunduse valdkonnast, mille koos käsitlemine on oluline turvalise tagamise sesiukohalt. Töö fokusseerub ADS-B süsteemis esinevatele kitsaskohtadele, mis küberturvalise seisukohalt võivad kätkeda ohte või häirida tõsiselt lennuliiklusteeniduse tööd. Potentsiaalsed ohud ADS- S süsteemi vastu on kirjeldatud ja liigitatud sõltuvalt ohuastmest. Analüüsi põhiosa moodustab lennundus spetsialistide seas läbiviidud küsitlus, mille põhjal on hinnatud ohu tõsidust, selle mõju lennundussüsteemile ja milliseid toiminguid on vajalik rakendada ohu

esinemise korral. Töö analüüs hindab mõned käsitletud ohtudest ebaoluliseks, mis ei kujuta endast märkisväärset probleemi süsteemi operaatoritele. Sellegi poolest esineb teatava keerulisuse astmega ohustsenaariumeid, mille tagajärjel on süsteem tugevalt häiritud või millega võib kaasneda ulatuslik kahju. Läbiviidud küsitluse põhjal on esitatud meetmeid, kuidas maandada võimalikke negatiivseid mõjusid ohuolukorras. Töö tulemused on olulised pööramaks tähelepanu lennunduses esinevatele küberohtudele. Töö on kirjutatud inglise keeles ja sisaldab 58 lehekülge, 5 peatükki, 17 joonist ja 15 tabelit.

Võtmesõnad:

Lennundus, Küberkaitse, Küberrünnakud, Automaatse Sõltuva Seire Üldsaade

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine

Table of abbreviations and terms

ADS-B	Automatic Dependent Surveillance Broadcast
ANSP	Air Navigation Service Provider
ATN	Aeronautical Telecommunication Network
CO_2	Carbon Dioxide
CRC	Cyclic Redundancy Code
COTS	Commercial-Off-The-Shelf
CDTI	Cockpit Display of Traffic Information
CPDLC	Controller Pilot Data Link Communications
DME	Distance Measuring Equipment
EFB	Electronic Flight Bag
FAA	Federal Aviation Administration
FIS-B	Flight Information Services Broadcast
FLS	Field Loadable Software
FMS	Flight Management System
GBAS	Ground-Based Augmentation System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
IFE	In-Flight Entertainment
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
IPS	Internet Protocol Suite

LFR	Low Frequency Radio
MLS	Microwave Landing System
MTCD	Medium-Term Conflict Detection
NDB	Non-Directional Beacon
NextGen	Next Generation Air Transportation System
NRA	Non-Radar Areas
PSR	Primary Surveillance Radar
RNAV	Radar Navigation
RVSM	Reduced Vertical Separation Minimum
SESAR	Single European Sky ATM Research
SSR	Secondary Surveillance Radar
STCA	Short-Term Conflict Alert
TCAS	Traffic Collision Avoidance System
TIS-B	Traffic Information Service Broadcast
UAV	Unmanned Aerial Vehicle
USRP	Universal Software Radio Peripheral
VHF	Very High Frequency
VMC	Visual Meteorological Conditions
VOR	Very High Omnidirectional Range

Table of Contents

1 Introduction 8
1.1 Problem Statement 8
1.2 Contribution of the Author 9
1.3 Thesis Limitations 9
1.4 Thesis Structure 9
2 Literature Review 11
2.1 Aviation 11
2.2 Aviation and Computer Science 12
2.3 Automatic Dependent Surveillance Broadcast 14
2.3.1 Vulnerabilities of ADS-B 17
2.3.2 Exploitation of ADS-B Vulnerabilities 18
2.3.3 Exploitation of GPS vulnerabilities 20
3 Methodology 21
3.1 Research Design 21
3.2 Qualitative Analysis Procedure 21
3.3 Interviews and Data Analysis 22
4 Findings and Analysis 24
4.1 Qualitative analysis of cyber-attacks against ADS-B 24
4.1.1 Aircraft Reconnaissance 24
4.1.2 Aircraft Target Ghost Inject 25
4.1.3 Ground Station Target Ghost Inject 27
4.1.4 Ground Station Multiple Ghost Inject 29
4.1.5 Replay Attack 31
4.1.6 Aircraft Spoofing 33
4.1.7 Virtual Trajectory Modification 34
4.1.8 Aircraft Disappearance 36
4.1.9 False Alarm Attack 38
4.1.10 Aircraft Flood Denial 40
4.1.11 Ground Station Flood Denial 41
4.2 Dynamic Analysis of Cyber Attacks against ADS-B 42
4.2.1 Threat Model 43
5 Conclusions and Recommendations 46
5.1 Conclusions 46

5.2 Recommendations 47
6 References 48
Appendix 54
Background of participants 54
Air traffic controllers questionnaire 56
Pilots questionnaire 57
I. License 58

1 Introduction

The development of new technologies have brought about concerns related with the safety of industrial aviation due to the vulnerabilities embedded in information systems [1]. The main objective of all the studies and research in process is to create state of the art technologies to enhance the communications, navigation and surveillance in order to provide pilots and air traffic controllers with timely information for the decision-making.

The International Civil Aviation Organization (ICAO) has made a huge effort in order to provide an appropriate set-up to allow Aeronautical Telecommunication Network (ATN) based on the Internet Protocol Suite (IPS) to meet the requirements for a reliable aircraft-to-aircraft and aircraft-to-ground communications[2]. With the enhancement of the communication in aeronautical networks, the interdependency of the systems involved poses more security issues [1]. One of the applications used for air traffic surveillance is the Automatic Dependent Surveillance Broadcast (ADS-B), which has vulnerabilities by design and its possible impact in airworthiness is not clear. [3]

Indeed, it is important to understand that the networks and nodes in aviation are not similar to a ground-based network of computer devices [4]. ATN is an Ad-Hoc wireless network that has a large number of mobile nodes, and this mobility becomes in the weakest point in the chain that the adversary might exploit in order to compromise the applications used in the communication [5].

The increasing involvement of computer science in aviation has caused the increment of a variety of vulnerabilities that might be exploited with different objectives in mind by cyber criminals. Moreover, there are relevant factors to comprehend the risk of a cyber-attack in aviation such as awareness, preparation, the impact in aeronautical operations, and the possible reactions of pilots and air traffic controllers in a hypothetical attack situation. Although some technology developments enhance information security, threat detection and network security in the aeronautical environment, it is completely clear that human decisions based on previous knowledge and abilities are still needed to cope in critical situations [6].

The aim of this thesis is to investigate the exploitation of ADS-B vulnerabilities and its impact in aeronautical operations. The review of the literature is grounded on the academic knowledge and research in aviation and cyber security fields. The study gathers essential information and a systematic qualitative analysis is made in order to understand how the aviation experts would proceed in a cyber-attack situation and which tools and procedures can be used to cope in a critical situation.

Furthermore, the study involves the author personal experience in military aviation field, which contributes to perform the analysis. To the best of the author knowledge, there is not any study which aims to analyze the possible effects of cyber-attacks against ADS-B and to determine the possible ways that aviation professionals would proceed in a cyber-attack situation.

1.1 Problem Statement

The objective of ICAO is to implement ADS-B in every airplane in the world by 2020. With the full implementation of ADS-B, Secondary Radar Surveillance (SSR) will be useless and Primary Surveillance Radar (PSR) might be used as a complement [7]. Aviation national organizations are claiming that the data fusion between PSR and ADS-B will take place, but at the same time they allude the discontinuation of PSR and SSR when ADS-B

is fully implemented [8], [9]. The system was designed without security measures and its vulnerabilities have not been addressed and mitigated completely [10].

There is no common vision, standards or strategy defining cyber security in aviation [11]. Consequently, this fact draws the attention to the lack of knowledge and awareness that pilots and air traffic controllers have about the vulnerabilities and possible effects of a potential attack [12],[13]. Therefore, it is relevant to analyze the possible impact that the cyber-attacks against ADS-B can cause to aviation system. Pilots and air traffic controllers take important decisions based on the instruments they have in the cockpit and air traffic control respectively, and wrong decisions might have undesirable effects on aviation.

Main issues addressed by this thesis are:

1 Exploitation of the vulnerabilities of Automatic Dependent Surveillance Broadcast.
2 Lack of understanding of security and safety risks prone by the vulnerabilities that might be exploited in a cyber-attack against ADS-B system.
3 Lack of understanding of the real issues that cyber-attacks against ADS-B could cause to pilots and air traffic controllers.

Research Questions: The primary questions that this study sought to answer are:

1 How does the exploitation of the vulnerabilities of ADS-B might confuse air traffic controllers and pilots to lead to a critical situation?
2 Which cyber-attacks against ADS-B can cause a major impact in aviation?
3 Which current procedures might be used by pilots and air traffic controllers to deal with the cyber-attacks against ADS-B?

1.2 Contribution of the Author

The contribution of this thesis is the analysis of the impact in aviation caused by the cyber-attacks which might affect to ADS-B. This analysis provides a better understanding of the effects in aeronautical operations and the procedures that aviation personnel might use in order to deal with a cyber-attack situation.

1.3 Thesis Limitations

The first limitation imposed to the development of this thesis is the restricted access to aviation documents. The description of the function and security vulnerabilities of ADS-B system are not publicly available due to the high level of confidentiality of the information.

The second limitation that the thesis faced is the amount of information the experts in aviation are allowed to disclose. The implementation of ADS-B is in process and that limits the number of authorized aviation personnel who have operated the system. The personnel contacted for the research were from aviation civil organizations of Colombia and Estonia, TESDA Research group and Colombian Air Force.

The third limitation is the legal restriction to perform a real attack in order to evaluate empirically the effects in aviation system. Despite of all the limitations posed to continue with the research, it was considered that the gaps could be filled with advisory and feedback received by aviation experts.

1.4 Thesis Structure

The goal of the thesis is to make a qualitative analysis of cyber threats, which might affect Automatic Dependent Surveillance Broadcast system in aviation, and to analyze how they

might affect to air traffic controllers, pilots and aviation safety based on the knowledge and perception of the aviation experts. The paper is organized as follows:

- Chapter 1. Introduction – gives a general explanation of the topic and the purpose of the thesis.
- Chapter 2. Literature Review – defines the two fields of the research, Aviation and Cyber Security, the vulnerabilities and exploitation of ADS-B system and defines the scope of this thesis.
- Chapter 3. Methodology – describes the methods used to make the qualitative analysis of the cyber-attacks against Automatic Dependent Surveillance Broadcast and the evaluation of the impact in aviation.
- Chapter 4. Findings and Analysis – this chapter provides the analysis of the cyber-attacks against ADS-B, the proposed mitigations for the attacks and the analysis of the impact in aviation given by aviation experts.
- Chapter 5. Conclusions and Recommendations – this chapter provides additional discussion in regards of the results and recommendations.

2 Literature Review

2.1 Aviation

Aeronautical transportation has been constantly developing from the outset in 1903 when the Wright Brothers made the first flight in history and it has not stopped its evolution yet. Nowadays, aviation is not only seen as the safest means of transportation [14] but it also has become in part of the critical infrastructure of many countries that have clearly established its protection, for instance United States which issued the Homeland Security Presidential Directive 7 for this purpose [15]. The importance of commercial aviation is not only focused on the transportation of great amount of passengers and goods but also it is key in the maintenance of the economy [16].

More than one hundred years of history with failures and accomplishments have turned aviation into the powerful set of state of the art technologies, high qualified personnel and safety environment that nowadays is essential for the life of many people in the world. According to Delloite [17] by 1919 it was already needed the application of rules to control the air traffic and the solution to this problem was the creation of the International Commission for Air Navigation.

The number of airplanes in the sky increased even more when the aircrafts were used for commercial purposes, like in North America to deliver the mail by the U.S. Postal Department. The development increased even more with the rush to have better airplanes for combat during the time of the First World War. It was not only the need to improve technology in the aircraft, but also the intrinsic requirement to control the air space [18].

Because of the improvements in technology and increased number of aircrafts, the air traffic control began to be more precise in the decade of 1930 when the air traffic controllers did not have the need to use archaic methods to safely separate aircrafts [18]. New devices were introduced such as beacons, radios and gun lights in order to improve the problems experimented by pilots in Instrument Meteorological Conditions (IMC), but these improvements were not completely accurate [19].

In the aftermath of the Second World War and with all the developments reached during this time, one of the most important progress in aviation was made with the creation of the radar system. This system equipped air traffic controllers with the ability to watch the movements of any plane that is in the range of the radar [17]. The increased necessity to install navigation systems in the aircrafts to help the pilots to fly in the right direction and to help them to land in adverse meteorological conditions brought about the introduction of radio navigation technologies such as Low Frequency Radio (LFR), Non-Directional Beacon (NDB), Very High Omnidirectional Range (VOR) and Distance Measuring Equipment (DME) [20].

After the 1960 decade, many new systems have been produced and new standardized procedures in manuals and approach charts were established to give pilots and air traffic controllers more accurate information to aid in navigation in order to execute a safe landing. Modern systems and concepts like the Instrument Landing System (ILS), Microwave Landing System (MLS), Area Navigation RNAV and Global Navigation Satellite System (GNSS) were introduced to provide more efficient paths to follow to save time and fuel and to supply accuracy in flight procedures [18].

2.2 Aviation and Computer Science

The revolution of the computer science could not be out of the way of aviation technology and with this the possibility to store, transmit and display digital information for the operators [19]. ICAO has already defined the concept of Cyber Security in Aviation in the document 9985. In specific terms, Cyber Security in Aviation was defined as follows: "*refers to all matters pertaining to the security of information and communication systems, technology or applications of all kinds. This includes analogue or digital devices, and encompasses radio, telecommunications, computer and network hardware and software, data storage systems and devices, satellite systems, surveillance systems, navigation systems, as well as the various services and applications associated with them"*[13],[21].

Information systems are increasing their role in aviation using cyber-physical elements to process and display data used by operators [22]. Today, these information systems are providing new capabilities that aim to improve the services, enhance processes and to increase the interconnection of aeronautical network devices [23]. There are new technologies and modernizations that are posing a new paradigm in terms of cyber security.

Many of these innovations have been made to support aircraft systems, for instance fly-by-wireless components, In Flight Entertainment (IFE) for passengers, air traffic management based on GPS reports and the communication between pilots and air traffic controllers through data link satellite-based systems. These enhancements have physical components that completely rely on aeronautical information systems in order to operate properly [24].

Furthermore, other transitions such as the increasing use of Commercial-Off-The-Shelf (COTS) software, Field Loadable Software (FLS) and the creation of the concept of autonomous flight for e-enabled aircrafts have facilitated air traffic management while lowering the maintenance and costs, but they are not meeting the security compatibility required to guarantee the standards of civil aviation [25]. In addition, the integration with aircraft and off-board systems has started to become closer than ever, creating cyber physical security considerations [26].

When it comes to think that an accident might be caused through cyber means, the current belief of that possibility is hardly considered. It is completely clear that most of accidents occurred in aviation have been caused due to human factor [27] -[29] and the known cyber security incidents in aviation have not caused any major impact in the safety of passengers and aircrafts as shown on Table 1. However, this list only shows the known cyber-incidents and it does not mean that the list is complete. Since there could be an unknown number of cyber incidents, which have not been disclosed to the public yet.

Nevertheless, it has been recognized that these cyber incidents do not really demonstrate the dangerous effect that actually they might cause [13], and because of these rising concerns, the credibility in aviation safety could be at risk. Some potential vulnerabilities have been disclosed by aeronautical organizations, hackers community and media as it can be evidenced on Table 2.

The evolution of information technology has reached aviation at any level. From the improvement of the surveillance, navigation and communication systems to the applications used by pilots to receive, store and display relevant aeronautical information, which is used for the decision-making in the cockpit. In spite of the FAA has approved in 2012 the use of many aeronautical applications in the Electronic Flight Bags [35], it has been demonstrated that since the software of those applications are not tested with the reliability standards used for built-in cockpit devices [36], they are vulnerable to cyber-attacks which might mislead the judgement of the pilots.

Table 1. Aviation Cyber Security Incidents.

YEAR	DESCRIPTION
1997	A hacker broke into a Bell Atlantic computer system causing that the Federal Aviation Administration control tower and the runway lights transmitter were shut down [30],[31].
2006	A virus spread into the air traffic control systems of the Federal Aviation Administration caused that a part of the air traffic control systems were shut down in Alaska[30].
2007	A virus was loaded into Thai Airways Electronic Flight Bags. The virus disabled the EFBs and it was spread to other electronic flight bags [30].
2008	800 cyber incident alerts were detected at air traffic control facilities and over 150 incidents have not been solved yet [30].
2009	A server of the Federal Aviation Administration was compromised and 48,000 employee social security numbers were disclosed [30].
2009	A truck driver carrying a Global Positioning System (GPS) jammer unintentionally caused outages to Newark Liberty International Airport's ground-based augmentation system (GBAS)[32].
2011	A group of software engineers was accused of disrupting operations at a new airport. There was a sabotage in the program code which caused that the check-in services failed and delayed a considerable amount of flights in many airports [33].
2014	Many aircrafts were vanished from the radar screens in Austria, Germany, Czech Republic and Slovakia. It was brought about by alleged military warfare exercises [34].

Finally, the Federal Aviation Administration in United States and EUROCONTROL in Europe are implementing NextGen and SESAR programs respectively, to modernize air traffic management and to improve the data link communications. Moreover, ICAO is supporting the implementation of similar programs all around the world in an attempt to standardize aviation [9]. These programs use advances in digital information technologies to increase the security, safety, operational efficiency, capacity and to lower costs and Carbon Dioxide (CO_2) emissions with the new regulations and technologies [17].

The Automatic Dependent Surveillance Broadcast system is an essential part of these programs, providing not only more accurate surveillance information than radars, but also it is expected to produce benefits such as capacity, safety and efficiency for aeronautical operations [42]. Nevertheless, these implementations pose new cyber security vulnerabilities to aviation due to the increased interconnectivity, integration and the interoperability of the involved systems [43].

Table 2. Potential Vulnerabilities Found in Aviation.

YEAR	DESCRIPTION
2008	The FAA stated that the proposed architecture of the Boeing 787 allows new kinds of passenger connectivity to previously isolated data networks, which are connected to systems that perform operations needed for the safety of the aircraft [37].
2010	The FAA published a notice indicating that some computer systems on the Boeing 747-8 and 747-8F may be vulnerable to outside attacks due to the nature of their connectivity [38].
2012	Andrei Costin demonstrated a weakness in the air traffic control. With low cost commercial hardware and software it was possible to spoof ADS-B signals to inject a ghost aircraft into ground control display [10],[33].
2012	Hacker demonstrated theoretically the possibility to use an Android to remotely attack and hijack an airplane [39].
2012	A potential vulnerability in Electronic Flight Bags programming could corrupt with malicious intentions when the devices are connected to external networks to receive updates [33]
2014	Security expert allegedly told that he was able to hack and to steer airliner mid-flight breaking into the In Flight Entertainment [40].
2015	WestJet aircraft was allegedly transmitting 7500 code, which indicates a hijacking. It was possibly a modification through cyber means [41]

2.3 Automatic Dependent Surveillance Broadcast

The aviation surveillance has been governed for the last six decades by radars. Old legacy radar systems have been the devices which air traffic controllers and pilots have trusted in to support their decisions when it comes to have a better traffic flow to any airport in the world. Currently, the radars are still the main system on which the air traffic control is used for aircraft surveillance [44].

The radar systems are categorized in two different types: Primary Surveillance Radar and Secondary Surveillance Radar. Primary Surveillance Radar (PSR) works sending signals that are evaluated according to the time elapsed from the signal is sent until the time signal is received again to the antenna after reflection on the aircraft [45]. This system is independent since it does not need of any additional device on the aircraft, it only provides position and it does not provide altitude nor identity [46]. The other type of radar operation is Secondary Surveillance Radar (SSR), which is a dependent system that sends interrogation signals to the aircraft. A built in device located in the aircraft called transponder responds to the request signals. The system is able to provide range, bearing, identity and altitude [47].

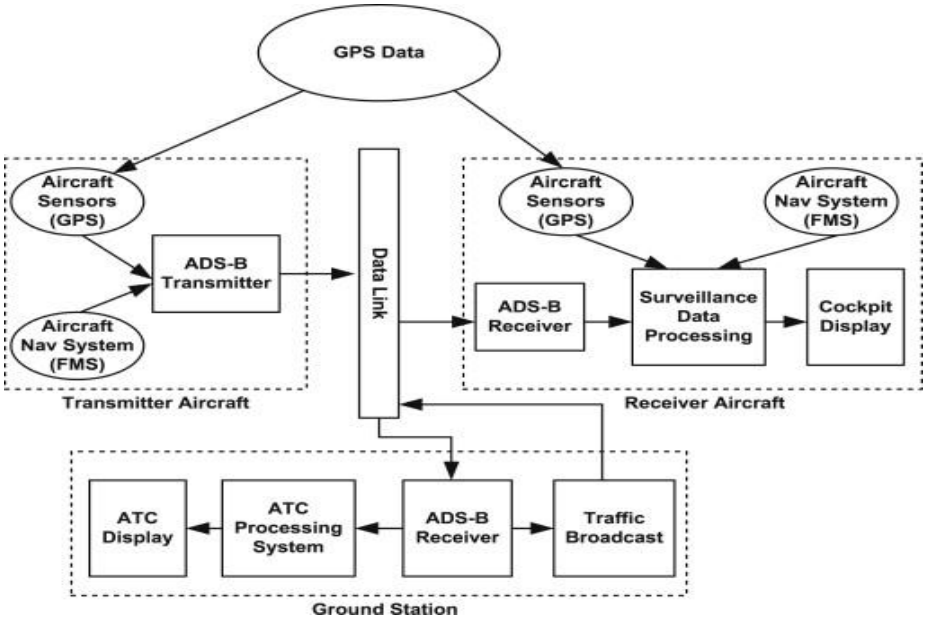

Figure 1. Main Components of ADS-B [7].

One of the main issues with radar systems is that they do not provide the required precision and do not have the detection accuracy for the growing air traffic flow [48]. As a solution to this problem, the implementation of ADS-B is in process. The Automatic Dependent Surveillance-Broadcast is the next generation system that is planned to replace the old standing radar systems [50]. The main purpose of ADS-B is to make use of Global Positioning System (GPS) and Radio Frequency (RF) data link to broadcast twice per second the aircraft information to airborne and ground receivers, instead of just responding to interrogations as it is standardized with radars [44].

The source of position information is provided by GPS system. The aircrafts have a transmitter, receiver and a processing device, which receives information from the GPS, and the Flight Management System (FMS) to provide an image to the pilot on the cockpit display. The FMS gives information about the flight plan, ensures the correct trajectory of the aircraft [49], and automates procedures when the aircraft is airborne. Moreover, the GPS sensors and FMS provide information to the transmitter to broadcast surveillance data to the other aircrafts and to the ground stations. The ground station executes the same process to display the information on the respective screen and, thereafter to broadcast the air traffic information [7]. The composition of ADS-B and its subsystems can be observed in Figure 1.

The purpose of ADS-B is to enhance capabilities of surveillance in every phase of the flight from the engine start until the shutdown, which means that even the movements on the ground during taxi and every airborne phase will be supported by ADS-B [50]. The onboard ADS-B system calculates the aircraft data using the GPS sensors and then the calculated data is combined with identification information to be broadcast through the ADS-B OUT subsystem [7].

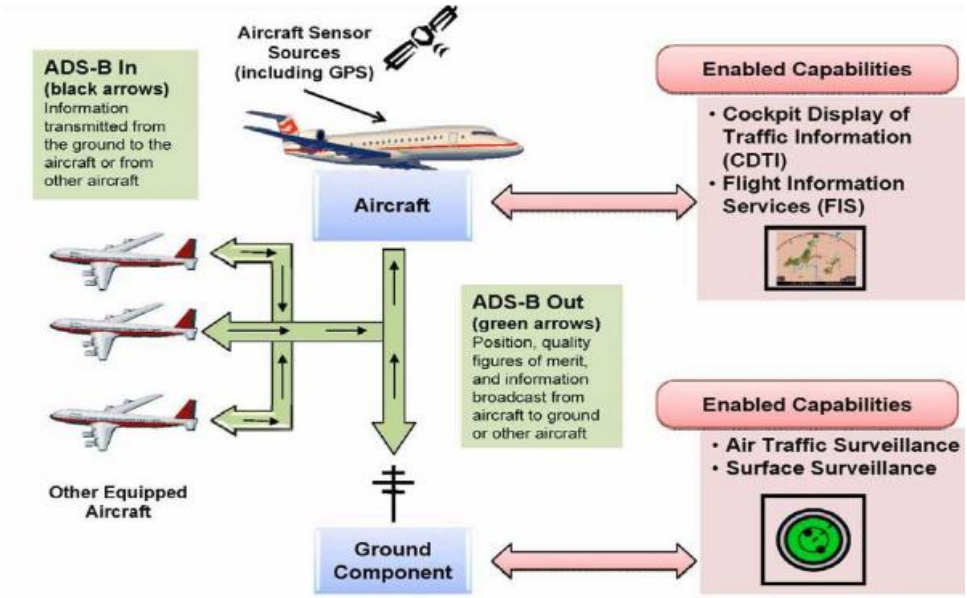

Figure 2. ADS-B Functional Diagram [51].

Afterwards the ADS-B ground stations, which are in the range, receive the signals and transmit the messages making use of the network backbone until they reach the ground control station [7] and the broadcast also reaches the nearby airplanes making use of the ADS-B IN subsystem [44]. Figure 2 provides an ADS-B functional diagram to understand the operation of ADS-B OUT and ADS-B IN subsystems and the interaction among aircrafts and ground stations.

With ADS-B, the information transmitted is processed by the aircrafts and ground stations so that the receivers can have a four-dimension trajectory to improve decision-making of pilots and air traffic controllers [50]. The messages transmitted by ADS-B contain the next information: aircraft identification, urgency code, intent and uncertainty level [52]. ADS-B is categorized as automatic since it does not require any input from the pilot or air traffic controller. It is dependent because the aircraft needs the GNSS in order to derive its location and it needs a transmitter in the aircraft to broadcast the messages [7]. Moreover, the accuracy is improved with ADS-B over the radars allowing to reduce the standard separation of aircrafts and to reduce time and consumption of fuel in flight procedures [53]. The Extended Squitter 1090ES in the 1090 MHz frequency and the Universal Access Transceiver (UAT) are the two data links which support ADS-B to enhance interoperability, regulatory and legacy purposes [10].

The design of ADS-B enhances the air traffic management by improving the situational awareness for the air traffic controllers on the surface while controlling aircrafts executing taxiing. It also enables greater agility to prevent mid-air collisions and is the perfect solution for areas where the use of radar systems is not possible like in Gulf of Mexico or where radars are not completely reliable like in Alaska due to the rugged terrain [7].

Furthermore, an additional improved characteristic is that the precision of ADS-B is not deteriorated with the distance and it maintains an accuracy of 20 meters that is significantly better than radar, which in 60 nautical miles is deteriorated to 300 meters of difference [53]. The complete implementation of ADS-B will allow the reduction separation between aircrafts in order to increase the capacity of the control for the airspace [50].

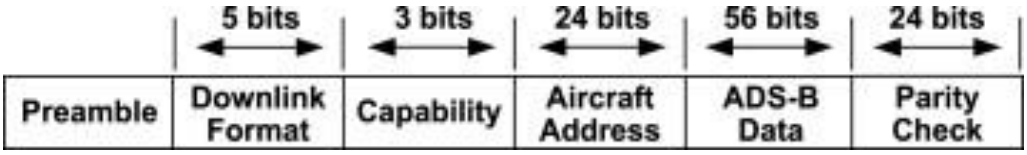

Figure 2. ADS-B Extended Squitter Format [7].

2.3.1 Vulnerabilities of ADS-B

The analysis of the vulnerabilities has to be executed in a way so that the most sensible components of the system can be included. The critical components of ADS-B are GPS, ADS-B transmitter, the data link medium and the ground systems for the air traffic control center [53].

A security assessment evaluates the vulnerabilities of a system based on the ability of the system to protect the confidentiality, integrity and availability of the data [7]. In the case of ADS-B the loss of confidentiality must be determined as completely obvious since the principle of the system is to openly broadcast the information constantly at a rate of 2HZ [54]. Although the information is available to anyone who has a proper ADS-B receiver, due to the lack of encryption on ADS-B [7], it has to be taken into account that many of the aviation services are required to be openly broadcast for safety and information purposes. For instance, some of these broadcast services are the Very High Frequency (VHF) radio signals, meteorological information for pilots such as Traffic Information Service Broadcast (TIS-B) and Traffic Information Service Broadcast (FIS-B) which provide relevant information of the traffic and meteorological conditions.

The real problem arises due to the sensible information transmitted through ADS-B about the aircrafts and the possible malicious purposes that this information might be used for [7]. In comparison to Primary Surveillance Radar and Secondary Surveillance Radar PSR and SSR signals which are more difficult to intercept and require a high level of ability to obtain the same data. Hence, the dependency of ADS-B on wireless networks, GPS and the use of a low-power signal makes it more prone to security issues than radar systems [55].

The integrity of ADS-B might be affected due to the ability that the system has to share messages with any two different devices [56]. The purpose of ADS-B message is to transmit information not only to ground stations but also to aircrafts; hence, the messages might be intercepted and modified. As a result of this vulnerability it can be confirmed the lack of authentication of the system [52]. As the Figure 3 shows, ADS-B has a Cyclic Redundancy Code (CRC) in the format of the message which is used for data integrity [54], although this is not enough to guarantee the integrity of the message from the cyber security perspective. It has been experimentally demonstrated by Schäfer *et al.* [57] and Costin *et al.* [10], the methods to guarantee that the CRC does not produce any kind of error which can make the system to disregard the message. Therefore, the susceptibility of receiving false messages and the deletion of the messages prompts a significant concern [58].

Finally, the availability of the system lies on the possibility that the system might not be disrupted by external intentional or unintentional actions. The susceptibility to jamming not only to GPS signals but also to the extended squitter 1090 MHz channel creates the threat to disrupt the communications and create denial of the service for a determined period of time [53]. The effect of a GPS jamming could be even more chaotic if the action is executed in different locations at the same time, entailing the disruption of GPS based sur-

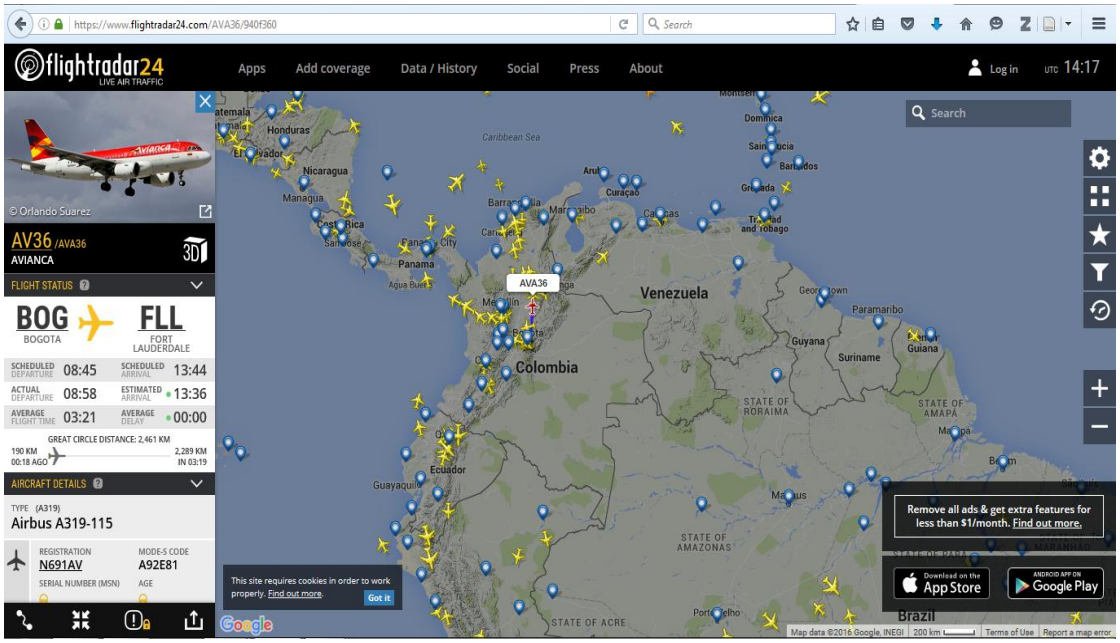

Figure 3. Open source track of a commercial airplane from www.flightradar24.com.

veillance system used by aircrafts and airports. In addition, attackers have the capability to transmit an unmanageable amount of messages in order to saturate the channel. This saturation is directed to the system data processing of the ground station and poses the threat of totally disable the functionality of the ground station [58].

2.3.2 Exploitation of ADS-B Vulnerabilities

To exploit the vulnerabilities of ADS-B a variety of attacks have been identified. The attacks can affect the confidentiality, integrity and availability of the system. However, these attacks are the result of coordinated established steps in the process to achieve the final goal of the attack. The next attack techniques were categorized in [7], [57], [59]to better understand more complex attacks against ADS-B system:

Interception of ADS-B OUT: the technique is called as aircraft reconnaissance [7] or simply eavesdropping. The acquisition of any ADS-B commercially available receiver and the proper set-up of the COTS to decode the messages in the right format is enough to perform the attack. For a better understanding of the interception of ADS-B messages, it will be described two examples of current public available means to execute it:

1. **Radarcape and Mode S beast:** Günter Köllner offers on his website an ADS-B passive receiver. The device contains a Linux computer with a network interface to connect to any required network [60]. Furthermore, the device has a built-in software with a web interface that offers the possibility to be configured by any inexpert user. In certain cases the users do not have the software, however in the public market exists the open-software package GNU Radio, which has been used in [10], [49]to execute the interception of ADS-B OUT and additional attacks.
2. **Kinetic Avionics SBS-3 with Flightaware:** The Company Kinetic Avionics Products offers the SBS-3, which is an ADS-B receiver of the 1090 MHz channel [62]. Flightaware offers the capacity and the instructions to use the hardware with the website in order to track the airplanes transmitting ADS-B signals without running a specific computer application [63].

Moreover, the information can also be obtained from publicly available websites such as www.flightradar24.com, www.radarvirtuel.com and www.flightaware.com as it can be evidenced in Figure 4.

The visible data in publicly open websites (see also Figure. 4) are: airline company, 24 bit ICAO identification number, registration, type of aircraft, itinerary, departure time, estimated time of arrival, flight time, delay in flight and departure, mode-S code, True Air Speed (TAS), Ground Speed (GS), calibrated altitude, vertical speed, track, specific current coordinates of the aircraft and flight radar receiver.

Jamming: The execution of jamming disables one of various nodes in the wireless network from sending or receiving messages with enough power to disrupt 1090MHz frequency [59]. Performing the technique does not need a high level of expertise and it has been demonstrated that it might affect messages that have been already sent in wireless networks [64].

Message Injection: This technique takes advantage of the ease to exploit the lack of authentication of the system. The attacker must implement a proper transmitter and to modulate the message in the correct message format [59]. The technical steps for implementation are based on using a system comprised of a GNU Radio, a Universal Software Radio Peripheral (USRP) [49]. The software can be developed by the attacker, which might be by writing a native C or C++ based GNU Radio modulator and encoder, or to execute the encoding and modulation in a specific software such as MatLab [10]. The ADS-B receivers have omnidirectional antennas that cannot discriminate the direction of the received messages; therefore, it is not possible for the system to determine the location of the possible attacker [57]. Some attacks require the injection of multiple messages. The additional requirement for multiple injections is a high level of bandwidth of the channel according to the number of messages to be injected [57].

Message Deletion: This attack is executed mainly by means of interference to delete messages from the wireless network [59]. The constructive interference is the preferable method to execute the attack, since it requires less strict synchronization than the destructive interference [57]. The attack has a level of difficulty if the attacker wants to delete selected messages. As a requirement the attacker must to eavesdrop the channel of 1090 MHz extended squitter and to create the interference with the message that he wants to delete prior it reaches the ground station [57]. In addition, the 1090 extended squitter Mode S checksum has the ability to correct at most 5 bit errors per message, the message cannot exceed this limit in order to be valid [59].

Message Modification: The integrity of the message is affected with the modification of the information contained in the message. The technique might be performed by two means, overshadowing and bit-flipping [59]. The preferable way to modify the message is to overshadow the signal since it is easier for the attacker to decode the message without error [57]. The message is modified during the transmission and the attacker must locate himself at a correct position and angle to the aircraft, plus to calculate the precise timing to inject the modified message [57].

For a better understanding of the reader the figure 5 provides the hardware set-up established in [57] to execute their experiment. This figure shows the device used to play the role as attacker in the case of the Linux computer and the Windows computer plays the role as the receiver, which can be an aircraft or an air traffic control facility. This set-up demonstrates that the resources needed to execute every kind of attack to any ADS-B receiver is utmost 2500 dollars [57].

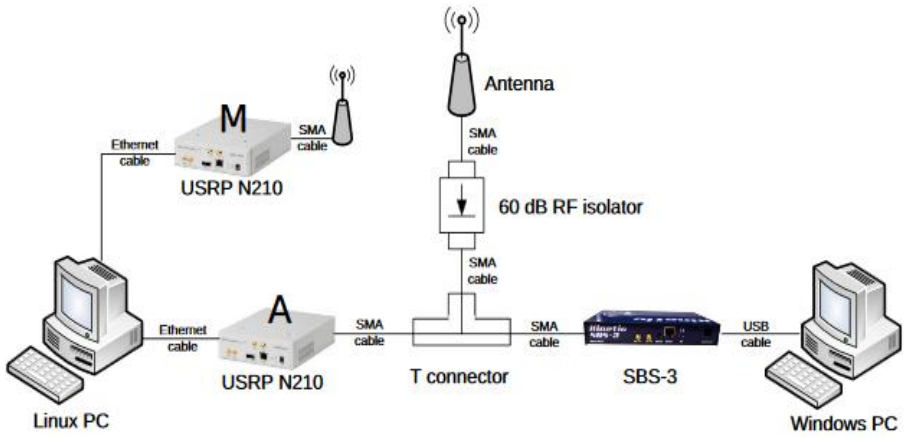

Figure 4. Experimental Hardware Set-Up to Perform Attacks Against ADS-B[57].

2.3.3 Exploitation of GPS vulnerabilities

An important concern is the inherent reliance of ADS-B on GPS. GPS signals are vital to the whole operation of the system and accuracy of the information received by the operators [65]. The different vulnerabilities that might affect GPS might be divided into intentional, unintentional and human factor problems [66]. The unintentional vulnerabilities and hazards that might be brought about by the environment and nature such as earthquakes, floods, solar cosmic radiation and space objects that might affect the GPS ground stations and data links [67]. The unintentional human interference must be considered since it could cause a huge problem to an air traffic control facility. An example of this was the interference generated in Newark airport in New Jersey, which caused many troubles to the air traffic center, by a truck driver who used a cheap and easy to obtain jammer to disrupt the signals of the GPS device used to track the vehicle [68].

The vulnerabilities of GPS systems do not only represent a problem for the surveillance systems. There must be cyber security considerations regarding the possibility that an Unmanned Aerial Vehicle (UAV) can be spoofed through the transmission of false information using GPS signals [69]. In addition in [69], it is analyzed the vulnerabilities of the current autopilot system of the UAV and the behavior of the system after the attack in order to promote the development of improved design of autopilot system resilient to cyber-attacks. Therefore, the vulnerabilities of GPS might also affect the data transmitted to the aircraft through data link that finally reaches the Flight Management System (FMS), which uses GPS sensors to automate in-flight procedures.

3 Methodology

3.1 Research Design

The research design used for this thesis is a qualitative analysis to determine the possible impact of the threats (see section 2.3.2) that might affect Automatic Dependent Surveillance Broadcast in the aviation system and the tools that can be used by air traffic controllers and pilots to deal with the attacks. The research is based on official documents of aviation, academic papers about cyber-attacks against ADS-B, hackers' community publications, aviation safety assessment and interviews with the experts in the field.

3.2 Qualitative Analysis Procedure

The attacks that have been object of experiments in the science realm were identified in order to consider only those that are the real concern to be executed against the system. The taxonomy described by McCallie [7] is used to systematically classify the attacks. Moreover, in order to take into account that security risk implies safety risk in aviation [70], the impact of the attacks is assessed with aviation safety considerations. This section describes the steps followed to make the qualitative analysis, to determine the impact of the cyber-attacks and to obtain the results.

1. Determine the Impact on Confidentiality, Integrity and Availability: The effects caused by each kind of attack are determined according to the effect caused in confidentiality, integrity and availability of the system, which are described in the "Guidance Material: Security Issues Associated with ADS-B" issued by ICAO [58], and the effect caused in pilots and air traffic controllers with the operation of the system. Any kind of damage or impact caused to the assets will affect the operation of the system. It will probably cause the deterioration in the communication between air traffic controllers and pilots and safety concerns for the aeronautical operations. The assets identified in the ADS-B wireless network are confidentiality of the information transmitted through ADS-B channel, integrity of the information transmitted with the ADS-B messages and the availability of the ADS-B communications.

2. Identification of Attack Targets: The targets can be categorized in three according to Mahmoud [70]: ground segment, which refers to the ground networks of ADS-B including the data link ground stations such as ADS-B ground stations, the distributed computer network and the ground control station of the air traffic controllers. The second target is the air segment which is compounded by the ADS-B system that is onboard the aircraft and finally the air-ground segment that comprises the communication medium used to broadcast the data. The targets are identified according to the effects that the attacks cause to the end users, which in the case of ADS-B are the pilots and the air traffic controllers, because they are the direct operators of the system.

3. Classification of Attack Techniques: Every attack is executed with specific methods. Although the method used by any attacker might be different, in general terms they can be categorized in interception of ADS-B OUT signals, jamming [7], message injection, message deletion and message modification [57].

4. Classification of the technical difficulty of attack: The level of difficulty helps to perform a risk analysis of the attacks. The levels are categorized according to McCallie [71] description of the technical expertise, knowledge and additional implementation

required to execute an attack. The level of difficulty are classified in Low, Medium or High.

5. Development of Attack Trees: The concept of attack tree was first established by Schneier [72] in his book "Secrets and lies: digital security in a networked world". Attack trees have a common relation with fault trees. Fault trees have been used in order to check the safety, performance and interoperability requirements of ADS-B [73]. Attack trees provide a means to evaluate the risk of an attack making use of the capabilities of fault trees but also taking into consideration the adversary willing to attack [74].

The attack tree can be developed with AND and OR nodes. The nodes represent different steps in order to execute the final goal. In addition, all the the children nodes of an AND node have to be achieved to get to the final goal. OR nodes do not require that all children nodes have to be achieved, with only one node is enough to be satisfied [72]. The attack trees were developed based on the literature review to understand the technical steps that an attacker must to carry out to achieve the final objective. However, in the phase of this research there is not a solid foundation to provide a quantitative analysis. They were not set any metrics to the nodes of the attack trees in that there was not available data to do it and to perform further validation.

6. Evaluation of Impact: To make a systematic qualitative analysis of the possible consequences of every attack, the impact of the attacks can be assessed based on the amended OSA ED78A/DO264 classification matrix [73]. Taking into consideration the perspective of aviation experts, this matrix provides a systematic approach to analyze the impact in the aeronautical operations brought about by the cyber-attacks. Figure 6 represents the rating from 1-5 with 1 being the most severe and 5 rates as least severe.

The severity of impact of each attack was discussed with experts in the field of aviation in the Colombian Air Force and civil aviation organizations of Colombia and Estonia. The importance of this classification is that provides information of the possible conditions that an attack might produce in the ATC and in the flight crew.

3.3 Interviews and Data Analysis

The type of interview was semi-structured (See Appendix 2 and 3) in that to allow the interviewer to ask additional questions, which might provide relevant information about the topic in study. An interview guide was used, explanation of the purpose and topic of the interview and specific questions to be asked. This kind of interview provides more profound information, which cannot be achieved with a standardized multiple-choice questionnaire, and gives the possibility to get more honest responses [75]. Similar studies have been recently realized using survey-based analysis in the aviation domain by Strohmeier, et al. [76]and Silva, et al. [77], but it was considered that a survey does not provide the advantages that only one-to-one interview gives to obtain more valuable data [75].

The main objective of the interview was to obtain the most relevant information from the participants regarding the predicted reactions in a cyber-attack against ADS-B surveillance system, the most critical situations that could be caused and the best mitigations that might be executed based on their experience. It is important to highlight that ADS-B is still in process of implementation, and it allowed analyzing the preparation that aviation personnel have to deal with the vulnerabilities of the system. The analysis of the interviews and notes were compared and categorized to answer the research questions of this thesis.

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or in ATC capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.
Example of ASAS operational effects	• *Mid-air collision* • *Controlled flight into terrain* • *Total loss of flight control* • *High speed surface movement collision (i.e. collision in runway)* • *Leaving a prepared surface at high speed.*	• *Large reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at low altitude.* • *Large reduction in safety margins like abrupt manoeuvre is required to avoid mid-air collision or CFIT (e.g. one or more aircraft deviating from their intended clearance)* • *Large reduction in aircraft functional capabilities* • *Total loss of air traffic control for a significant period of time*	• *Significant reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at high altitude.* • *Low speed surface movement collision (i.e. collision in taxiway)* • *Leaving a prepared surface at low speed* • *Significant reduction in aircraft functional capabilities* • *Significant reduction in air traffic control capability*	• *Slight reduction in separation or safety margins* • *Significant increase in air traffic controller workload* • *Slight increase in flight crew workload*	• *No effect on operations /traffic* • *Slight increase in air traffic controller workload* • *No effect on flight crew*

Figure 6. Severity of the impact of the attacks on ADS-B vulnerabilities [73].

3.3.1 Selection of the Aviation Experts

The selection of the professionals of aviation was determinant to obtain the required knowledge. Therefore, the people selected were only related with piloting, air traffic control and Air Traffic Management (ATM) experts. The interviewees were selected according to their experience in their specific aviation discipline (See Appendix 1), expertise in aviation realm, and the operational usage they have with ADS-B. It is important to highlight that not all the pilots and air traffic controllers have used the system worldwide, but this research sought to interview those who have already operated ADS-B. Although the participants were from two different geographical locations, that added value and different perspectives of the issue.

4 Findings and Analysis

4.1 Qualitative analysis of cyber-attacks against ADS-B

The attacks contemplated in this thesis are those, which have been experimentally proven in an enclosed laboratory in [10], [57], [49], and which represent the real concern. These attacks named in Table 3 are the threats for the assets identified in ADS-B system. In the next sections, the analysis of each cyber-attack against ADS-B is performed following the procedure described in chapter 3.

During the interviews, every attack was thoroughly described and explained to the participants, since the majority of the interviewees did not have previous knowledge about the vulnerabilities of ADS-B. Furthermore, it was noticed that despite the disparate geographical locations of the participants, the responses showed a similar pattern in the procedures and possible reactions to the attacks.

4.1.1 Aircraft Reconnaissance

Aircraft Reconnaissance is known as eavesdropping. Any attacker executes it in order to carry out further attacks [78]. This attack is based on the interceptions of the ADS-B OUT signals and the correct decoding and demodulation using a proper set-up of open source software and hardware, which can be easily accessible in the commercial market [10], [57].

Table 3. Attacks and Affected Assets of ADS-B.

THREATS	**AFFECTED ASSETS**		
Attacks	**Confidentiality**	**Integrity**	**Availability**
Aircraft Reconnaissance	X		
Aircraft Target Ghost Inject	X	X	X
Ground Station Target Ghost Inject		X	
Ground Station Multiple Ghost Inject		X	X
Replay Attack	X	X	
Aircraft Spoofing	X	X	
Virtual Trajectory Modification	X	X	
Aircraft Disappearance	X	X	X
False Alarm Attack	X	X	
Aircraft Flood Denial			X
Ground Station Flood Denial			X

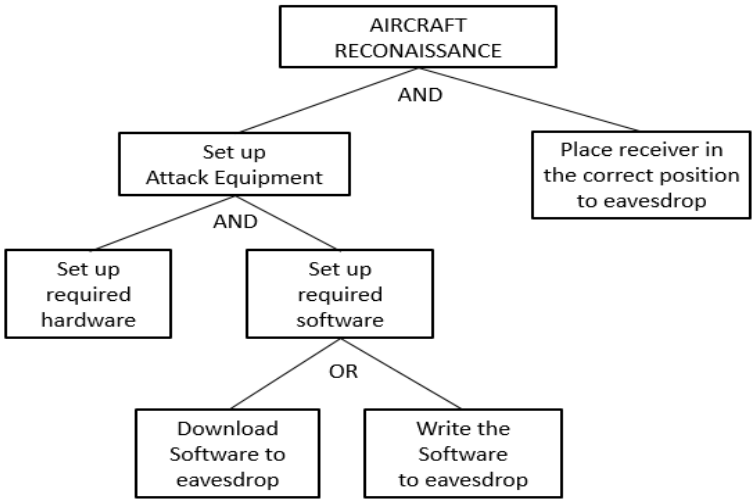

Figure 7. Aircraft Reconnaissance Attack Tree.

The open source websites such as flightradar24 (www.flightradar24.com) are not completely reliable to perform aircraft reconnaissance, and the main reason is that this kind of organizations eliminate the information of the website according to the requirements received by aviation companies or governmental organizations. For example in 2014, the information of the airplanes used to transport the Japanese prime minister and the imperial family were tracked online on flightradar24, therefore the ministry of defense of Japan asked the heads of the website to remove the information[79]. This attack affects the confidentiality of ADS-B.

Target: air-ground segment.

Attack Technique: Interception of ADS-B OUT.

Technical Difficulty: Low [7]. The Figure 7 shows the steps followed by an attacker to execute aircraft reconnaissance attack. The level of difficulty is low due to many open source software and hardware available to execute the attack [71]. In addition, placing the receiver at a correct position allows the attacker to have a larger range to acquire the signals of the aircrafts.

Impact: The attack does not produce any direct impact to the aviation system. However, it provides a means to gather information for economic intelligence [58]. Moreover, It can be used to gather relevant information of military aircrafts of an enemy state as it was stated by Cenciotti [80], and a means to gather information by terrorists which plan to execute a deliberate attack against a specific plane. The main concern in aviation is the loss of privacy with the interception of ADS-B OUT signals. The aviation experts were not consulted about this attack because it does not have any direct impact on the operators of the system.

4.1.2 Aircraft Target Ghost Inject

The attack aims to inject a ghost airplane into the cockpit display of traffic information (CDTI). The aircraft does not possess a mechanism to verify the authenticity of the information, but the necessity to have proximity to the aircraft increases the difficulty [7]. To make it more realistic the information provided with the injection must contain all the specific data characteristics that a real airplane broadcasts through data link. The attack affects the confidentiality, integrity and availability of ADS-B.

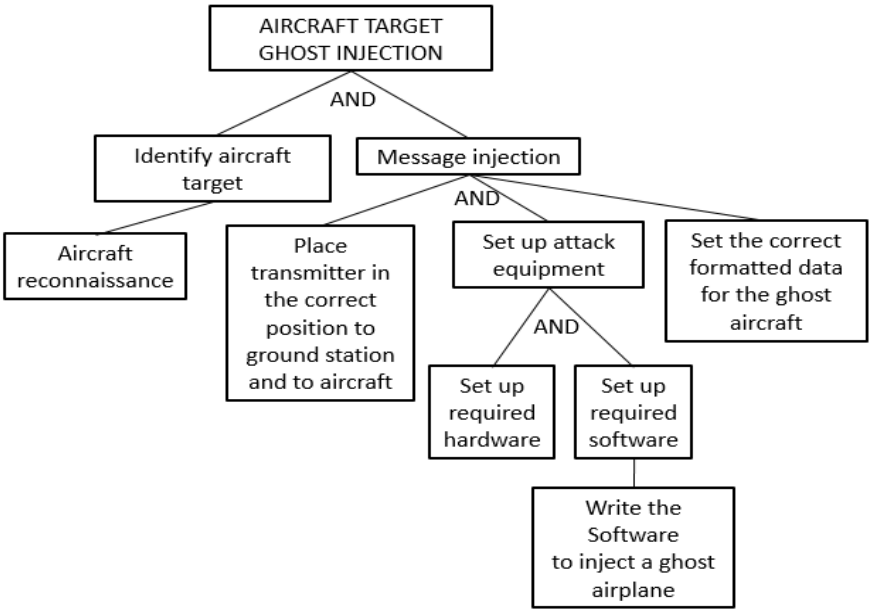

Figure 8. Aircraft Target Ghost Inject Attack Tree.

Target: Air segment.

Attack Technique: Message injection and interception of ADS-B OUT.

Technical Difficulty: Medium-High [7]. For this attack, it is initially important to set up the equipment in order to eavesdrop and to identify the aircraft target. Figure 8 shows that for this attack it is important to set the correct format of ADS-B message and to inject an aircraft with credible data so that the receiver cannot detect the "ghost aircraft" as fake.

Impact: Table 4 shows the classification of the attack considered by the aviation experts. Three out of five of the consulted pilots classified the attack with a severity of four. The main reason was the slight increase of workload while trying to identify by other means a possible real aircraft, which may interfere with the trajectory. The pilots, who rated the severity as three, considered the closeness of the ghost aircraft and the unnecessary maneuvers that have to be done, if the injection is in a proximity to their airplane.

Analysis by aviation experts: The most critical situation of this kind of attack determined by the participants was that an aircraft might be injected into the CDTI and the ghost air-

Table 4. Classification of Aircraft Target Ghost Inject attack impact by aviation experts.

Participant	**Severity**
PILOT	3
PILOT	4
PILOT	3
PILOT	4
PILOT	4

plane is addressing directly to the aircraft that the pilot controls. This situation may bring about doubts and immediate reactions by the pilot, even more if the pilot is flying in IFR conditions. The reaction of the pilot in this situation depends on the phase of the flight: take off, cruise or approach, being approach the most critical because the pilots could make an abrupt maneuver close to the terrain.

ADS-B system may be connected with the Traffic Collision Avoidance System (TCAS) and the signal of the ghost airplane could activate the TCAS alarm if the ghost airplane is approaching to a real aircraft such as in an opposite direction and to the same altitude. A participant stated: "That creates safety concerns because of the high trust that pilots have on the instruments. We are trained to follow the indications of the instruments as if they were completely right. Therefore, if there is an injection and that activates my TCAS alarm, I would follow immediately the indications of the TCAS".

Moreover, if the attack is recurrent and the aircraft is flying in a RVSM airspace, the pilot might be forced to turn off the TCAS and to change the altitude, or in the worst case to operate the aircraft without TCAS, situation that might pose additional safety concerns. However, the Minimum Equipment List (MEL) allows to operate the aircraft up to 10 days according to the Eurocontrol [81]. The MEL may vary according to the regulations of every country or manufacturer, and in some cases it could be very restrictive that the aircraft must be on the ground immediately the same day of the event.

One participant considered the injection of a ghost airplane on the runway while his airplane is on approach. Such event would activate the alert of collision avoidance and hence the aircraft will be forced to make a go-around in a situation which is not needed. Although, the injections of many aircrafts on the CDTI would make the pilot to think that there is an error of the system, the availability of the system would be compromised because the pilot cannot trust anymore in the information displayed on the CDTI.

Mitigations:

If there is enough time to verify the traffic:

- **a.** Verify traffic with ATC and other aircrafts using radio communications.
- **b.** Confirm visually the traffic if the visibility allows to do that.

If there is not time

- **a.** Follow immediately the indications of TCAS resolution advisory to avoid any possible mid-air collision.

4.1.3 Ground Station Target Ghost Inject

The attack injects a single "ghost aircraft" in the ground station of the air traffic control. It is required the ability to create a 112 bit-message that has the characteristics of a legitimate traffic in the screen of the air traffic controller [7]. In addition, the attack must comply with the required information that an aircraft broadcasts at a rate of 2Hz. Therefore, the attacker must know the proper data contained in an ADS-B message for legitimate flights in order to create the ghost aircraft. The attack affects the integrity of ADS-B.

Target: Ground segment and air ground-segment.

Attack Technique: Message injection.

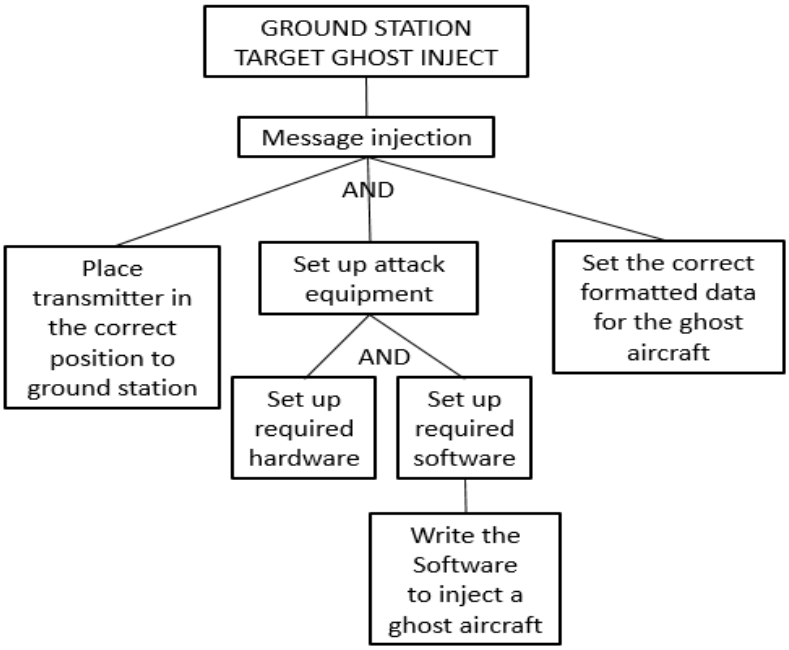

Figure 9. Ground Station Target Ghost Inject Attack Tree.

Technical Difficulty: Medium-High [7]. Figure 9 shows the process to execute the attack. It is important to note that an attacker needs to have special knowledge of the ground station equipment. This knowledge provides the attacker with the ability to set the specific software and hardware to break the security of the air traffic control.

Impact: Table 5 shows the classification of the attack considered by the aviation experts in ATC. Four out of five of the interviewees classified the attack with a severity of four. The main reason was the significant increase in the air traffic control workload while trying to identify the ghost aircraft using other means. One air traffic controller classified the attack with a severity of three due to the possible reduction in separation in the case that another aircraft is ordered to avoid a conflict with the ghost airplane.

Analysis of aviation experts: The general perception of the participants was that an injection of a single aircraft ghost airplane does not represent a problem for the air traffic control. Some of them recalled that there are many aircrafts which do not identify themselves, and it is not possible to confirm the real information of that aircraft.

However, two air traffic controllers expressed the concern that the injection of the aircraft could be in a terminal area TMA. In that case, the injection could affect the normal procedures of the approach. They remembered past experiences of a phenomenon called "garbling". Garbling is an error presented in SSR when the signals of two aircrafts overlap and then they make the collision avoidance systems detect a close proximity to another aircraft. It means, for instance that the aircraft could be injected in the holding pattern in the radar screen. Therefore, it should generate an alert or modification on the radar display, causing to order unnecessary maneuvers to the aircrafts to avoid the ghost airplane, and delays in the procedures to land and take off.

Mitigations:

a. Vectorization of other airplanes in order to avoid any conflict with the trajectories until the injected airplane is identified as such and the verification with a less accurate surveillance system.

b. Correlation with a legal flight plan and transponder code. This would eliminate at least the doubt if it is a legal airplane or in other case a possible infringement and that would give the hint to identify it as a ghost aircraft.

c. Transmission of instructions to the aircraft to confirm if it can follow the orders and information to other aircrafts about the "ghost traffic" in case it might be real.

d. If none of the previous procedures is satisfied then it must be started an interception mission by the military aviation.

Table 5. Classification of Ground Station Target Ghost Inject attack impact by aviation experts.

Participant	**Severity**
ATM expert	4
ATC	4
ATC	3
ATC	4
ATC	4

4.1.4 Ground Station Multiple Ghost Inject

This attack is performed using the same technique of ground station target ghost inject attack, but the attacker must increase the bandwidth according to the number of aircrafts that wants to inject [57]. In 2012 at the Defcon Hacking Conference [82], [83] it was proven that as many as 50 ghost aircrafts can be injected on the display of an air traffic controller and generate the correct ADS-B data broadcast. The attack affects the integrity and availability of ADS-B.

Target: Ground segment and air-ground segment.

Attack Technique: Message injection.

Technical Difficulty: Medium-High [7]. The attack tree in figure 10 depicts an additional node that increases the difficulty of the attack, since the bandwidth has to be considerable to inject a sufficient number of ghost planes in order to create enough confusion in ATC.

Impact: Table 6 shows the classification of the attack determined by the aviation experts in ATC. Four out of five of the interviewees classified the attack with a severity of three. The main reason was the significant reduction in separation caused by the confusion of having a considerable number of ghost airplanes. Situation that might lead to take wrong decisions in the air traffic control. The ATM expert classified the attack with a severity of four, since the participant considered that the degradation to another surveillance system could solve the problem rapidly.

Analysis of aviation experts: The general perception of the participants was that this attack might be critical if the degradation to a less accurate surveillance system cannot be executed immediately. Moreover, in the event that this attack might happened, the confusion caused in the moment of the attack might can be simply solved with the degradation to a less accurate surveillance system such as PSR or MLAT. The congestion would be

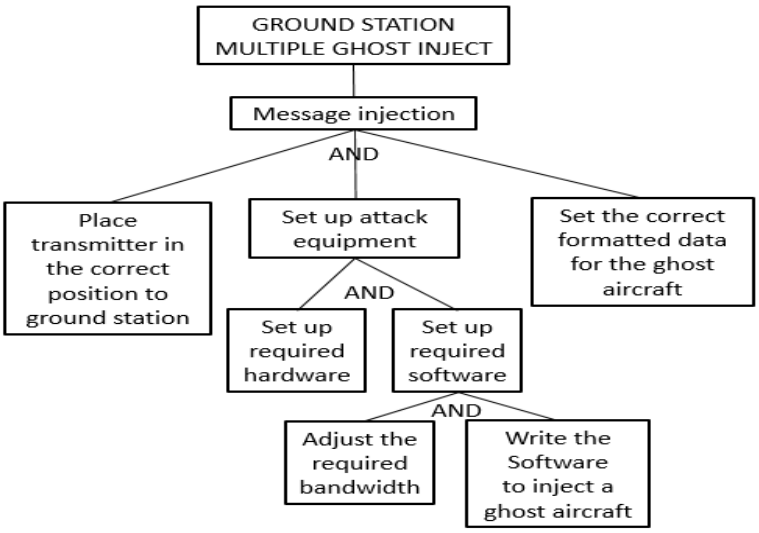

Figure 10. Ground Station Target Ghost Inject Attack Tree.

generated due to the extension of separation that has to be applied to the aircrafts based on each surveillance system, causing problems with the normal flow of the air traffic. That would consequently cause more workload to the air traffic controllers.

The participants shared the same thought when they were asked about the number of airplanes they could handle. A participant noted: "There are tools for the Air Traffic Flow Management. They can determine the capacity and number of aircrafts which can be controlled in that area per hour and it depends on the type of airport as well. For instance, if the airport has parallel runways or a single runway". However, when the injection of multiple airplanes is so evident, then they prefer to change to another surveillance system or to start conventional control.

A participant expert in air traffic management stated: "It is possible that the amount of injections can overload the system due to the limits of capacity of itself. The system receives and verifies all the information from the airplanes, and then in that case there could be loss of the display in the ATC". The participant also added that with the current structure of the surveillance system, the injection of the ghost airplanes can be executed easily in the ADS-B receivers but not in the receivers of PSR, SSR or MLAT with the same ease. However, with the correlation with other surveillance systems the ghost airplanes can be

Table 6. Classification of Ground Station Multiple Ghost Inject attack impact by aviation experts.

Participant	**Severity**
ATM expert	4
ATC	3
ATC	3
ATC	3
ATC	3

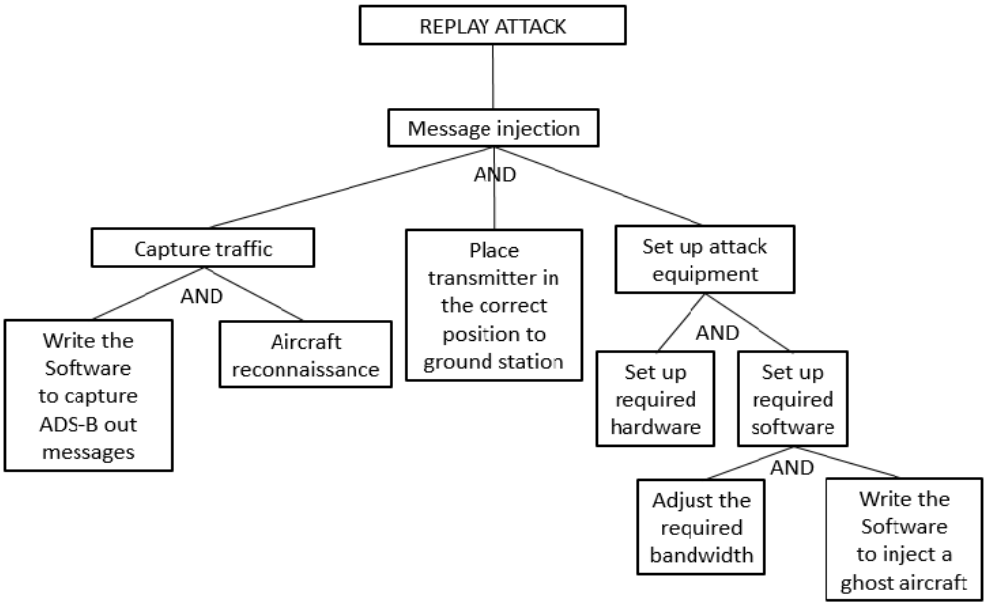

Figure 11. Replay Attack Tree.

filtered.

One air traffic controller stated his doubts about the attack with the current but not the future operation of the system: "Currently the priority of the systems in our airspace is: first SSR, then Multilateration and finally ADS-B, there is always redundancy with the systems even with the elimination of SSR and PSR we can have MLAT".

Mitigations:

- **a.** Immediate degradation to a less accurate surveillance system. Start a conventional control to apply the standard separation according to the surveillance system which will be used.
- **b.** Divide the airspace in order to split the workload in more air traffic controllers.
- **c.** Start deviation of aircrafts to holding patterns and alternate airports in order to reduce congestion in the terminal area of the air space.

4.1.5 Replay Attack

The attack aims to send information of a previous flying aircraft to broadcast it again to the ATC. The attack requires to capture ADS-B OUT signals on 1090MHz frequency and to adjust the transmitter to replay the captured data using the proper file to transmit the file of captured data via GNU Radio hardware [10]. The attack affects the confidentiality and integrity of ADS-B.

Target: Ground segment and air-ground segment.

Attack Technique: Message injection and interception of ADS-B OUT.

Technical Difficulty: Medium [10]. The attack tree in Figure 11 exhibits that the attacker has to perform additional steps for the message injection. The attacker must intercept and capture the data and finally to replay the captured messages making use of message injection.

Impact: Table 7 shows the classification of the replay attack determined by the aviation experts in ATC. Three out of five of the interviewees classified the attack with a severity

Table 7. Classification of Replay Attack attack impact by aviation experts.

Participant	Severity
ATM expert	5
ATC	4
ATC	5
ATC	4
ATC	5

of four, stating that the attack is easy to detect and it will just slightly increase the workload of the air traffic controller. Two participants classified the attack with a severity of four. They support their classification noting that it might cause to deviate aircrafts and reduction in the separation. Even though they can identify the fake aircrafts, they would not take the risk with real airplanes in conflict with the ghost airplanes.

Analysis of aviation experts: The participants considered that it is an easily detectable attack due to the wrong correlation of the flight plan, transponder code or identifier with the origin flight. The information can be confirmed with the air navigation service provider (ANSP) or airlines. One air traffic controller stated: "The airlines have scheduled flights and it would be just so evident if the information of a previous flight is replayed". The verification with radio communications and the deviation of other aircrafts would solve any conflict with the replayed ghost aircraft. If the aircraft does not have a correlated flight plan then it is shown with a different color on the screen and can be easily identified by the air traffic controllers.

It was also considered by the participants that there could be possible collision avoidance alert if the replayed aircraft is in the trajectory of another plane. One air traffic controller stated: "There are two systems which help to avoid collisions or at least to alert to air traffic controllers. STCA Short Term Conflict Alert and MTCD Medium-Term Conflict Alert advise to an air traffic controller if the ghost aircraft could be converging with a real aircraft:" Therefore, keeping the other aircrafts out of the trajectory is enough to manage the traffic in the case that the replayed aircraft cannot be identified as fake. The attack would just create confusion but it can be handled with no further consequences.

Mitigations:

- **a.** Try to establish radio communication with the aircraft.
- **b.** Verify correlation with flight plan, transponder code, aircraft information with the airline and to confirm flight information with the previous airspace where the aircraft is coming from.
- **c.** Use Short Term Conflict Alert (STCA) and Medium-Term Conflict Alert systems (MTCD) to receive alerts of a possible collision and to keep other aircrafts out of converged trajectories in order to avoid any conflict.

Table 8. Classification of Aircraft Spoofing attack impact by aviation experts.

Participant	Severity
ATM expert	5
ATC	5
ATC	5
ATC	5
ATC	5

4.1.6 Aircraft Spoofing

The attack is achieved by the combination of message injection and message deletion [57]. The attacker must to eavesdrop the 1090MHz channel in order to interpret the messages and to interfere with the required message [52]. The attack is useful to reduce the propensity of alarms when an attacker disguises as a legal aircraft [44]. The attack affects the confidentiality and integrity of ADS-B.

Target: Ground segment and air-ground segment.

Attack Technique: Message Deletion, message injection and interception of ADS-OUT.

Technical Difficulty: Medium [10],[57],[53]. Although the attack was classified as medium, it requires a combination of techniques that must be executed with a proper coordination. Figure 12 illustrates the required procedures that an attacker must to execute and the two options that an attacker has in order to delete a selected message.

Impact: Table 8 shows the classification of aircraft spoofing attack determined by the aviation experts in ATC. All five participants determine that the level of severity is five, since the attack would only slightly increase the workload of the air traffic controllers without any additional consequence.

Analysis of aviation experts: There is not standard procedure for this kind of attack and it could not cause a critical situation. The participants proposed the same solution to the problem. The information of the aircraft would be verified with the flight plan, transponder code, time of departure, and communication with the controller of the previous air space, airline or the air navigation service provider where the aircraft is proceeding from. For most of the participants, it was unlikely that an aircraft would try to deceive the air traffic control. One air traffic controller stated: “it would be just easier to not transmit with ADS-B transponder or to jam the 1090Mhz channel”. The aircraft would be detected as illegal if it is not following the instructions of ATC.

Moreover, one air traffic controller said: “The procedure is standardized to be that way, and the air traffic controller is always transferring the traffic to the next air traffic controller who manages the next air airspace. Although in some areas with no strict control, the crew could just pretend to be a legal airplane and continue with their flight”.

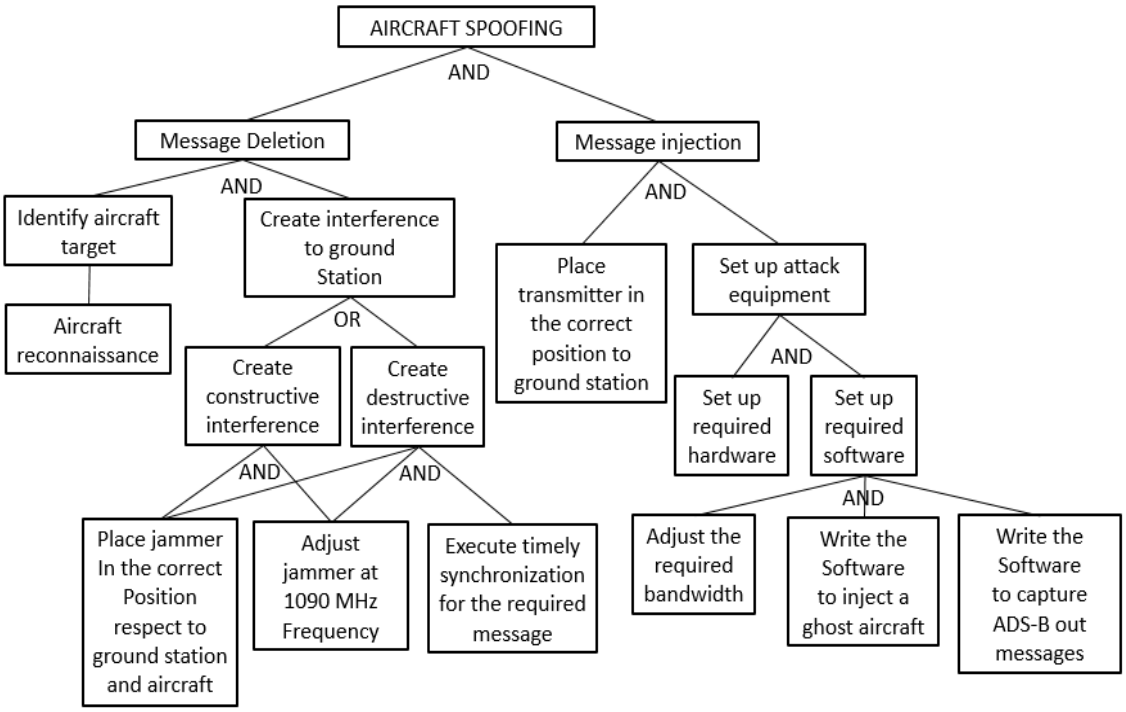

Figure 12. Aircraft Spoofing Attack Tree.

Mitigations:

- **a.** Try to establish radio communications with the aircraft.
- **b.** Verify correlation with flight plan, transponder code, aircraft route and information with the controller of the previous air the airplane is proceeding from.
- **c.** Confirm that aircraft follows instructions from ATC.
- **d.** If the airplane does not comply with the previous requirements, start interception procedure with military aviation.

4.1.7 Virtual Trajectory Modification

The objective of the attack is to modify the trajectory of an aircraft in flight [52]. The attack can be achieved making use of combination of techniques. The first combination is to do message deletion and message injection and the second option is to modify directly the broadcast message by the aircraft while is being transmitted [44]. The attack affects the confidentiality and integrity of ADS-B.

Target: Ground segment and air-ground segment.

Attack Technique: Message deletion and message injection, or message modification.

Technical Difficulty: Medium [57]. Figure 13 shows that the attack requires a combination of techniques to be performed. Therefore, the difficulty is increased and the attacker must have the ability to be precise while executing the required procedures.

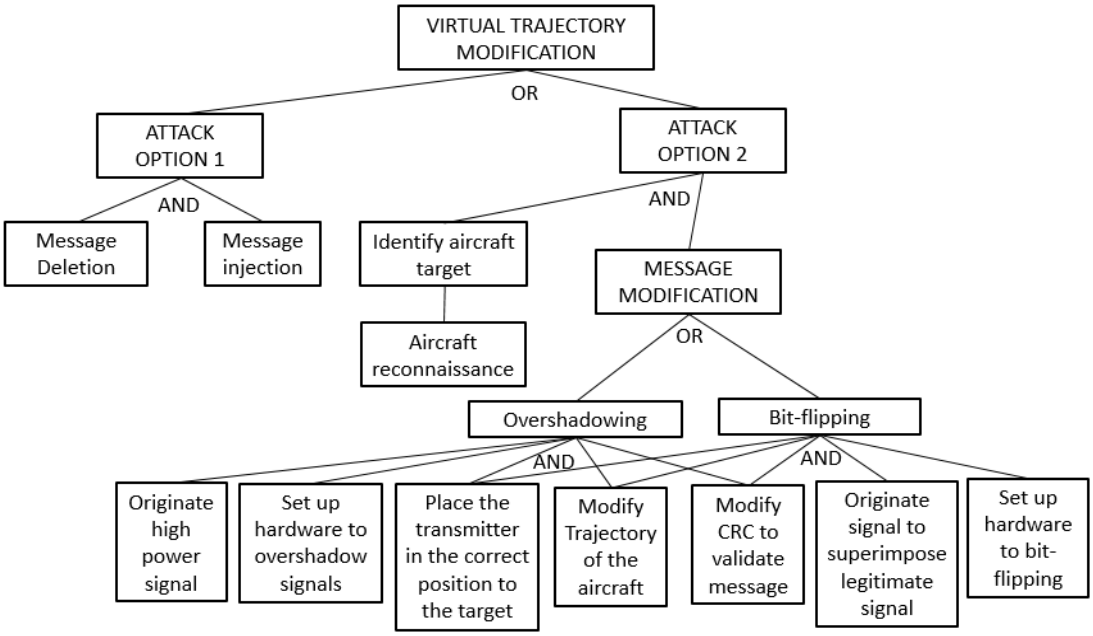

Figure 13. Virtual Trajectory Modification Attack Tree.

Impact: Table 9 shows the classification of the attack determined by the aviation experts in ATC. Three out of five of the participants classified the attack with a severity of three. The reason for this classification is that the air traffic controller takes decisions of reduction of separation between aircrafts based on the location of the aircraft on the screen. Therefore, it could be evidenced a significant reduction in separation between two aircrafts that is out of the standard. Two participants classified the attack with a severity of four, stating that the workload would only be increased due to the increment in communications with the crew, since they cannot trust anymore in the position of the screen

Analysis of aviation experts: The perception of the participants was that it would be a problem if the attack cannot be detected. However, it would not be critical as long as the information of the real position of the aircraft can be confirmed with the crew. Another participant said that if he can identify the attack then he would not trust in ADS-B anymore and would use conventional control to solve any conflict of aircrafts, or to rely only in another less accurate surveillance system.

Table 9. Classification of Virtual Trajectory Modification attack impact by aviation experts.

Participant	**Severity**
ATM expert	4
ATC	3
ATC	3
ATC	4
ATC	3

An air traffic controller gave an example of a critical situation with a possible reduction of the separation of the aircrafts, because the air traffic controller gives instructions based on the actual position that he can see on the screen. Therefore, in IFR or on approach, the reduction could represent a safety concern or possible mid-air collision and at the same time, it will increase the workload of the air traffic controller.

A participant noted that the most and scariest situation is if the modification of the trajectories of all the aircrafts occurred at the same time. He gives an example calling the phenomenon as "if the radar freezes", then the traces of aircrafts do not move and it could take long time for the air traffic controller to understand what is happening, while the aircrafts are still moving without the control of ATC.

Mitigations:

- **a.** If detected, the real position of the aircraft must be verified with the crew.
- **b.** Stop trusting in the information received by ADS-B system and start a conventional control to give vectors to the aircraft.
- **c.** Use an alternate surveillance system if possible to have improved reports of the position of the aircraft and to avoid any conflict.

4.1.8 Aircraft Disappearance

The attacker aims to delete all the ADS-B messages that the aircraft broadcast to ground station or to another aircraft [57]. The attack might delete not only one but many selected aircrafts by the attacker. The attack affects the confidentiality, integrity and availability of ADS-B.

Attack Target: Ground segment, air-ground segment and air segment.

Attack Technique: Message deletion.

Technical Difficulty: Medium [57]. The attack represents certain level of difficulty, since the synchronization and timing are the key to delete the desired message [57]. Therefore, the attacker needs to eavesdrop the channel and interpret the messages before starting the attack. Figure 14 shows the combination of interception of ADS-OUT signals and message

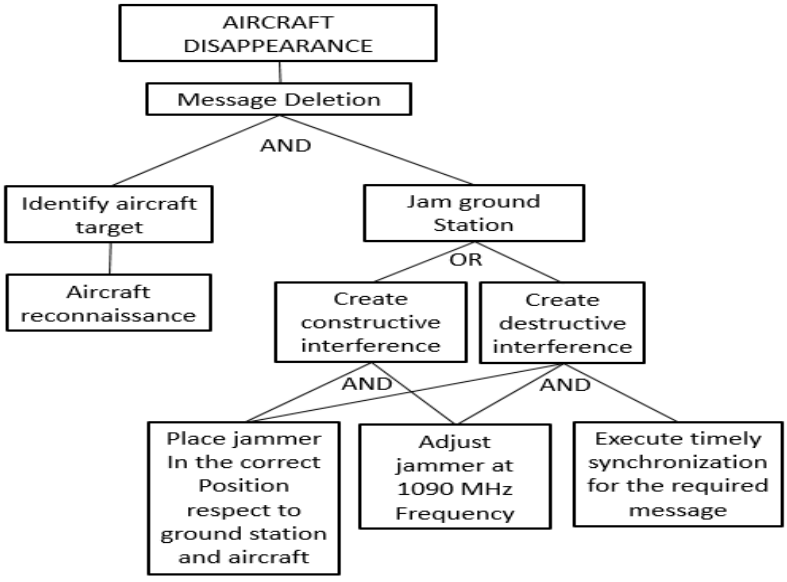

Figure 14. Aircraft Disappearance Attack Tree.

Table 10. Classification of Aircraft Disappearance attack impact by aviation experts.

Participant	Severity
ATM expert	2
ATC	2
ATC	2
ATC	2
ATC	2

deletion to perform aircraft disappearance attack.

Impact: Aviation experts in air traffic control classified the attack with a severity of two. They expressed the concern that with the disappearance of one or more aircrafts from the

Table 11. Classification of Aircraft Disappearance attack impact by pilots.

Participant	Severity
PILOT	4
PILOT	4
PILOT	4
PILOT	4
PILOT	4

radar screen, the loss of air traffic control for a long period could be critical and that might cause large reduction in the separation of the airplanes. Table 10 shows the classification by the ATM expert and air traffic controllers.

The pilots rated the attack as four level of severity as it is shown in Table 11. The main reason is that the attack would increase the workload due to the loss of situational awareness related with the traffic around the aircraft they fly.

Analysis of aviation experts: The attack was identified by most of the participants as highly dangerous. One participant said that the air traffic controller might forget that there was an airplane there, and in some cases the next radio communication with the crew could take long time. The disappearance of one aircraft could lead to a conflict that the STCA and MTCD would not alert to air traffic controllers. A participant stated special concern to this attack saying: “10 or 15 minutes without seeing an aircraft could lead to an accident”. The problem might be more critical if it is in a congested air space, and it might be easy to forget about two or more aircrafts which disappear from the ATC radar screen. If the attack is noticed by the air traffic controller the solution is straightforward, it would only be necessary to give priority and to establish conventional control to that aircraft.

The pilots determined that the disappearance of one aircraft can be detectable easily because there is a constant crossed check to the CDTI throughout all the flight. A participant considered that it is a critical problem in a congested airspace because there is a loss of situational awareness of the aircrafts around his airplane. Moreover, without those signals, the TCAS would not generate the respective alerts to instruct the pilots how to respond for a collision avoidance.

Mitigations for ATC:

- **a.** Use mechanisms of prediction of trajectory for ADS-B so that the predicted trajectory is shown on the screen in the case that the aircraft disappears.

If the disappearance of the aircraft is detected:

- **b.** Request position of the crew and establish conventional control.
- **c.** Transmit vectors to the crew in order to give priority to the aircraft.

Mitigations for Pilots:

- **a.** If the disappearance is detected: Inform immediately to air traffic control about the loss of an aircraft from the CDTI.
- **b.** Verify correct operation of the equipment on board.
- **c.** Increase situational awareness by using visual search methods and radio communications to verify the position of the disappeared aircraft.

4.1.9 False Alarm Attack

ADS-B transponders have a mode to indicate de current status of the aircraft. For instance, the pilot can set a status of emergency or hijacked aircraft, information which is transmitted to the ATC ground station. The attack executes similar steps to virtual trajectory modification attack because the attacker has the options to delete and inject messages or just to modify the messages [52]. The purpose of the attack is to create a false alarm on the ATC

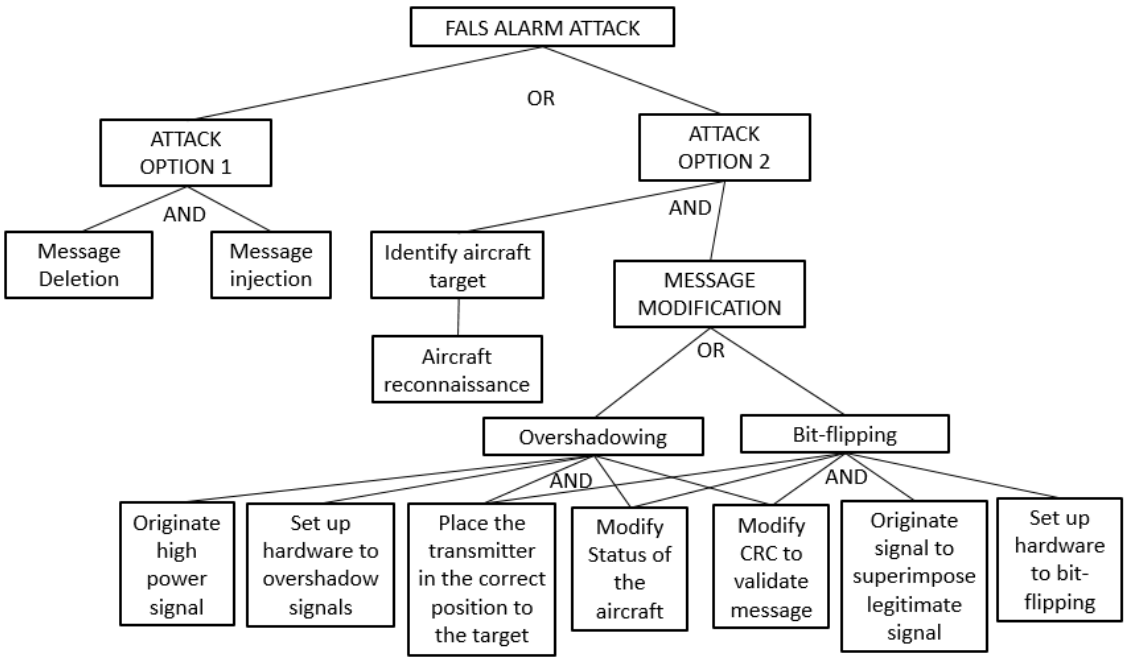

Figure 15. False Alarm Attack Tree.

Table 12. Classification of False Alarm Attack attack impact by aviation experts.

Participant	Severity
ATM expert	4
ATC	4
ATC	4
ATC	4
ATC	4

which has not been set by the crew of the respective aircraft. The attack affects the confidentiality and integrity of ADS-B.

Target: Ground segment and air-ground segment.

Attack Technique: Message deletion, message injection and message modification.

Technical Difficulty: Medium [57]. Figure 15 exhibits the combination of various techniques for executing false alarm attack. The attack tree shows the options that the attacker can choose after doing aircraft reconnaissance in order to identify the desired target.

Impact: Aviation experts in air traffic control classified the attack with a severity of four. The participants stated the same considerations. The increase in the air traffic controller workload would be caused due to the additional procedures that have to be followed in accordance to the regulations for each kind of alarm. They have to be followed even though the alarm is false. Table 12 shows the classification by ATM expert and air traffic controllers.

Analysis by aviation experts

It was determined by all the participants that the attack would not cause any critical situation but it would create safety concerns if the code is of a hijacked aircraft or aircraft emergency, and consequently that will increase the workload of the air traffic controller in an unnecessary task. A participant stated: “I would consider that many false alarms on different airplanes not only create confusion but also would draw the attention of the air traffic controller in tasks that are not needed at the moment”. It was also considered that radio communications with the crew will solve the problem, but in the case of a hijacked airplane the ATC cannot trust in the crew.

Mitigations:

- **a.** Follow the standard procedures given in the Document 4444 by ICAO [84] in the case of an emergency code such as 7700, 7600 and 7500.
- **b.** If there is not radio communication with the aircraft, it is needed to confirm with the airline the real status of the airplane.
- **c.** The same procedure applies if the aircraft has a hijacked code, and it is not possible to trust in the crew.

4.1.10 Aircraft Flood Denial

The attack has the main objective to jam the 1090 MHz channel or the GPS signals which are transmitting the information to the aircraft. It would cause the denial of service of ADS-B system that provides surveillance information to the aircraft. As noted by McCallie [7] the difficulty of the attack is determined based on the proximity that an attacker has to have to the aircraft. Therefore, a state sponsored attacker is the only one who might have the airborne equipment to approach in the air to a high altitude flying aircraft, for example a drone or a military aircraft with such capabilities [52]. The other attackers have the opportunity to jam the signals of an approaching or on the ground aircraft since they can have easy access to the facilities of an airport [57]. The attack affects the availability of ADS-B

Target: Air segment and air-ground segment.

Attack Technique: Jamming that disrupts 1090 MHz channel or GPS signals.

Technical Difficulty: Medium [7]. The steps considered for this attack (Figure 16) require jamming and the correct identification of the aircraft making use of aircraft reconnaissance.

Impact: Table 13 shows the classification of the attack made by the consulted pilots. The attack represents a real problem for the pilots as it can be evidenced in the similarity of the responses and the classification of the impact severity of the attack with a level of 3.

Analysis by aviation experts: The participants agreed that the attack raises safety concerns in congested air spaces and adversarial weather conditions, since the traffic is high and there is more probability of mid-air collisions. Providing information of the problem to the ATC will help to increase the situational awareness of air traffic controllers as well. All the participants stated that this attack could cause a possible mid-air collision because there is a loss of situational awareness about the traffic which is around the plane. Moreover, the loss of the traffic from the CDTI cause that the pilots do not have the ability to prevent a possible TCAS alarm with enough time in advance. It might be possible that TCAS uses ADS-B signals and therefore the system works with the reception of the signals of two aircrafts simultaneously. That means that while receiving the signals from only

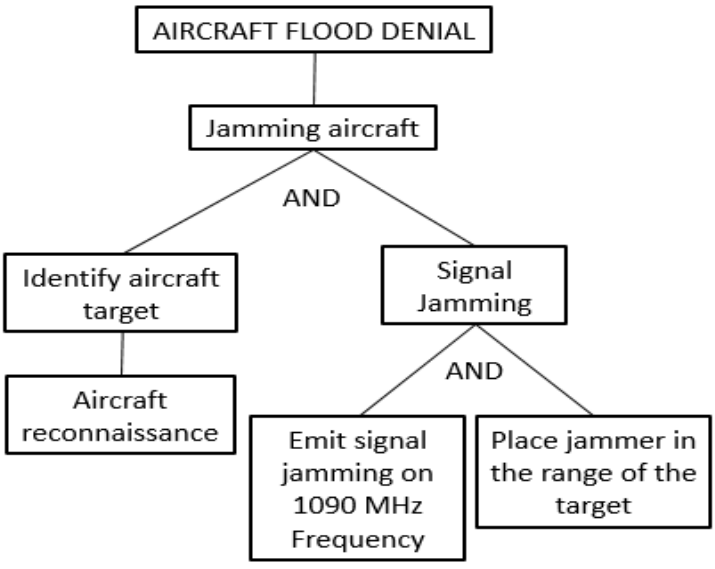

Figure 16. Aircraft Flood Denial Attack Tree.

Table 13. Classification of Aircraft Flood Denial attack impact by aviation experts.

Participant	Severity
PILOT	3
PILOT	3
PILOT	3
PILOT	3
PILOT	3

one airplane, the system would not give any advisory resolution to any crew.

The general perception was a real safety issue which can be manageable by the pilots with the radio communications with ATC and other aircrafts. However, they would be limited to the information of the ATC because of the loss of safety elements such as the ADS-B and TCAS.

Mitigations:

- **a.** Inform to ATC about the issue in order to confirm if the position of the aircraft is still displayed on the ATC radar screen.
- **b.** Increase situational awareness on radio communications to be aware of the other nearby aircrafts.
- **c.** Follow the instructions according to MEL for the maintenance of the aircraft.

4.1.11 Ground Station Flood Denial

The attack is executed with the same technique as for the aircraft flood denial attack. The attacker must get proximity to the ground station in order to emit jamming signals that disrupt completely ADS-B transmission and reception in the 1090 MHz frequency [7]. The attack affects the availability of ADS-B.

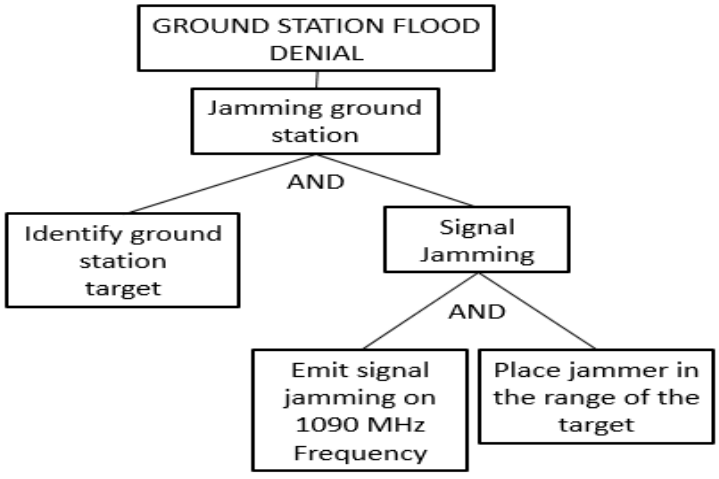

Figure 17. Ground Station Flood Denial Attack Tree.

Table 14. Classification of Ground Station Flood Denial attack impact by aviation experts.

Participant	Severity
ATM expert	2
ATC	2
ATC	2
ATC	2
ATC	2

Target: Ground segment and air-ground segment.

Attack Technique: Jamming that disrupts 1090 MHz channel or GPS signals

Technical Difficulty: Low [7]. Figure 17 depicts the straightforward steps that can be followed by an attacker and that confirms the low classification that cyber security experts give to this attack.

Impact: The classification made by the air traffic controllers considered the real loss of all the aircrafts shown on the screen (Table 14). The aviation experts classified the severity as level two, demonstrating that this attack might cause significant reduction of separation between aircrafts.

Analysis of aviation experts: The participants consider that losing the aircrafts from the radar screen might be a critical situation only if the air space is congested. The conventional control would help but there could be conflicts if the standard separation of the airplanes is reduced. An air traffic controller stated: "The loss of situational awareness is big; I would not remember where all the aircrafts were". The reorganization of the air space could take time and the capacity of the airspace is reduced, which will force many aircrafts to be diverted to alternate airports.

Mitigations:

- **a.** Switch to a less accurate surveillance system and reduce the capacity of the airspace.
- **b.** Inform to all the aircrafts of the air space about the problem in order to alert them and to increase the situational awareness of the crews.
- **c.** Divide the air space with other air traffic controller and extend the separation with aircrafts to reduce the probability of a mid-air collision.
- **d.** Start conventional control to send the airplanes to holding patterns or alternate airports in order to reduce the congestion.

4.2 Dynamic Analysis of Cyber Attacks against ADS-B

To complement the analysis it is important to assess the attacks based on a scenario-based approach as it is stated by McCallie [7]. However, the countless scenarios derived by many additional factors such as adverse meteorology conditions, amount of air traffic,

Table 15. Average severity of impact of attacks

Attacks	Severity of Impact Average	
Ground Station Flood Denial	2	
Aircraft Disappearance	ATC	2
Virtual Trajectory Modification	3	
Aircraft Flood Denial	3	
Ground Station Multiple Ghost Inject	3	
Aircraft Target Ghost Inject	4	
Aircraft Disappearance	PILOT	4
Ground Station Target Ghost Inject	4	
False Alarm Attack	4	
Replay Attack	5	
Aircraft Spoofing	5	
Aircraft Reconnaissance	None	

failures in other type of communications or emergencies in the aircraft, and that may occur in aviation due to the complexity of the system, will always limit the analysis. Therefore, the attacks are dynamically analyzed based on the threat model described in section 4.2.1 and the average impact results given by the aviation experts which are summarized in Table 15 from the most severe to the least severe attack.

4.2.1 Threat Model

A threat model is considered to focus the study in the main intentions of the attacker and to analyze the impact on the mission of aviation based on the results of the interviews. It was taking into consideration that the means to affect a safety critical infrastructure such as aviation, is not anymore only physical, but also cyber-physical, the integration and controlled coordination between on-board and off-board systems [85], and the transition from analog to digital communications in aviation [70], which are creating new possibilities for cyber attackers. The attackers are categorized based on the main objective that each attacker aims to achieve. The adversaries were categorized and analyzed as follows:

a. "Script Kiddies": this kind of attacker aims to execute actions with readily available software and hardware in the public market. Although the capabilities of script kiddies cannot be exactly defined, they can also perform attacks at different levels of difficulty if they can count with sensible information of the aeronautical network and operations. The main intention of the attacker is to cause confusion or annoyance to the air navigation traffic management.

Due to the availability of software tools such as software-defined radios (SDR), the script kiddies might execute any of the attacks analyzed on this thesis. The attacks might create confusion in the air traffic control or in the cockpit, if the attacker is in close proximity to an airplane. The attacks could become safety concerns into incidents as it is evidenced in the results given by aviation experts. However, the capacities to create an impact of large scale surpass the capabilities of this kind of attacker.

b. Cyber Criminals: category is divided into two groups according to the intention to better analyze the objectives of a criminal. This kind of attacker possesses quite considerable capabilities to cause an extensive impact on the system, also the equipment used is more complex in order to achieve the proposed effect.

- **Economic purpose attacker:** the attacker has as main objective to obtain an economic gain by means of cyber-attacks on ADS-B infrastructure.

An attacker who aims to get any profitable gain might use aircraft reconnaissance to gather information in order to make economic intelligence. In addition, the attacks against a specific aircraft such as aircraft target ghost inject and aircraft flood denial can be used to create safety concerns, related with the proper function of the CDTI display of the airplane, in the pilots and maintenance personnel. That would force to make an annotation on the book of the aircraft that might lead to ground the airplane. The economic gain is evidenced in the airlines and manufacturers that are competitors of the affected company.

Another consideration is related with other type of criminal such as smugglers or drug traffickers. These criminals can use ground station ghost inject attack to have the ability to divert the attention of the authorities to a ghost airplane while at the same time an illegal aircraft is using another trajectory to reach a desired destination. The event can only be considered in a Non-Radar Area (NRA).

- **Terrorist attacker:** the attacker has as main objective to create chaos and massive death of people to create fear. Aviation has been used for criminals to execute terrorist attacks such as the events on September 11 of 2001 and the long list of hijacked aircrafts in aviation history.

To create a huge chaos the terrorist attackers might use ground station multiple ghost inject, aircraft disappearance and ground station flood denial. These attacks were rated by the aviation experts as those that can cause the most severe impact in aviation system. Those attacks can create lots of confusion, which can lead to mid-air collisions and conflicts, but the certainty to achieve an accident is far from the capacities that a cyber attack might provide as it can be evidenced in the results of chapter 4. However, a special consideration is the use of aircraft reconnaissance to track commercial aircrafts, and use it as a tool to improve the efficiency to target a specific airplane with military weaponry.

c. State sponsored attackers: the category is divided into two groups according to the specific intention that the state wants to achieve at a high level. The attacker counts with specialized and military equipment to cause large-scale damage in ADS-B system and air navigation.

- **Cyberwarfare attacker:** the main intention of the attacker is to create cyber-attacks against ADS-B system with political motivations in order to affect financial stability of the target state.

The attacks can be executed massively since this kind of attacker can use tools that are more sophisticated. For instance, to create a large impact in the economy of a country it is useful to use ground station flood denial in many airports in the target country. The same

way as the massive attack using aircraft target disappearance to create conflicts in the most congested air spaces of the target and to make the biggest economic impact due to the delays and ground of many flights. The other attacks do not represent a real problem since the impact evaluated by the aviation experts would not cause the necessary damage intended by this kind of attacker.

- **Military attacker:** the main objective of the attacker is to execute attacks with high level equipment such as jammers, software, hardware and additional military weaponry to obtain a military advantage.

In order to gain any military advantage, aircraft reconnaissance plays a key role to identify those military airplanes, which are using ADS-B system without encryption. Moreover, the massive jamming on ground stations of the system would force to the enemy to use less accurate surveillance system. For that purpose, the ground station flood denial attack might be ideal to create the desired impact. With the advanced tools that a state sponsored attacker can use, the aircraft flood denial can be used to jam the signals not only of ADS-B, but also GPS of an aircraft, creating difficulties for military airplanes to execute high accuracy approaches while using the capabilities of ADS-B and GPS.

In a military context, the use of ground station multiple ghost inject can be used to create confusion to the enemy. The injection of multiple airplanes can deviate the attention to other areas to make a trap and to carry out an attack in a different target. Although this confusion can be neutralized with the use of a primary radar, with the elimination of primary radars around the world that might be a vulnerability.

5 Conclusions and Recommendations

5.1 Conclusions

This thesis accumulates the information and knowledge obtained from the academic, hackers and aviation communities to systematically analyze the cyber-attacks against ADS-B and to determine the possible impact that these threats can cause to aviation. For the purpose of the analysis, aviation experts were consulted in regards to the topic to get an approach to the truth, the safety impact of the attacks and the mitigations that can be executed by controllers and pilots to cope in this kind of situations. In this thesis, a different threat model was considered in order to make a dynamic analysis of the cyber-attacks and the possible intentions of the attackers. It was taking into consideration that the means to affect a safety critical infrastructure, such as aviation, are not anymore only physical, but also cyber-physical due to the availability of open source software-defined radios that are creating new possibilities for cyber attackers.

The findings of this thesis have identified the lack of awareness of aviation experts about the vulnerabilities of ADS-B. It was determined that the experience and the capacitation that aviation personnel have could be an important factor to deal with a cyber-attack. The study identified that the common effect caused by the attacks in air traffic controllers is the increment of workload. The attacks could be dangerous depending on the level of congestion of the airspace, the magnitude of the attack and the conditions in the moment of execution. Additionally, the results of pilots interviews considered that the attacks might cause loss of situational awareness and force to take unexpected decisions that might lead to undesirable consequences. The study identified as a concern how to identify a cyber-attack against ADS-B. The detection part is the most difficult for the operators of the system. The procedure after the detection can be executed according to the experience and criteria of the air traffic controllers and pilots. Therefore, the aviation professionals require training to identify the different cyber-attacks against ADS-B system

The analysis classified aircraft disappearance and ground station flood denial with the maximum level of severity of impact among all the cyber attacks. The severity of 2 for these attacks was given according to OSA ED78A/DO264 classification matrix. It was determined that these attacks can cause enough confusion to make the air traffic controllers to lose situational awareness of the controlled airspace. The common factor of the attacks is the disappearance of one or all the aircrafts. Therefore, it can be concluded that disappearing is more dangerous that injecting a ghost aircraft or modifying an ADS-B message.

Aircraft target ghost inject, ground station target ghost inject, false alarm attack and aircraft flood denial were classified with an impact severity of 3 or 4. These attacks with medium severity cannot cause a major effect in the aeronautical operations. The attacks also might be handled with the current tools and procedures that aviation experts currently have. On the other hand, ground station multiple ghost inject attack was assessed by all the ATC experts with a severity of 3. Since the increase in the workload of the air traffic controllers could be higher, there could be lots of confusion if the switch to other surveillance system is not executed immediately. In addition, an ATM expert explained that the attack might be mitigated with filtering procedure due to the fusion of information with other surveillance system; however, it was also noted that the multiple injection could overload the data processor system and leave the ATC without display.

The attacks assessed and classified with impact severity of 4 or 5 were aircraft spoofing and replay attack. The analysis revealed that these attacks are easy to identify and easy to handle due to the straightforward manner to correlate the information of the “ghost airplanes” with information provided by air navigation service provider or airlines. With the current procedures the air traffic controllers are able to deal with the attacks with no further consequences.

The dynamic analysis assessed attackers with different profiles and intentions. One of the main intentions is to create confusion. The attackers who aim low level objectives might use attack techniques such as single injections or single message modifications to achieve a specific low level purpose. On the other hand, the high level attackers require a combination of cyber attacks to genreate enough confusion in aviation system, such as massive disappearance of aircrafts or ground station flood denial. However, based on the analysis the cyber-attacks do not provide the attackers with the certainty and the sufficient ability to cause an accident.

5.2 Recommendations

The main recommendation is to create awareness about the vulnerabilities of the system to pilots and air traffic controllers. In order to provide more capacitation to face this kind of events it is recommended to train aviation personnel with ATC and aircraft simulators with scenerios of cyber-attacks. The training would give more abilities to identify a cyber attack stuation and would provide knowledge of procedures that must be folllowed to avoid any mislead action.

The second recommendation is to encourage aviation and information technology industries to work together on the discovery, research and mitigation of cyber threats. Experiments in real environments should be exectuted to determine the feasibility and the consequences of a cyber attack against ADS-B. That would allow to take the necessary meassures to face the attacks, instead of waiting until an accident occurs to issue new regulations or procedures as it has been evidenced in aviation in the aftermath of every accident.

6 References

[1] Center for the Protection of National Infrastructure. Cyber Security in Civil Aviation ver.1.2010 [WWW] http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf?epslanguage=en-gb (27.02.2016)

[2] ICAO, ACP. "Manual for the ATN using IPS Standards and Protocols (Doc 9896)." (2009)

[3] Sampigethaya, K., Poovendran, R. and Bushnell, L., 2010, March. Assessment and mitigation of cyber exploits in future aircraft surveillance. In *Aerospace Conference, 2010 IEEE* (pp. 1-10). IEEE.

[4] Wood, R.G.: A security risk analysis of the data communications network proposed in the nextgen air traffic control system. PhD thesis, Stillwater, OK, USA (2009)

[5] Spiewak, D., Engel, T. and Fusenig, V., 2007. Unmasking threats in mobile wireless Ad-Hoc network settings.- *WSEAS Transactions on Communications*, 2007, 6(1), 104-110.

[6] Ben-Asher, N., Gonzalez, G. Effects of Cyber Security Knowledge on Attack Detection.- *Computers in Human Behavior*, 2015, 48, 51-61

[7] McCallie, D., Butts, J. and Mills, R. Security analysis of the ADS-B implementation in the next generation air transportation system. -*International Journal of Critical Infrastructure Protection*, 2011, 4(2), 78-87.

[8] Federal Aviation Administration. Automatic Dependent Surveillance-Broadcast ADS-B OUT Performance Requirements to Support Air Traffic Control Service; Final Rule, Federal Aviation Administration, "FAA's NextGen Implementation Plan," Washington, DC, March 2011. 14 CFR Part 91.- Federal Register, May 28, 2010, 75(103)

[9] Gomez, L. and Sierra, I.T. Implementation of Automatic Dependent Surveillance (ADS-B) in Colombia- *In 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague,* 2015, *2B2-1 - 2B2-9.*

[10] Costin.A. and Francillon, A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices- *Black Hat USA*, 2012, 7, 1-12.

[11] American Institute of Aeronautics and Astronautics. A Framework for Aviation Cybersecurity. 2013 [WWW] https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf (12.03.2016)

[12] International Federation of Air Line Pilots' Association. 2013.14POS03. Cyber Threats: Who controls your aircraft? [WWW] http://www.ifalpa.org/store/14POS03%20-%20Cyber%20threats.pdf (13.03.2016)

[13] Siu, M., Goh,D. and Lim,C .Aviation Cyber Security: A New Security Landscape.- *Journal of Aviation Management*, 2014, 154–165.

[14] Stoop, J.A. and Kahan, J.P. Flying is the safest way to travel: How aviation was a pioneer in independent accident investigation.- *European journal of transport and infra-*

structure research, 2005, 5 (2), 115-128.

[15] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection. December 17, 2013 [Online] https://www.dhs.gov/homeland-security-presidential-directive-7 (22.02.2016)

[16] Aviation infrastructure performance: A study in comparative political economy. Brookings./ Eds. Winston, C. and de Rus, G. Institution Press. 2009.

[17] Deloitte. Transforming the Air Transportation System A business case for program acceleration, 2011 [Online] http://s3.amazonaws.com/zanran_storage/www.deloitte.com/ContentPages/2513816742.pdf (12.11.2015)

[18] Nolan, M. Fundamentals of air traffic control. Cengage Learning, 2010.

[19] National Air Traffic Controllers Association. A History of Air Traffic Control, 2013 [Online] http://tol.natca.org/NATCA_Local_TOL/Reloaded_Commitee_files/ATCHistory2.pdf (11.01.2016)

[20] AAAE. Air Traffic Control, Airspace and Navigational Aids, 2005.

[21] Document 9985 – Air Traffic Management Security Manual (1st Edn). Montreal. International Civil Aviation Organization. 2014.

[22] Sampigethaya, K. and Poovendran, R. Aviation cyber–physical systems: foundations for future aircraft and air transport.- *Proceedings of the IEEE*, 2013, 101(8), 1834-1855.

[23] Prasad, K.V., Broy, M. and Krueger, I.Scanning advances in aerospace and automobile software technology.- *Proceedings of the IEEE,* 2010, 98 (4), 510–514.

[24] Rife, C. T., and Enge, P. Scanning theissue: Special issue on aviation information systems.- *Proceedings of the IEEE*, 2008, 96 (12), 1898–1901.

[25] Casals, S.G., Owezarski, P. and Descargues, G. Risk assessment for airworthiness security. Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, 2008, 25-36.

[26] Federal Aviation Administration. 14 CFR Part 25, Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security Protection of Airplane Systems and Data Networks From Unauthorized External Access, Federal Register, 2007, 72:72. [Online]. http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf (12.03.2016)

[27] O'Hare, D., Wiggins, M., Batt, R. and Morrison, D. Cognitive failure analysis for aircraft accident investigation. -*Ergonomics*, 1994, 37(11), 1855-1869

[28] Wiegmann, D.A. and Shappell, S.A. Human error and crew resource management failures in Naval aviation mishaps: a review of US Naval Safety Center data, 1990-96. Aviation, Space, and Environmental Medicine, 1999, 70(12), 1147-1151.

[29] Yacavone, D.W. Mishap trends and cause factors in naval aviation: a review of Naval Safety Center data, 1986-90. -*Aviation, space, and environmental medicine*, 1993, 64(5), 392-395

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

[31] Stern, D. 1998. Teen hacker faces federal charges. [WWW] http://edition.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html?eref=sitesearch (11.04. 2016)

[32] Andrew Wood. Newark Airport GBAS Vulnerable to Truckers' GPS Jammers.-*Ainoline*, 2011.01. 2015.[WWW] http://www.ainonline.com/aviation-news/ainalerts/2011-01-25/newark-airport-gbas-vulnerable-truckers-gps-jammers (24.03.2016)

[33] International Civil Aviation Organization. Working Paper. In *TWELFTH AIR NAVIGATION CONFERENCE Montréal, 19 to 30 November 2012*. [Online] http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf (25.03.2016)

[34] A. Williams. Jets vanishing from Europe radar linked to war games.-*Reuters*, 13.06 2014. [Online]. http://www.reuters.com/article/us-europe-airplanes-safety-idUSKBN0EO1CW20140613(11.2015)

[35] Circular, Advisory. "120-76B." Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags (2012).

[36] Lundberg, D., Farinholt, B., Sullivan, E., Mast, R., Checkoway, S., Savage, S., Snoeren, A.C. and Levchenko, K. On the security of mobile cockpit information systems. *In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, 633-645.

[37] Administration, F.A.: Federal Register, 2008, 73(1).[Online] https://www.gpo.gov/fdsys/pkg/FR-2007-04-16/pdf/07-1838.pdf

[38] FAA Tells Boeing To "Hack Proof" 747-8, -8F.- *Aero News Network*, October 12, 2010

[39] Teso, H. Aircraft hacking. Conference presentation in *HITB Security Conference, Amsterdam, The Netherlands, April 2013* [WWW] https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf (15.04.2016)

[40] Malia Zimmerman. Security expert pulled off flight by FBI after exposing airline tech vulnerabilities.-*Fox News*, 2015, April 17 [WWW] http://www.foxnews.com/us/2015/04/16/security-expert-pulled-off-flight-by-fbi-after-exposing-airline-tech.html (11.04.2016)

[41] Moran,N. and G. De Vynck, WestJet Hijack Signal Called False Alarm. Bloomberg, Jan 2015. [Online]. Available (11.02.2016)

[42] Rekkas, C. and Rees, M. Towards ADS-B implementation in Europe. In Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, 2008. TIWDC/ESAV 2008. Tyrrhenian International Workshop on, 3-5 September 2008, 1-4. doi:10.1109/TIWDC.2008.4649019

[43] The roadmap for delivering high performing aviation for Europe.- European ATM Mas-

ter Plan Executive View Edition 2015

[44] Strohmeier, M., Schäfer, M., Lenders, V. and Martinovic, I.. Realities and challenges of nextgen air traffic management: the case of ADS-B. *Communications Magazine*, 2014, 52(5), 111-118

[45] Kingsley, S. and Quegan, S. Understanding radar systems. SciTech Publishing, 1999.

[46] Skolnik, M.I. Radar Handbook, 3rd ed. McGraw-Hill, 2008.

[47] Stevens, M.C. Secondary surveillance radar. Artech House on Demand, 1988

[48] RTCA Inc. Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broad-cast (ADS-B).- *DO-242A (including Change 1),* Dec.2006.

[49] Magazu III, D., 2012.Exploiting the automatic dependent surveillance-broadcast system via false target injection:master thesis. Ohio, Air Force Institute of Technology, Department of electrical and computer engineering, 2012

[50] Federal Aviation Administration. NextGen Implementation Plan. 2014 [Online] http://www.faa.gov/nextgen/library/media/nextgen_implementation_plan_2014.pdf (23.03.2016)

[51] ADS-B Aviation Rulemaking Committee, Recommendations on Federal Aviation Administration Notice No. 7-15, Automatic Dependent Surveillance - Broadcast ADS-B OUT Performance Requirements to Support Air Traffic Control Service. Notice of Proposed Rulemaking, 2008. [Online] https://www.faa.gov/nextgen/programs/adsb/media/arcReport2008.pdf (12.02.2016)

[52] Strohmeier, M., Lenders, V. and Martinovic, I. On the security of the automatic dependent surveillance-broadcast protocol. -*Communications Surveys & Tutorials*, 2015, 17(2), 1066-1087

[53] Purton, L., Abbass, H. and. Alam, S. Identification of ADS-B system vulnerabilities and threats. -In: *Proceedings of the Australasian Transport Research Forum* 29 *September – 1 October 2010, Canberra, Australia*. [Online] http://atrf.info/papers/2010/2010_purton_abbass_alam.pdf

[54] Agbeyibor, R.C. Secure ADS-B: Towards Airborne Communications Security in the Federal Aviation Administration's Next Generation Air Transportation System: master thesis. Ohio, Department of the Air Force Air University, Air Force Institute of Technology, 2014.

[55] Li, W. and Kamal, P.. Integrated aviation security for defense-in-depth of next generation air transportation system. *-In Technologies for Homeland Security (HST), IEEE International Conference on November 2011*, 136-142

[56] Sampigethaya, K. and Poovendran, R. Visualization and Assessment of ADS-B Security for Green ATM. - *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th*, Salt Lake City, UT, 2010, 3.A.3-1 - 3.A.3-16.

[57] Schäfer, M., Lenders, V. and Martinovic, I. Experimental analysis of attacks on next generation air traffic communication.- *Applied Cryptography and Network Security*, Springer Berlin Heidelberg, 2013, 253-271.

[58] ICAO. Guidance Material: Security Issues Associated with ADS-B, 2008. [Online] http://www.icao.int/APAC/Documents/edocs/CNSdocs/01gd_security_adsb.pdf (15.03.2016)

[59] Strohmeier, M., Lenders, V. and Martinovic, I., 2013. Security of ADS-B: State of the Art and Beyond. -*arXiv preprint*, 2013.

[60] Günter, K.. Radarscape and The Mode S Beast. [WWW] http://www.modesbeast.com/ (23.03.2016)

[61] Costin.A. and Francillon, A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. -*Black Hat USA*, 2012, 7, 1-12.

[62] Kinetic. Kinetic Avionics Limited, 2016[WWW] http://www.kinetic.co.uk/ (17.04.2016)

[63] Flightaware. Have a Kinetic SBS-3? 2016 [WWW] https://flightaware.com/adsb/sbs3/ (17.04.2016)

[64] Wilhelm, M., Martinovic, I., Schmitt, J.B. and Lenders, V. Short paper: reactive jamming in wireless networks: how realistic is the threat? *In Proceedings of the fourth ACM conference on Wireless network* sec*urity*, Hamburg, Germany, June 14 - 17, 2011, 47-52.

[65] Federal Aviation Administrator. NextGen Implementation Plan. NextGen Integration and Implementation Office, Federal Aviation Admin, Washington, DC, 2010, [Online] http://www.faa.gov/nextgen/media/ngip_3-2010.pdf

[66] Hoey, D. and Benshoof, P. Civil GPS Systems and Potential Vulnerabilities.- *Proceedings of ION GNSS 18th International Technical Meeting of the Satellite Division*, Long Beach, CA, September 13-16, 2005.

[67] General Accounting Office, Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed, 2002 [Online] http://www.gao.gov/new.items/d02781.pdf

[68] No Jam Tomorrow. -The Economist, March 11, 2011 [WWW] http://www.economist.com/node/18304246 (22.04.2016)

[69] Kim, A., Wampler, B., Goppert, J., Hwang, I. and Aldridge, H. Cyber attack vulnerabilities analysis for unmanned aerial vehicles.- *Infotech@ Aerospace*, 2012, 1-30.

[70] Mahmoud, M.S.B., Pirovano, A. and Larrieu, N. Aeronautical communication transition from analog to digital data: A network security survey.- *Computer Science Review*, 2014, 11, 1-29.

[71] McCallie, D.L. Exploring Potential ADS-B Vulnerabilites in the FAA's Nextgen Air Transportation System: master thesis. Ohio, Department of the Air Force Air University, Air Force Institute of Technology, 2011.

[72] Schneier, B.Secrets and lies: digital security in a networked world. John Wiley & Sons. 2011.

[73] EUROCAE. Safety, performance and interoperability requirements document for ADSB/NRA application, 2005 [Online] http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=1B5FA6C6E410ECA27CABC

401A5CAD248?doi=10.1.1.129.6059&rep=rep1&type=pdf

[74] Ericson, C.A. and Ll, C. Fault tree analysis.- *In System Safety Conference, Orlando, Florida*, 1999, 1-9.

[75] Gay, L.R., Mills, G.E. and Airasian, P. Educational research: Competencies for analysis and research, Upper Saddle River, N.J.: Pearson Merrill Prentice Hall, 2006.

[76] Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V. and Martinovic, I. On Perception and Reality in Wireless Air Traffic Communications Security.- *arXiv preprint arXiv*:1602.08777, 2016.

[77] Silva, S., Jensen, L. and Hansman Jr, R.J. Pilot Perception and Use of ADS-B. -*Traffic and Weather Services (TIS-B and FIS-B)*, 2014.

[78] Sampigethaya, K., Poovendran, R. and Bushnell, L. A framework for securing future e-enabled aircraft navigation and surveillance.- *AIAA Proceedings*, 2009, 1-10.

[79] Japan PM's official plane 'tracked online'-BBC News, 2014, September 4 [WWW] http://www.bbc.com/news/world-asia-29057971 (14.04.2016)

[80] Cenciotti David, U.S. airborne communication plane could be tracked on the Web for 9 hours during air strike that killed Taliban leaders in Afghanistan-The Avionist, 2014, August 13 [WWW] http://theaviationist.com/2014/08/13/ (03.04.2016)

[81] EUROCONTROL. ACAS II equipage requirements, 2016 [WWW] http://www.eurocontrol.int/articles/acas-ii-equipage-requirements (30.03.2016)

[82] Costin, A. and Francillon. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.-*Black Hat USA*, 2012, 1-12.

[83] Renderlab. Hackers + Airplanes = No Good Can Come Of This. -*Proceedings of Defcon* 20, Las Vegas, NV, USA, 26–29 July 2012.

[84] ICAO, P. Air Traffic Management. Doc-4444, 2007.

[85] Sampigethaya, K. and Poovendran, R. Cyber-physical system framework for future aircraft and air traffic control. In Aerospace Conference, March 2012 IEEE, 2012. 1-9, IEEE.

Appendix

Background of participants

PARTICIPANTS DISCIPLINE	EDUCATION	BACKGROUND	YEARS OF EXPERIENCE	ADS-B OPERA-TION
ATM EXPERT	Bachelor in Navigation and Surveillance Sytems	Local support engineer	10	YES
	Master's Degree, Telecommunications	Estonian Air Navigation Services Engineer		
	Doctor of Philosophy (PhD), Electrical, Electronics and Communications Engineering	Head of Surveillance and Navigation Systems Subdivision Estonian Air Navigation Services		
		ATM Expert Estonian Air Navigation Services		
ATC	Tartu Aviation College degree	Lennart Meri Airport Air Traffic Controller	15	YES
	Technical Training	Estonian Air Navigation services		
ATC	Bachelor in Aeronautical Engineer	El Dorado Airport Air Traffic Controller	18	YES
	Master's Degree in Aviation Safety	Aviation Safety Consultant		
ATC	Bachelor in Aeronautical Engineer	Millitary Air Traffic Controller	25	YES
	Master's Degree in Aviation Safety	El Dorado Airport Air Traffic Controller		
		Aviation Safety Consultant		
ATC	Bachelor in Aeronautical Engineer	El Dorado Airport Air Traffic Controller	30	YES
	Master's Degree in Aviation Safety			
		Aviation Safety Consultant		

PILOT	Bachelor Aeronautical Administration, Colombian Air Force Academy	Military Pilot	18	YES
		Fokker 50 Copilot/Pilot		
		Airbus 320 Copilot/Pilot		
		Boeing 787 Copilot/ Pilot		
PILOT	Bachelor Aeronautical Administration, Colombian Air Force Academy	Military Pilot	14	YES
		Boeing 737 Copilot/ Pilot		
		Airbus 330 Copilot/Pilot		
PILOT	Bachelor in Aeronautical Science, Pacific Aviation Academy	Fokker 50 Copilot/Pilot	16	YES
		Airbus 320 Copilot/Pilot		
PILOT	Bachelor Aeronautical Administration, Colombian Air Force Academy	Military Pilot	15	YES
		Airbus 318 Copilot/Pilot		
PILOT	Bachelor in Aeronautical Science, Pacific Aviation Academy	Airbus 320 Copilot/Pilot	18	YES
		Boeing 767 Copilot/Pilot		

Air traffic controllers questionnaire

AIR TRAFFIC CONTROLLERS QUESTIONAIRE

PREDICTED REACTIONS OF AIR TRAFFIC CONTROLLERS TO CYBER ATTACKS AGAINST ADS-B SYSTEM

Camilo Pantoja

Section 1: Formal information of the interviewed person:

Name of Organization:

Position :

Section 2: Main questionnaire:

The current implementation of ADS-B is being carried out worldwide and there are still concerns related with the vulnerabilities that could be exploited through the identified cyber-attacks. The attacks might affect the confidentiality, integrity and availability of the system. The attacks against confidentiality provides to the attacker unauthorized information. The attack against integrity modifies the information of ADS-B messages and the attacks against availability disrupt the access to the information of the system.

Now we are going through the attacks which affect the confidentiality, integrity and availability of ADS-B. Every attack will be explained for your knowledge and then a set of questions will be asked for every attack. The attacks are Ground Station Target Ghost Inject, Ground Station Multiple Ghost Inject, Replay Attack, Aircraft Spoofing, Virtual Trajectory Modification, Aircraft Disappearance, False Alarm Attack and Ground Station Flood Denial.

a. Do you have any standard procedure to deal with this situation?
b. How do you believe you can cope with it?
c. How would you rate the impact of the attack according to OSA ED78A/DO264 classification matrix?
d. What would be the most critical situation that the attack might cause?

Pilots questionnaire

PILOTS QUESTIONAIRE

PREDICTED REACTIONS OF PILOTS TO CYBER ATTACKS AGAINST ADS-B SYSTEM

Camilo Pantoja

Section 1: Formal information of the interviewed person:

a. Name of Organization:

b. Position :

Section 2: Main questionnaire:

The current implementation of ADS-B is being carried out worldwide and there are still concerns related with the vulnerabilities that could be exploited through the identified cyber-attacks. The attacks might affect the confidentiality, integrity and availability of the system. The attacks against confidentiality provides to the attacker unauthorized information. The attack against integrity modifies the information of ADS-B messages and the attacks against availability disrupt the access to the information of the system.

Now we are going through the attacks which affect the confidentiality, integrity and availability of ADS-B. Every attack will be explained for your knowledge and then a set of questions will be asked for every attack. The attacks are Aircraft Target Ghost Inject, Aircraft Disappearance and Aircraft Flood Denial.

a. Do you have any standard **procedure** to deal with this situation?

b. How do you believe you can cope with it ?

c. How would you rate the impact of the attack according to OSA ED78A/DO264 classification matrix?

d. What would be the most critical situation that the attack might cause?

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Camilo Andres Pantoja Viveros**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright of my thesis.

Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts,

(title of thesis)

supervised by Olaf Manuel Maennel, Raimundas Matulevicius

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **19.05.2016**