3-2021

A Cyber Threat Taxonomy and a Viability Analysis for False Injections in the TCAS

John W. Hannah

A CYBER THREAT TAXONOMY AND A VIABILITY ANALYSIS FOR FALSE INJECTIONS IN THE TRAFFIC COLLISION AVOIDANCE SYSTEM (TCAS)

THESIS

John W Hannah, B.A.M., Captain, USAF

AFIT-ENG-MS-21-M-045

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-21-M-045

A CYBER THREAT TAXONOMY AND A VIABILITY ANALYSIS FOR FALSE INJECTIONS IN THE TCAS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

John W Hannah, B.A.M., B.A Mathematics

Captain, USAF

March 25, 2021

AFIT-ENG-MS-21-M-045

A CYBER THREAT TAXONOMY AND A VIABILITY ANALYSIS FOR FALSE INJECTIONS IN THE TCAS

THESIS

John W Hannah, B.A.M., B.A Mathematics
Captain, USAF

Committee Membership:

Robert F. Mills, Ph.D
Chair

Patrick J. Sweeney, Lt Col
Member

Richard Dill, Maj
Member

Abstract

Safety is a simple concept, but an abstract task, specifically with aircraft. One simple aberration from standard flight procedure and hundreds of individual lives are at-risk. One critical safety system during flight is the Traffic Collision Avoidance System (TCAS). TCAS protects against mid-air collisions by communicating an aircraft's location with the surrounding aircraft. If TCAS falters, the only protection against a mid-air collision is the pilot's ability to visually recognize a dangerous situation. This necessity of an operational TCAS warrants further investigation into its shortcomings. Therefore, to understand its shortcomings, this thesis delves into the technical specifications of TCAS and Mode S and presents a taxonomy of threats and threat actors. The cause of these shortcomings is from an adversary intentionally targeting TCAS, rather than mechanical or design failure. The threat taxonomy presents 4 threats, with false injection having the most substantial detriment to the system. After broaching the threat taxonomy, the thesis further explores the requirements for a successful false injection attack against TCAS. This includes timing Mode S messages to satisfy the following requirements: a range test, an altitude test, a received signal power test, and a directional heading requirement, or bearing constraint. Following requirement development, the thesis introduces the development of a MATLAB simulation of a ground-based adversary targeting a Boeing 737-800 with Mode S communications. The ground-based adversary false injects a spoofed Boeing 737-800 into the air picture. The program tests various ranges, altitudes, and bearings for the target aircraft, ultimately comparing the results to the requirements of TCAS. With verified and validated results, the thesis provides a clear threat picture for false injection attacks against an aircraft.

Table of Contents

Page

Page

List of Figures

List of Tables

A CYBER THREAT TAXONOMY AND A VIABILITY ANALYSIS FOR FALSE INJECTIONS IN THE TCAS

I. Introduction

Air travel is the second most used mode of travel in the United States [1]. Over 1 billion travels use aircraft as their mode of transportation. The Federal Aviation Administration (FAA) is the primary policing force for air traffic standards. The mission for the FAA focuses on providing safe aerospace systems for air travel users [1]. The mission statement highlights the importance of safety in the air travel sector.

The FAA mandates aircraft have a collision avoidance system operational at all times [2]. TCAS is the certified implementation of Aircraft Collision Avoidance System (ACAS). Traffic Collision Avoidance System (TCAS) protects against mid-air collisions by monitoring the relative airspace of an aircraft. TCAS uses Mode S transponder communications for collision avoidance. If an aircraft enters a specified zone, the TCAS monitoring screen notifies the pilot and provides recommendations on correcting the situation.

1.1 Motivation

National Aeronautics and Space Administration (NASA) conducted experiments using real world flights and simulations, and the results showed that without an operational TCAS, 4 declared near mid-air collisions (less than 1000 feet horizontal and 200 feet vertical separation) occurred during 32 total flights [3]. With an operational TCAS, zero near mid-air collisions occurred across 96 total flights. Without TCAS, the probability for a near mid-air collision increased by 12.5 percent. Additionally,

the study proved that TCAS is a premiere safety system, and when operational, there is an almost zero percent chance for a mid-air flight collision occurring.

Another study focused on pilot trust in aircraft cyber-physical systems [2]. The results demonstrated that TCAS is the most trusted system on the aircraft. Pilots follow TCAS recommendations whenever provided with no distrust in the recommendations.

Given two-way radio frequency capabilities, specifically the software-defined radio (SDR), unequivocal trust in TCAS is not achievable nor is it prudent for passenger safety [4]. SDRs provide a vector for adversaries to craft malicious RF messages, including Mode S TCAS messages, to subvert pilot trust in TCAS. The ease of obtaining an SDR paired with the RF message processing and creation presents a threat to the integrity of Mode S messages used by TCAS. These threats mandate further investigation into potential attacks and capabilities.

1.2 Problem

This thesis focuses on TCAS security, both generally and specifically. It contributes to the academic, professional, and industry understanding of TCAS vulnerabilities. First, using open-source documents and reports, the thesis answers the following question: What are the possible vulnerabilities/threat actors associated with TCAS and its communication process? The thesis enumerates and characterizes risks to TCAS. After risk are discussed, the prominent risk chosen to further explore is a false injection.

False injection, also known as spoofing, presents a capability for a threat actor to introduce distrust into the TCAS system. That distrust has second and third-order effects that may have a potential impact on passenger safety. A previous study [4] on TCAS spoofing occurred, but there were assumptions made. This thesis further

centers on determining specific requirements to implement the false injection attack. This answers the question: What are the requirements to satisfy the range test, altitude test, and bearing constraints of TCAS?

Lastly, with the false injection requirements known, the last contribution focuses on simulating timing-based false injection attacks against TCAS. In specific, the simulation implements a ground station, a target aircraft, a spoofed aircraft, and all the requirements from the previous questions. This contribution answers the following question: What conditions allow a ground-based adversary to appropriately time responses and falsely-inject a realistic aircraft into a target aircraft's TCAS, eventually triggering an RA?

1.3 Organization

Chapter II provides necessary background knowledge of TCAS and Mode S. It details TCAS processes and capabilities that support the threat taxonomy and the methodology of the false injection program. Additionally, Chapter II presents TCAS components to assist with understanding what is impacted during potential attacks. Lastly, the chapter discusses TCAS warning notifications and their respective thresholds.

Chapter III presents a novel threat actor model and TCAS attack taxonomy. The chapter classifies TCAS threat actors from various other cyber threat models. Second, the chapter examines the capabilities of those threat actors. Third, the chapter defines an attack taxonomy using previous studies in other cyber-physical aircraft systems, presenting them in a formalized threat tree. Lastly, the chapter compares the actors with potential attacks, determining likely attacks by particular threat actors,

Chapter IV studies and presents requirements for timing, the range test, altitude test, power test, and bearing constraints. Additionally, the chapter discusses the

methodology in creating a simulation to implement those requirements during a false injection attack against a target aircraft, B737, from a ground-based attacker. Also, the chapter presents and implements how TCAS tracks and projects paths of aircraft and speed/turning capabilities of simulated aircraft. Lastly, the chapter discusses starting ranges, altitudes, and bearings of target aircraft, determining the ending horizontal time to impact (TAU) values for warning notification threshold comparison.

Chapter V analyzes the results from the simulation in Chapter IV. The chapter presents the average TAU values of each set of 500 simulations and determines which range, altitude, and starting bearing combination present a false injection vulnerability. Additionally, the chapter provides a statistical analysis of the skewness and kurtosis of the data, and compares them against normal distribution requirements. Lastly, the chapter presents the percentage of success for each starting range, altitude, and bearing, resulting in the development of threat maps for pilots.

Chapter VI discusses the impact of the simulation results and the attack taxonomy. Also, the chapter presents rudimentary solutions to the issues and discusses future work possibilities of TCAS security research. Lastly, Chapter VII concludes the thesis and overviews all work performed.

1.4 Scope

Initially, this thesis analyzes the threats of TCAS and its communications processes. Afterward, the thesis details the methodology and requirements for the false injection attack. The limitations relate to physical access to a non-stationary TCAS system. All data regarding TCAS communications comes from technical mandates and previous experiments, rather than physical access to a TCAS system.

Additionally, the false injection simulation focuses on the B737. It is the most widely-used commercial aircraft in flight operations around the world [5]. With ad-

justed parameters for aircraft, the false injection attack and partnering simulation apply to other aircraft. The simulation focuses on the cruising sector of a flight profile. At this point, the target B737 is at its cruising speed with an altitude that remains relatively constant. The takeoff and landing section of the flight profile are not analyzed.

II. Introduction to Mode S and TCAS

This chapter discusses the history of Mode S and TCAS. Additionally, the chapter presents a detailed overview of Mode S and TCAS, along with its components. This knowledge is vital in understanding components of the TCAS threat taxonomy and false injection requirements detailed in future chapters.

2.1 History of Mode S and TCAS

The creation of Mode S started with the Identification Friend or Foe (IFF) system [6]. Great Britain developed the IFF system during World War II. It created the system to determine if an aircraft was friendly or hostile. The base components include a ground-based transmitter used to broadcast radio signals and a transponder that receives and replies to signals. Aircraft equipped with IFF respond to interrogation modes employed by specific countries and/or alliances. If an interrogated aircraft responds correctly, the interrogating aircraft labels it as friendly. Contrarily, if an interrogated aircraft responds incorrectly or IFF cannot decipher the signal, the interrogating aircraft labels it as an unknown aircraft, or as hostile. As air travel increased across the United States, air traffic control (ATC) required more robust identification capabilities than IFF [6]. In 1975, this requirement resulted in the development of Mode S that offers identification capabilities and increased data transmission size. In parallel to the development of Mode S, the need for a mid-air collision system came to light.

On June 30, 1956, a mid-air collision between two aircraft occurred near the Grand Canyon in Arizona, resulting in the death of 128 individuals [7]. Four years later, there was a collision in New York City resulting in the death of 134 individuals [7]. These catastrophes identified a lack of safety, prompting the ATC evolution

and necessitating technology updates to aircraft radar systems. In 1961, due to the mid-air collisions, President Kennedy ordered the Federal Aviation Administration (FAA) to conduct a review of current aviation technology and create a long-term plan to enhance air safety [6]. The plan consensus was creating an improved radar system, known as the Air Traffic Control Radar Beacon System (ATCRBS).

ATCRBS follows the same interrogation principle as TCAS; interrogations broadcast from an antenna and any aircraft equipped with ATCRBS would then respond [6]. ATCRBS uses 1030 MHz and 1090 MHz frequencies and two types of interrogators. The interrogators were Mode A and Mode C. Mode A identified the aircraft, while Mode C determined the aircraft's altitude. Due to growth limitations, in 1971, the FAA began specifying a new system that would help improve air traffic safety while ensuring backward compatibility with ATCRBS. The FAA committee developed the requirements for the new system and contracted the physical implementation of the system to the Massachusetts Institute of Technology - Lincoln Laboratory (MIT-LL). They developed Discrete Address Beacon System (DABS), later known as Mode S. Mode S requirements included backwards compatibility with Mode A and Mode C. Also, MIT-LL decided to have Mode S use addresses to interrogate aircraft and reduce radio frequency traffic.

In parallel to the development of Mode S, the FAA also asked for the creation of a collision detection system [7]. A number of systems were created and tested; however, an exorbitant number of false alarms occurred. In 1974, Andrew Zeitlin and the MITRE center began creating the capability for a system to perform aerial surveillance of its surroundings using its existing transponders [8]. During the development of the system, two aircraft collided near San Diego airport resulting in the death of 144 individuals [7]. This incident forced the FAA to mandate the implementation of an aerial surveillance system. The FAA decided to use the Mitre Center for Advanced

Aviation System Development (CAASD) developed capability from 1974. CAASD partnered with Lincoln Labs at Massachusetts Institute of Technology to finalize the system, now known as TCAS [8]. In 1986, another collision occurred between two aircraft in Mexico, resulting in 82 fatalities [7]. This led to the FAA mandating all passenger and commercial aircraft to be equipped with TCAS in 1987 [7][8]. The last major update to TCAS requirements was TCAS 7.1, implemented in 2011.

2.2 Overview of Mode S

A transponder is a radio transmitter and receiver combined to allow automatic communications with aircraft and ground radar sites [9]. Mode S equipped aircraft selectively interrogate other aircraft [10]. This occurs when an aircraft replies to an original all-call or broadcast interrogation. Figure 1 displays a simple overview of the communication dynamic for Mode S between an aircraft and a ground station.

Once a reply is received, the next Mode S interrogation specifies the aircraft by its unique aircraft address, commonly referred to as the International Civil Aviation Organization (ICAO) address. The ICAO address is a 24-bit address used to identify aircraft. Mode S sends interrogations to other aircraft at 1030 MHz and sends/receives unencrypted responses at 1090 MHz, allowing for interception. Mode S uses Uplink Format (UF) and Downlink Format (DF) for communications. UF is a specific interrogation originating from an aircraft asking specific addressable information about another aircraft. DF is the reply from the aircraft. For UF interrogations, TCAS uses UF-0, UF-11, and UF-16. For DF replies, TCAS uses DF-0, DF-11, and DF-16 formats. Figure 2 presents the message formats for all of the above-listed UFs and DFs.

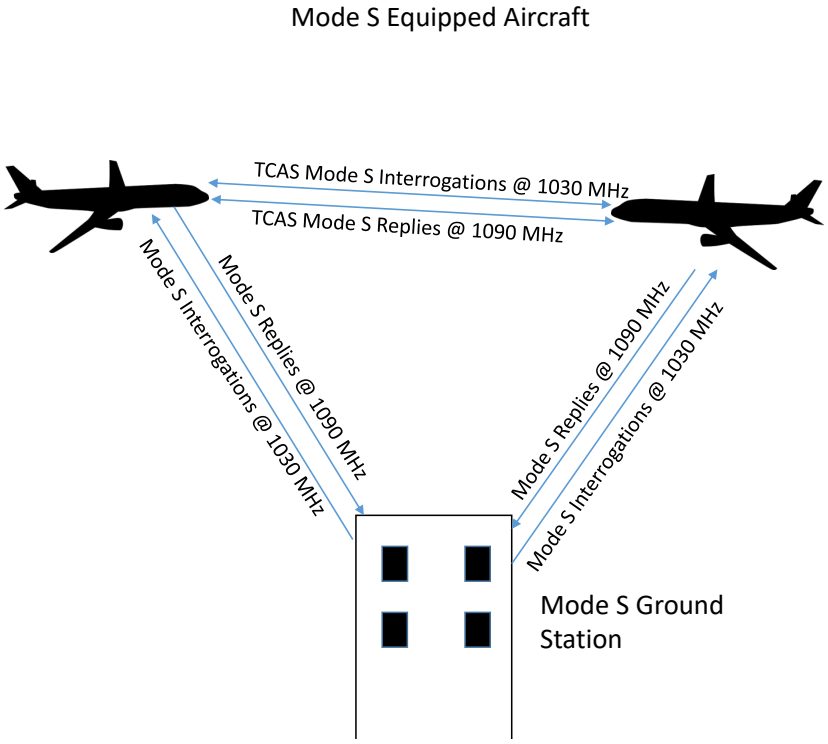

Figure 1: Mode S Communications Overview: Interrogations and Replies between Aircraft and a Ground Station [9].

UPLINK FORMATS FOR TCAS

UF: 0	00000	3	RL: 1	4	AQ: 1	18	AP: 24	Short Air-to-Air Surveillance
UF: 11	01011	PR: 4	IC: 4	CL: 3	16	AP: 24		Mode S All-Call Interrogation
UF: 16	10000	3	RL: 1	4	AQ: 1	18	MU: 56	AP: 24	Long Air-to-Air Surveillance

DOWNLINK FORMATS FOR TCAS

DF: 0	00000	VS: 1	7	RI: 4	2	AC: 13	AP: 24	Short Air-to-Air Surveillance
DF: 11	01011	CA: 3	AA: 24	PI: 24				Mode S All-Call Reply
DF: 16	10000	VS: 1	7	RI: 4	2	AC: 13	MV: 56	AP: 24	Long Air-to-Air Surveillance

Figure 2: TCAS Uplink and Downlink Formats: The Mode S formats for TCAS interrogations and responses [11].

2.2.1 Mode S Acquisition

Mode S acquisition is the first step in TCAS communications [12]. The Mode S system uses a squitter, an all-call broadcast interrogation, to interrogate surrounding aircraft. TCAS specifically uses the UF-11 (56-bit) format to send broadcast interrogations to all surrounding aircraft. Those all-call interrogations contain an interrogator code (IC). The IC is an address for the Mode S radar. Once an aircraft receives the UF-11 interrogation, the aircraft decodes the IC and decides whether to reply or ignore the interrogation. If the two aircraft have no previous communications, then the aircraft replies with an all-call reply. If the two aircraft previously communicated, they are considered associated and Mode S discards the message. Once an interrogating aircraft receives a DF-11 all-call reply, that aircraft decodes and checks the IC and the ICAO address. The interrogating aircraft determines the position of the aircraft by the reply. At this point, the associating process completes and TCAS ignores all other all-call broadcasts. It is important to note that DF-17, known as an extended squitter, offers the same capability for acquisition. After Mode S acquires a target, selective interrogations begin.

2.2.2 Selective Interrogations

Once an aircraft locks onto another aircraft using all-call, the originating aircraft sends selective interrogations using the ICAO address [12]. Upon selective interrogation, an aircraft cannot respond to all-call broadcasts. For selective interrogations, TCAS uses UF-0/DF-0 and UF-16/DF-16. TCAS uses UF-0/DF-0 for short air-to-air interrogations. These formats belong specifically to TCAS/ACAS. DF-0 replies include both the altitude and the ICAO address of the aircraft. Two other major components of DF-0 replies include the vertical status (VS) and the reply information (RI) field. The VS field indicates if the aircraft is in-flight or grounded. A VS

value of 1 indicates an aircraft is airborne. A VS value of 0 indicates an aircraft is grounded. The RI field is a four-bit word that relays the speed capability of the aircraft.

UF-16/DF-16 is used for long air-to-air interrogations and surveillance for TCAS. The major difference between UF-16/DF-16 and UF-0/DF-0 is the length. UF-16/DF-16 is 112 bits long and UF-0/DF-0 is 56 bits long. They have many other similar aspects. For example, DF-0 and DF-16 replies contain the reported altitude and the ICAO address. Selective interrogations include a parity overlay. The ICAO address is the parity overlay. It ensures the message contents do not have any errors. Additionally, DF-16 replies contain the VS and RI fields. They both still indicate if the plane is grounded and its speed capability. Additionally, the Altitude Code (AC) field in both DF-16 and DF-0 replies is the reported altitude.

2.3 TCAS Overview and Components

TCAS [13] is an aviation-based system used as a protective measure against mid-air collisions between aircraft. In the United States, TCAS is a required component for all aircraft that carry 30 or more passengers. European regulations require aircraft to have TCAS if carrying 20 or more passengers. TCAS [14] is comprised of different components that allow the aircraft to process signals from other aircraft, send signals to other aircraft, and make decisions regarding the data sent and received. The components that comprise the TCAS system include the TCAS computer unit, the Mode S transponder, the TCAS control panel, the antennas, and the display. Figure 3 displays the components of the TCAS system, and the communication links between each component.

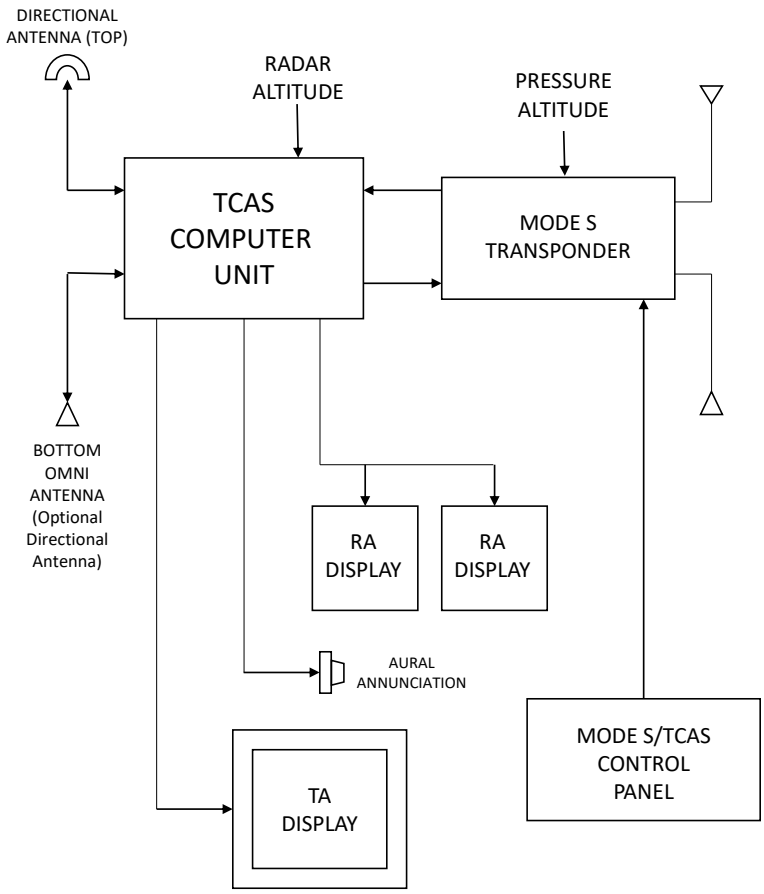

Figure 3: TCAS Component Overview: All components of the TCAS system [14].

2.3.1 Computer Unit

The computer unit is the hub of the TCAS system [14]. It is responsible for air surveillance, detection of possible threats, tracking of those threats once identified, and tracking the plane's altitude. The most important responsibility of the TCAS computer unit is the RA determination and generation of advisories and avoidance maneuvers. The computer unit notifies the pilots of imminent danger and offers a maneuver solution to avoid collision with the threat.

2.3.2 Mode S Transponder

TCAS uses the Mode S transponder to perform its communications between aircraft [11]. The Mode S overview describes the Mode S communications used: UF-0/DF-0, UF-11/DF-11, and UF-16/DF-16.

2.3.3 TCAS Control Panel

The TCAS control panel provides pilots manual control of the Mode S transponder and TCAS system [14]. Mode S settings for pilots include:

- Transponder: In this setting, the Mode S transponder communicates with all ground ATC systems and responds to TCAS interrogations from other planes; however, the on-board TCAS system is in Stand-by Mode.
- Stand-by: The TCAS processor and Mode S transponder receive power; however, the TCAS system does not actively interrogate the airspace around the aircraft. The aircraft's transponder still replies to discrete interrogations, as mandated by the FAA.
- TA Only: In this setting, the TCAS and Mode S transponder operate normally. TCAS interrogates nearby aircraft and maintains a consistent and accurate air picture. In this mode, the TCAS system only issues traffic alert (TA)s but not resolution advisory (RA)s.
- Automatic or TA/RA: Automatic is the fully operational TCAS and Mode S mode. TCAS conducts all tracking and alert notifications on board.

2.3.4 Antennas

In previous aircraft, four major antennas support the operations for TCAS [11]. In modern-day aircraft, there are two antennas. Mode S and TCAS share the antennas.

The TCAS antennas include a top-mounted directional antenna and either an omnidirectional or directional antenna attached to the bottom of the aircraft. These antennas transmit TCAS interrogations 360 degrees at 1030 MHz frequency. The antenna mounted on the bottom of the aircraft does not transmit as many interrogations as the top antenna. Both transponders receive interrogation replies at 1090 MHz. Upon receiving interrogation replies, TCAS sends them to the computer unit.

The two Mode S antennas mount to the bottom and top of the aircraft. Reverse the TCAS antennas, the Mode S antennas reply to interrogations at 1090 MHz and receive those interrogations at 1030 MHz. Since all of the antennas share the same frequencies, when one is transmitting, the other is disabled.

2.3.5 Displays

TCAS has two integrated displays [14]. The displays include the traffic display and the RA display. The traffic display provides a consistent air picture of surrounding aircraft that reply to interrogations. This provides an accurate air representation to the pilots. The RA display activates when another aircraft enters its imminent threat zone. In the imminent threat area, the intruding aircraft is a threat to the safety

Figure 4: TA and RA Displays: The left display is the TA display and the right is the RA display [14].

of the aircraft. The RA display aids the pilots by providing vertical speed or pitch recommendations to avoid a mid-air collision. Figure 4 shows a TCAS traffic display on the left and an RA display on the right. The TCAS traffic display shows several different aircraft on the screen, with the red block displaying a threat to the aircraft. The blue diamond on the screen represents another aircraft of no danger to the host aircraft. The RA display on the right shows the red line indicating an RA is in place. The aircraft maintains constant altitude; however, the recommendation is that the aircraft climb between 1500 to 2000 feet per minute. This recommendation is evident in the green section of the circle around the screen. The red block on the RA screen shows an aircraft 5 nautical miles to the right of the aircraft and only 200 feet below the aircraft, hence the recommendation to climb.

2.4 TCAS Warning Notifications

For horizontal collision detection, TCAS [15] uses the range threshold, TAU. It determines when a TA or RA is mandatory. TCAS calculates TAU and compares it to set values. TAU is an estimate of time-to-collision based on separation and closure rate. For vertical collision detection, TCAS uses time to co-altitude (vertical TAU), and vertical separation (ZTHR). The computation for vertical TAU is the vertical separation divided by the vertical closure rate between the two aircraft. With the altitude of both aircraft, vertical TAU, and the horizontal TAU, TCAS decides on the issuance of a TA or RA. Issuance of a TA or RA occurs when one of the following occurs:

- Exceed Horizontal TAU and ZTHR
- Exceed Horizontal TAU and Vertical TAU
- Exceed DMOD and ZTHR

- Exceed DMOD and Vertical TAU

2.4.1 Traffic Advisory

TCAS issues a TA whenever an aircraft becomes a threat to the aircraft [14]. A TA assists the pilot with visually locating the intruding aircraft and preparing the pilot for a possible RA. Responses to TCAS interrogations contain altitude values. TCAS determines range by the response time of the reply. With the altitude, range, and TAU, the aircraft decides whether to issue an RA. Those values compare to the TAU, DMOD, and ZHTR values in Table 1. The TA projects as a yellow dot on the RA display, as shown in Figure 4. If an intruder reports his or her altitude incorrectly, a vulnerability with Mode C, TCAS issues TAs due to horizontal closure only. TA is the precursor to the issuance of an RA for an intruding aircraft. Table 1 displays the thresholds for when a TA triggers. TAU is the same for horizontal and vertical limits [16].

2.4.2 Resolution Advisory

Once TCAS classifies an aircraft as an intruder, it is interrogated on a set time interval [11]. Using data from replies, the interrogating aircraft computes TAU and co-altitude. TCAS compares them against the thresholds of TAU, DMOD, and ZHTR,

Table 1: TA Thresholds

Ownship Altitude	SL	TAU(seconds)	DMOD(nmi)	ZTHR(feet)
< 1000	2	20	0.3	800
1000-2350	3	25	0.33	800
2350-5000	4	30	0.48	800
5000-10000	5	40	0.75	800
10000-20000	6	45	1.0	800
20000-42000	7	48	1.3	800
> 42000	7	48	1.3	1200

Table 2: RA Thresholds

Ownship Altitude	SL	TAU(seconds)	DMOD(nmi)	ZTHR(feet)
< 1000	2	N/A	N/A	N/A
1000-2350	3	15	0.2	600
2350-5000	4	20	0.35	600
5000-10000	5	25	0.55	600
10000-20000	6	30	0.8	600
20000-42000	7	35	1.1	700
> 42000	7	35	1.1	800

shown in Table 2. If the values exceed the thresholds, TCAS displays an RA notification on the pilot's TCAS screen. The TCAS display shows a red dot to represent an intruding aircraft on the TCAS display. The additional RA display displays the current altitude rate highlighted in red, as shown in Figure 4. The red dot also displays on the RA screen. Additionally, if an aircraft does not report its altitude, an RA cannot be generated for it. This presents a security concern, as the countermeasure for the intruder aircraft shifts to the visual identification skills of the pilot.

Once an aircraft exceeds the thresholds for an RA issuance, as shown in Table 2, it must resolve the RA. The TCAS computer unit is responsible for the generation and resolution steps of RAs. The initial step of the computer unit determines if the aircraft needs to ascend or descend based on the range and altitude of the intruding aircraft. The host aircraft then determines its flight path. The necessity for the altitude in this step is why non-altitude reporting aircraft cannot trigger an RA. The second step of the issuance process is the computer unit determining the strength of the RA. RA strength refers to whether the host aircraft needs a flight path bound by a vertical speed limit or an increase in the magnitude of the altitude rate. A vertical speed limit is a reduction in the rate of climb, and in many cases, leads to the aircraft leveling off. A magnitude increase is when TCAS recommends the aircraft to climb in altitude by a certain rate. TCAS uses TAU and DMOD for horizontal alerts.

III. Threat Actor and Attack Taxonomy

3.1 Threat Actor Model and Analysis

To understand TCAS threats, an individual must understand possible adversaries. At the time of this thesis research, there were no published threat actor analyses for TCAS. A model used to classify cyber threat actors against the Automatic Dependent Surveillance - Broadcast (ADS-B) protocol is the baseline for this model's development [17]. Also, two additional resources focused on air communication attacks, provide insight into developing the threat actors [18, 19].

This model categorizes threat actors based on their end-state goal, skill-set, and overall risk to the TCAS system. The following sections discuss the requirements for each category.

3.1.1 End-State Goals

End-State Goals refer to the desired end-state by a threat actor. Many models classify them based on their specific goal; however, this model focuses on the risk of their end-state goal. The end-state model classifications include high-risk, medium-risk, and low-risk. The details are listed below:

- High-Risk: An end-state goal classifies as high-risk if the goal is to deny, disrupt, degrade, or destroy a TCAS system. High-risk end-state goals are permanent solutions.

- Medium-Risk: An end-state goal classifies as medium-risk if the goal is to deny, disrupt, or degrade a TCAS system. Medium-risk end-state goals are temporary solutions until the threat actor meets the set goal.

- Low-Risk: An end-state goal classifies as low-risk if the actor has no intention to deny, disrupt, degrade, or destroy a TCAS system.

3.1.2 Skill-sets

Skill-sets refer to the technical capabilities of threat actors. The skill-set model classifications are high ability, medium ability, and low ability. The details are listed below:

- High Ability: A skill-set would classify as high ability if the actor can deny, disrupt, degrade, or destroy a TCAS system. A high ability skill-set can act from the air or ground. Also, a high ability skill set can cause persistent negative effects against the system.

- Medium Ability: A skill-set would classify as medium ability if the actor can deny, disrupt, or degrade a TCAS system. A medium ability skill-set can act from the ground. Also, a medium ability skill set can cause non-permanent negative effects against the system.

- Low Ability: A skill-set would classify as low ability if the actor cannot deny, disrupt, degrade, or destroy a TCAS system. A low ability skill-set only acts from the ground.

3.1.3 Overall Risk

Overall risk refers to true risk to the TCAS system, based on the skill-set and end-state goal. If the skill-set and end-state goals are both high, the overall risk is high. If either the skill-set or end-state goal is medium, the overall risk is medium. If either the skill-set or end-state goal is low, the overall risk is low.

3.1.4 Determined Threat Actors

The common adversaries associated with cyber-attacks are known as script kiddies, hacktivists, insider threats, organized crime, and advanced persistent threats [17]. Since TCAS is a communication system, those adversaries are a starting baseline for threat actors against TCAS. With further reduction, the list narrows to advanced persistent threat (APT), insider threats, criminal organizations, and script kiddies. Hacktivists do not fit the criteria for an possible threats against a safety critical system. Script kiddies are individuals with interest but no expertise in the area of cyber-attacks. Within the air communication community, the equivalent of script kiddies is hobbyists. Hobbyists replace script kiddies in this threat actor model. Figure 5 shows the classifications of each threat actor. The main column is the overall risk. It relays the true risk of an actor to the communication integrity of TCAS and Mode S. Subsequent sections provide further detail on each actor category.

3.1.4.1 Hobbyists

Hobbyists, similar to script kiddies, are individuals that have a genuine interest in the topic, specifically TCAS. This includes individuals that own a software-defined radio and track aircraft from their homes. Also, this includes universities that study Mode S aircraft communication. Most hobbyists complete their tasks from the ground. The threat posed by hobbyists is minimal to the safety of the aircraft; however, the intelligence provided by hobbyists provides intelligence to both criminal organizations and advanced persistent threats.

Hobbyists post gathered data on social media or input it to the ADS-B/TCAS tracking sites available online. A report released by BuzzFeed in August 2017 demonstrates this government intelligence risk. The report released flight tracks for certain military aircraft after individuals used ADS-B Exchange paired with a basic artifi-

Actor	End-State Goal	Skill-Set	Overall Risk
Advanced Persistent Threats	High Risk	High Ability	High
Insider Threat	High Risk	Medium Ability	Medium
Criminal Organizations	Medium Risk	Medium Ability	Medium
Hobbyists	Low Risk	Low Ability	Low

Figure 5: TCAS Threat Actor Model Results: A color-coded representation of end-state goals, skill-sets, and overall risks for each threat actor.

cial intelligence algorithm to discover military and government operations [20]. This demonstrates the impact that a software-defined radio (SDR) and/or access to a site with ADS-B/TCAS information offers. The data impacts operations and the safety of government and commercial. For this, hobbyists are TCAS threat actors; however, they do not impact the overall capabilities of a TCAS system.

3.1.4.2 Insider Threats

A report into airport security notes that Transport Security Administration (TSA) does not have adequate processes in place to guarantee the successful detection of an insider threat. In the aviation domain, an insider threat is an employee that uses their access privileges to exploit vulnerabilities with a goal of causing harm to aircraft or customers of aircraft services [21].

Financial incentives are possible motivational factors for insider threats, specifically from other airlines. A near mid-air collision creates the possibility of distrust

in a company's ability to safely fly passengers. Additionally, emotions drive insider threats due to negative events that have occurred within their organization. Even though motivations differ, some insider threats have direct access to the onboard TCAS system. If the insider threat is a pilot, they have direct control of the system. Physical access to a system presents a threat actor with the ability to cause considerable harm to the system. A potential possibility is a complete disable of the system; however, any additional pilots are able to reactivate TCAS and/or the Mode S transponder at any point. Since an insider threat cannot cause a permanent disabling of the system, their overall skill-set is only medium-risk.

3.1.4.3 Criminal Organizations

The next level of threat actors is criminal organizations. Even though there are no documented cases of criminal activity with TCAS-equipped aircraft, the risk is still present, especially as the knowledge of TCAS and ADS-B spreads. Criminal organizations typically focus on conducting operations that provide monetary gain. While there are no direct monetary gains in affecting TCAS systems, there are secondary effects. A secondary effect represents a consequence, positive or negative, from a primary mission or conducted operation. For instance, if a criminal organization can disrupt the air picture of an air traffic control tower or of an aircraft charged with tracking illegal aircraft, a criminal organization could bypass security checkpoints. Bypassing security checks allows the ability to transport any items without fear of discovery. This is just an example scenario; however, the ability and the incentive are there for criminal organizations. For this reason, they are a medium risk to the TCAS system.

3.1.4.4 Advanced Persistent Threats

APT is an overarching term for several groups that severely impacts the integrity and operational capability of TCAS. There are several sub-groups within the advanced persistent threat group. These groups' capabilities include disabling or destroying TCAS from both the ground and air. These sub-groups include nation-state militaries, state-sponsored groups, and terrorist organizations. The below list discusses these sub-groups in more detail.

- Nation-State Militaries: Nation-state militaries are militaries associated with different countries. These militaries equip themselves with technology that affords direct interaction with aircraft systems, including TCAS. The militaries have the capability to interact with aircraft on the ground and in the air. This sub-group poses the biggest risk to the confidentiality, integrity, and availability (CIA) of the TCAS system.

- State-Sponsored Groups: State-sponsored groups receive monetary support from a country's government; however, they are not directly associated with the government or military of the country. They are similar to nation-state militaries in their overall capabilities. The difference is that state-sponsored groups are limited to air operations within their host nation. This diminishes the capability to affect TCAS systems in an air-to-air environment unless the airspace is within their nation.

- Terrorist Organizations: Terrorist organizations are groups that conduct operations due to their religious or cultural beliefs. The objectives of terrorist organizations range from scare tactics to causing harm to citizens of other opposing nations or groups. The capabilities are similar to that of nation-state militaries; however, the tactics are less sophisticated. These organizations do

not typically have air-to-air access to other TCAS-equipped aircraft; however, it is still possible and requires consideration.

3.2 TCAS Threat Taxonomy Based on Threat Actor Model Results

With the potential threat actors, a taxonomy of threats for the TCAS system becomes plausible. Thorough research of the technical specifications in [11] and research of various other attack taxonomies against Mode S communication systems offer the determination of possible threats and attacks against TCAS. The presented attacks are only plausible from the threat actors in Section III. The main component focus of this section is on the Mode S transponder, TCAS control panel, and TCAS computer unit. Any impact on the two devices will impact the entire TCAS system. Since ADS-B uses Mode S, the attack model from [22] assists in the development of possible threats. The attack categories are passive and active attacks. A passive attack is an attack that does not require physical access or the ability to generate interrogations or replies. Active attacks require the threat actor to generate interrogations, replies, or physically interact with the system. There is one passive attack: eavesdropping, and three active attacks: ghosting, Denial-of-Service (DoS), and false injection.

3.2.1 Eavesdropping

Eavesdropping describes passively listening and collecting aircraft Mode S traffic. Since Mode S messages are unencrypted, their content is open to anyone. A threat actor would setup an SDR with an antenna and collect UF-11 TCAS all-call broadcasts. These messages will have the ICAO address of the aircraft, as well as the altitude and range. This information within these messages is easily logged and tracked. Publicly available sites contain information about the ICAO address. This information

can include the owners of the aircraft, including military affiliations. Gathering this information is an intelligence-gathering activity.

Eavesdropping provides threat actors with insight into daily activities and schedules. The unencrypted nature allows any individual or organization to passively listen to broadcast air traffic. Eavesdropping is the one passive attack possible against a TCAS system.

3.2.2 Ghosting

Ghosting is when an actual aircraft is not visible on TCAS displays to other aircraft. To accomplish this attack, an individual needs physical access to the TCAS control panel. This is considered an active attack against a TCAS system since it requires physical interaction. The most likely threat actor in this scenario is an insider threat.

If a pilot becomes an insider threat, this attack becomes plausible. Once airborne, a pilot can place TCAS in stand-by. An aircraft in stand-by replies only to discrete interrogations. Other interrogations from surrounding aircraft do not receive a response. Pilots also can disable the Mode S and Mode C transponders onboard [23]. Without active transponders, TCAS cannot issue or complete interrogations or replies. Without interrogations or replies, TCAS cannot advise TAs or RAs to other pilots.

The inability to receive or transmit TAs or RAs has a grave impact on air safety. An aircraft is much more likely to encounter a mid-air collision without an alert. This applies to the ghosting aircraft and any surrounding aircraft.

3.2.3 Denial-of-Service

In networking terminology, a DoS is an event that denies, degrades, or destroys the ability for a device or organization to communicate with other devices. This same principle applies to transponder communications between aircraft. Jamming is an implementation of DoS attacks.

Jamming is an electronic warfare attack capability that focuses on interrupting a signal at specific or multiple frequencies. Jamming creates a denial-of-service attack against radar systems. Once a signal is interrupted, the aircraft cannot correctly process signals. For TCAS, the 1090 MHz is the focus as it is the frequency for TCAS replies. The attacks jam the receivers of the intended targets, so they are prevented from recognizing and interpreting legitimate TCAS responses. With the advancement of technology, low-cost SDRs offer the ability to perform jamming techniques. Jamming offers multiple variations; however, the focus in on spot jamming and deceptive jamming [24].

Spot jamming occurs when a jammer focuses all its power on one particular frequency. A ground-based threat actor equipped with an SDR and an antenna offers an example spot-jamming scenario. The antenna has enough power to reach at least 35,000 feet and overpower the originating transponder's signal power. The antenna would need to reach 35,000 feet since most aircraft cruise between 31,000 and 38,000 feet [25]. In this scenario, an aircraft sends a TCAS interrogation to an aircraft at 1030 MHz. After a three microsecond delay, the interrogated aircraft replies at the 1090 MHz. Once the threat actor discovers the aircraft, they begin broadcasting garbled information at the 1090 MHz frequency. The antenna uses the highest amount of power to overcome the power of the Mode S transponder on the replying aircraft.

Deceptive jamming, similar to spoofing, senses incoming radar signals, alters the data within the signal, and then broadcasts them [24]. Range, azimuth, velocity, and

an establishment of an RA or TA are alterable fields. A threat actor captures a reply from the interrogated aircraft and then alters the contents. Once an aircraft is within the TA range, the threat actor has less than 40 seconds to broadcast the altered reply. Once the threat actor broadcasts the altered reply, the TCAS computer unit cannot distinguish between the correct reply and the false reply.

In these jamming schemes, the threat actor denies the aircraft from receiving valid replies, preventing TCAS from triggering an RA or TA. Also, the pilot is not alerted to malicious activity and continues to trust TCAS. The lack of integrity of the air picture along with the inadequate situational awareness of the pilot increases the chance of a mid-air collision.

This attack is plausible by any of the proposed threat actors except insider threats with the purchase of a basic SDR and antenna. Criminal organizations and advanced persistent threats can purchase more advanced equipment and further disrupt an aircraft from sending and receiving Mode S transponder signals.

3.2.4 False Injection

False injection is disguising communication from an untrusted source as communication from a trusted entity [26]. False injection allows an actor to inject aircraft into a target's air picture. The following section details the requirements for a false injection attack against a TCAS system. The requirements divide into 3 phases: Acquire, Emulate, and Trigger.

3.2.4.1 Acquire

The first step of false injection requires a threat actor to determine the International Civil Aviation Organization (ICAO) addresses of the surrounding aircraft. The ICAO address is the identification alphanumeric for each aircraft. A threat actor

could use a UF-11 message to interrogate all nearby aircraft [4]. In the DF-11 replies, the aircraft reports the ICAO address, altitude information, and range. Additionally, a threat actor could listen for UF-11 all-call interrogations from other aircraft. Those all-call messages contain the IC of the Mode S transponder and the ICAO address of the aircraft. Knowing the ICAO address of the target, the threat actor will choose a lower ICAO address. A lower ICAO address refers to an ICAO address that is numerically or alphabetically first between the two aircraft. The aircraft with the lower ICAO address takes priority during TA or RA maneuver selection.

3.2.4.2 Emulate

The threat actor inserts the chosen ICAO address into the AP field of a DF-11 reply to the target aircraft's UF-11 all call. Additionally, they insert the necessary altitude in the DF-11 reply. Both aircraft determine the range between the aircraft by the round-trip travel time (RTT) of an interrogation and a reply. After the first DF-11 reply, the target aircraft specifically interrogates the false aircraft by ICAO address. Over an average of 3 messages, the false aircraft must maintain an altitude and a range that meets the TAU, DMOD, and ZTHR requirements. The threat actor falsely injects the altitude into the DF-11 reply. The range requirement is satisfied by the threat actor making the RTT shorter between interrogation and reply messages. The threat actor then replies to the TCAS interrogation within three microseconds. If the false reply altitude, range, or timing requirements are not met, the TCAS system discards the spoofed aircraft.

3.2.4.3 Trigger

If the threat actor satisfies the altitude and range requirements, they can trigger an RA on the target aircraft with a resolution advisory complement (RAC). UF-16

messages contain the RAC field. The target aircraft will then register an RA alert on its TCAS screen for a spoofed aircraft. To continue the presence of an RA alert, the threat actor must send a UF-16 message at least every 3 seconds with the RAC field set [4].

A representation of false injection is shown in Figure 6. In this scenario, the attacker has already satisfied the altitude and range requirements for the target aircraft. At this point, the spoofed aircraft is sending a UF-16 with the RAC field set. This triggers an RA alert on the target aircraft, resulting in a successful attack.

This type of attack diminishes the integrity of the air picture. In an extreme scenario, the flight path of an aircraft alters. This type of attack is feasible by any of the three threat actors discussed. The most likely actor to accomplish due to need is an advanced persistent threat.

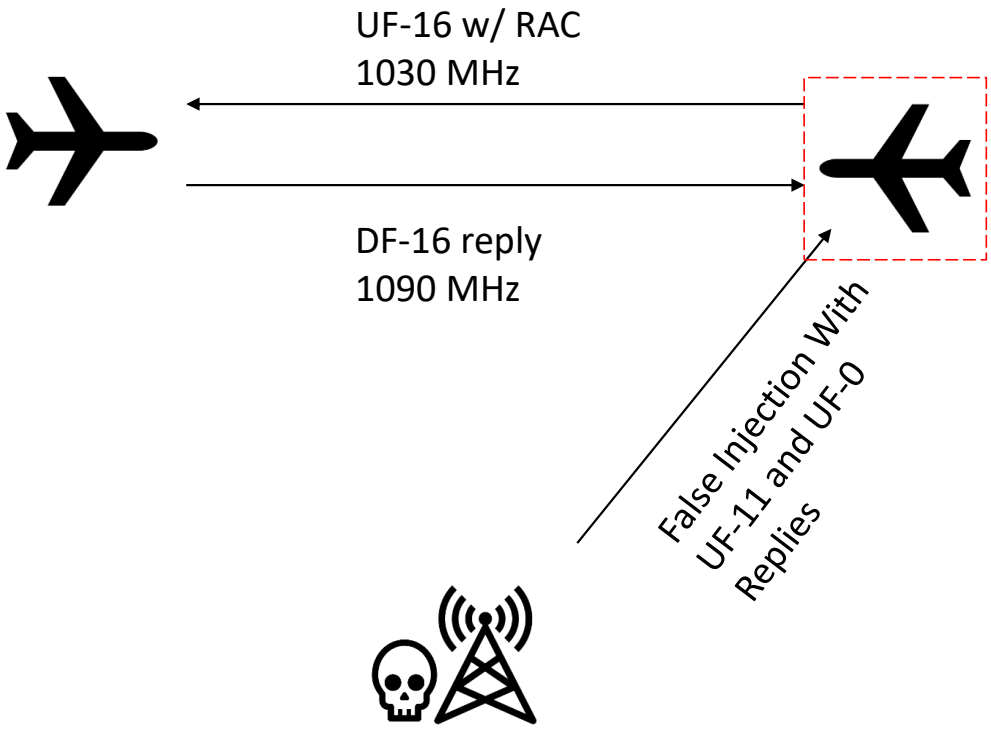

Figure 6: False Injection Graphic - Basic representation of false injection attack.

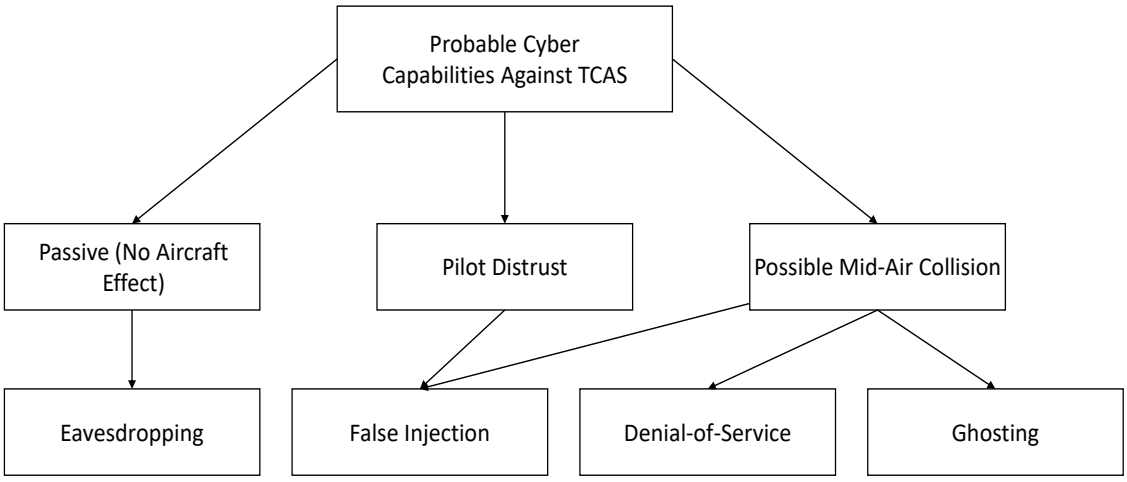

Figure 7: Formalized Threat Tree: Representation of Threats and Possible Outcomes.

3.2.5 Formalized Threat Tree

The determined attacks allow the creation of a formalized threat tree to understand the plausible effects on TCAS. Figure 7 illustrates the formalized threat tree. There are three outcomes considered from the attacks: passive, pilot distrust, and a possible mid-air collision. The threat tree notes that false injection has pilot distrust and a mid-air collision as possible outcomes. It is the only noted attack with two possible outcomes.

3.2.6 Chart Discussion

Figure 8 illustrates the threat actors' capabilities to perform the taxonomy of TCAS threats. Consistent with the high overall risk, APT's capabilities allow completion of all 4 discussed attacks due to their high overall skill-set. Insider threats' capabilities only allow the performance of 2 of the attacks. The attack surface and skill-set of insider threats is only physical aircraft access. Criminal organizations' capabilities allow the performance of 3 of the 4 attacks, with ghosting being the exception. Usually, criminal organizations do not have physical access to the TCAS

	APTs	Insider Threat	Criminal Organizations	Hobbyists
Passive				
Eavesdropping	X	X	X	X
Active				
Ghosting	X	X		
Denial of Service	X		X	
False Injection	X		X	

Figure 8: TCAS Taxonomy of Threats with Threat Actors: Representation of attacks with possible threat actors.

system of an aircraft. Lastly, hobbyists only have the skill-set to passively eavesdrop. The chart highlights the true risk to a TCAS system, and that is an APT followed by insider threats and criminal organizations.

3.3 Current Research

Much of the current research in aviation security focuses on ADS-B security. ADS-B uses Mode S interrogations, replies, and broadcasts [27]. Location data is constantly broadcast by ADS-B, offering tracking capabilities for individuals. Several threat taxonomies exist for ADS-B communications and its message formats. TCAS security is a newly developing aviation arena. There are brief mentions regarding potential security issues for TCAS in several papers focused on ADS-B security. Only two organizations published security-focused research on TCAS. They are a thesis completed by students at Virginia Tech and research papers from individuals associated with Open Sky Network. The research is on a threat overview for the next generation

TCAS system, ACAS X, and TCAS false injection.

3.3.1 ACAS X Threat Overview

Prior research explored possible vulnerabilities for the next generation collision avoidance system, ACAS X [28]. The paper discusses a simulation that analyzes ADS-B data for aircraft tracks that fit the criteria needed for triggering a false RA. The simulation focuses on altitude and the range components of an RA. The paper did not discuss the requirements in detail. That research did not address timing requirements in detail, and it assumed the satisfaction of timing requirements and bearing constraints. Additionally, the research focused on past flights rather than an overall flight risk profile.

3.3.2 False Injection Aircraft on TCAS

In [4], the focus is on falsely injecting an aircraft onto another aircraft. Specifically, the main focus is creating DF-0 replies that include all of the required information. The author creates the messages using the publicly available format for DF-0 messages. The experiment includes GNURadio and SDR for message development and transmission. There are many different assumptions made with the simulation:

- Timing: The simulation assumes an attacker accurately decreases the round trip travel time of replies.
- Range Test: The simulation assumes an attacker satisfies the range test requirements to trigger an RA.
- Bearing Constraints: The simulation assumes the relative aircraft bearing is 0 degrees. The spoofed aircraft and the actual aircraft are facing each other. The author does not explore bearing constraints.

- Stationary Aircraft: The simulation assumes the two aircraft remain stationary during communication.

The simulation is successful in creating DF-0 replies. The next section presents a simulation created to determine the range and bearing constraints. Additionally, the simulation presents timing details of Mode S that allow an attacker to successfully time responses.

3.3.3 Key Vulnerability Takeaways

The key takeaway from the vulnerability analysis is that various impacts of a false injection attack. The false injection attack is the only attack capable of causing pilot distrust and possibly creating a mid-air collision. This dual risk paired with the previous development of Mode S TCAS communications by [4] warrants an understanding of the requirements for a successful false injection and its probability of success.

IV. Viability of False Injection

The possibility of a mid-air collision and/or pilot distrust merit further investigation into a false injection attack. Additionally, the assumptions from the previous study on false injection require investigation to determine the true plausibility of such an attack.

The following chapter presents the methodology and completion of a simulation testing the viability of a false injection attack. The chapter presents the findings for the question: What are the requirements to satisfy the range test, altitude test, and bearing constraints of Traffic Collision Avoidance System (TCAS)? Additionally, this chapter along with the subsequent results chapter answers the question: What conditions allow a ground-based adversary to appropriately time responses and falsely-inject a realistic aircraft into a target aircraft's TCAS, eventually triggering an RA?

The scenario for the simulation is a ground-based adversary paired with SDR type technology, antenna, and other equipment targeting an operation aircraft in the sky. The adversary sends created messages to the targeted aircraft, allowing the insertion of a false aircraft into the air picture. The simulation uses different angle approaches, speeds, distances, and altitudes.

The key players of note in the simulation are:

- Attacker: An individual on the ground with equipment capable of creating, receiving, and sending Mode S messages.
- Target Aircraft: The aircraft that the attacker targets with the created Mode S messages.
- Spoofed Aircraft: The false aircraft created by the Mode S messages sent by the attacker.

4.1 Simulation Software

MATLAB R2019a offers matrix-based mathematics and real-time graphing capabilities [29]. The simulation occurs within MATLAB. MATLAB provides accurate mathematics results regarding necessary timing and positioning. All necessary code implementation transpires within the MATLAB framework. The coding framework begins with the first interrogation and then steps through each subsequent interrogation and reply, while measuring distance, bearing, and required timing of interrogations and replies.

4.2 Assumptions

To conduct the simulation within a reasonable environment and time, the simulation has assumptions. The assumptions include a flat earth, stable terrain/weather conditions, precise Mode-S timing, known aircraft characteristics, and attacker equipment.

4.2.1 Flat Earth

For this model and simulation, the flat-earth model for distance is appropriate; instead of using latitude and longitude, the distance and altitude are converted to x,y,z coordinates. The minimum altitude considered during simulation is 25,000 feet. The altitude of the ground attacker is 10 feet for this measurement. The program uses the following equation to measure the line-of-sight for an object on the ground and an object with an altitude of 25000 feet and radius measured in feet:

$$\begin{aligned} LOS &= \sqrt{\frac{8}{3} * R * Alt1 + (Alt1^2)} + \sqrt{\frac{8}{3} * R * Alt2 + (Alt2^2)} \\ &= 228.218\, miles \end{aligned} \tag{1}$$

The calculated line-of-sight is 228.218 miles. The farthest range implemented in the simulation is 30 miles, 13 percent of the line-of-sight visibility. The implication is that a flat-earth model is valid for distances $\leq$ 30 miles.

Additionally, ADS-B messages from a target aircraft provide the ground attacker with its latitude and longitude [27]. ADS-B messages continually broadcast and contain latitude, longitude, altitude, and bearing information. These messages provide the attacker with another method to determine an accurate range to translate to (x, y, z) coordinates.

Lastly, the ground attacker measures the range of the target aircraft by the time between consecutive interrogations. This measurement provides an accurate distance for the aircraft. The range measurement and bearing provide (x, y, z) coordinates for the target aircraft.

4.2.2 Terrain and Weather

For the simulation, the terrain and weather are clear and do not have an impact. Mountainous terrain presents challenges to accurately timing replies due to the reflection and/or blocking of signals. Additionally, adverse weather limits the visual identification range of pilots. To determine the non-existence of a falsely-injected aircraft and create pilot distrust, the pilot requires clear visibility for identification. For this reason, the simulation assumes open skies, clear weather, and no terrain issues.

4.2.3 Mode S Interrogation and Reply Timing

Mode S replies to interrogations 128 microseconds after the phase sync reversal of the interrogation [30]. Traffic Collision Avoidance System (TCAS) mandates a maximum of 0.1 microsecond jitter. There is not a published study on the accuracy of the interrogation and reply timing. Without a scientific study on the subject,

the simulation uses the TCAS technical mandate of once per second for TAU $\leq$ 60 and every 5 seconds when TAU $>$ 60 and the Mode S mandate of 128 microseconds between the interrogation phase sync reversal and the rising edge of the reply is used and considered accurate. Additionally, TCAS has a jitter of up to $\pm$ 10 % on the 1 and 5 second interrogation timing

4.2.4 Aircraft Speed and Altitude

The simulation includes two aircraft, the target and spoofed aircraft. Both simulated aircraft are the Boeing 737 (B737). The simulated aircraft speed models the cruising speed of the B737. The program assumes that the simulated aircraft maintain cruising speed plus or minus 10 feet per second. Additionally, the program assumes that the aircraft maintain their current cruising altitude plus or minus 700 feet from one interrogation to the next.

4.2.5 Antenna and Transmitter Requirements

TCAS has specific requirements to accept a reply from a responding aircraft. The power profile for TCAS is listed in Table 3 [11, 31].

With the listed parameters, the program assumes the ground station attacker has an antenna with enough power and gain to meet the sensitivity requirements listed of TCAS.

Table 3: TCAS Power Profile

Parameter	Value
Maximum Power	52 dBm
Minimum Power	32 dBm
Sensitivity	-74 dBm
Cable Loss	0 dB
Maximum Antenna Gain	7.5 dBi
Minimum Antenna Gain	0 dBi

4.3 Aircraft Parameters

There are two simulated B737 aircraft. The following two sections discuss the specific parameters and characteristics of each aircraft within the simulation. The sections discuss the cruising speed, cruising altitude, and turning radius of the aircraft.

4.3.1 Target Aircraft

The target aircraft, the victim of the false injection attack, is the B737-800. The B737-800 is the most widely used version of the B737, with over 4000 in active use [32]. Other current versions of the B737 have very similar characteristics. For this simulation, the B737-800 accurately depicts any of the new B737 aircraft from 600 to 900.

4.3.1.1 Aircraft Speed and Altitude

Boeing lists the cruise speed of the B737-800 at 0.789 mach [32]. Equivalently, it is 887.88 feet per second. To ensure variability in aircraft speed from one simulation to the next, the aircraft speed varies plus or minus 10 feet per second.

Additionally, the cruising altitude of the B737-800 is listed at 35,000 feet [32]. This altitude varies based on time of flight, surrounding aircraft, and other characteristics.

4.3.1.2 Turning Capability

The simulated aircraft turns left or right to alter course during the simulation. The speed of the aircraft and the bank angle determines how many degrees the aircraft turns, left or right, in one second. The maximum bank angle without putting the passenger's safety at risk is 25 degrees [33]. With the cruising speed and bank angle known, the standard rate of turn is below:

$$\begin{aligned} Bank\ Angle &= 25\ degrees \\ Velocity &= \frac{887\ ft/s}{1.688} = 525.533\ knots \\ Rate\ of\ Turn &= \frac{1091 * tan(Bank\ Angle)}{Velocity} \\ &= .97\ degrees\ per\ second \end{aligned} \tag{2}$$

1091 is a constant used in the standard rate of turn equation. Using the calculated standard rate of turn, the program allows the target aircraft to turn left or right 1 degree every second. Conversely, the program allows the aircraft to maintain its current bearing and projected path rather than turning left or right.

4.3.2 Spoofed Aircraft

Spoofed aircraft refers to a non-existent aircraft whose location and movement over time signals a collision with the target. The spoofed aircraft has the same capabilities as the target aircraft. The spoofed aircraft mirrors the altitude of the target. Interrogations and ADS-B squitters report altitude. The speed of the spoofed aircraft mirrors that of the target aircraft's speed range. The program is adaptable to other aircraft.

4.4 Aircraft Tracking and Movement

The program uses a 4 quadrant x, y, and z, where z is always greater than or equal to 0. There are also times the program evaluates on a 4 quadrant x and y plane. During the simulations, the target aircraft and spoofed aircraft require their positions to be consistently updated. The program simulates this by using the reported and measured bearings, as well as the speed of the target and spoofed aircraft.

4.4.1 Target Aircraft Positioning, Tracking, and Movement Specifics

The target aircraft starts a certain range from the ground station. As noted in the assumptions, the ground station already knows the target aircraft location due to ADS-B squitters. Further ADS-B squitters give updates to the location and bearing of the target aircraft. For position updating, the program uses the following equations:

$$\begin{aligned} X &= current\ X + (Velo * \Delta t * sin(bearing)) \\ Y &= current\ X + (Velo * \Delta t * cos(bearing)) \\ Z &= reportedaltitude \end{aligned} \tag{3}$$

This updates the (x, y, z) of the aircraft. The altitude adjusts by the change in the reported altitude. The reported altitude remains within plus or minus 700 feet of the originally reported altitude.

4.4.1.1 Relative Bearing Determination

The target aircraft determines the bearing by measuring the angle of arrival of the reply. The angle of arrival measures the horizontal angle and has no vertical component. The reply always comes from the same point, as the ground attacker remains stationary. The most direct point from the ground to the target aircraft

is the angle of arrival for the replies. The program uses the following equation to determine the angle between two points and the angle of arrival for the replies.

$$AOA = MODULO\left(\left(90^\circ - \left(arctan\left(\frac{y_1 - y_2}{x_1 - x_2}\right) * \frac{180}{pi}, 360\right)\right)\right) \tag{4}$$

The ground station remains at (0,0) so the equation reduces to:

$$AOA = MODULO\left(\left(90^\circ - \left(arctan\left(\frac{y_1}{x_1}\right) * \frac{180}{pi}, 360\right)\right)\right) \tag{5}$$

4.4.2 Spoofed Aircraft Positioning, Tracking, and Movement Specifics

The spoofed aircraft positioning updates its position in the program using the same equations as the target aircraft. The first step of the spoofed aircraft is insertion into the air picture. Following insertion, the target aircraft measures the new range/position of the spoofed aircraft based on the interrogation reply timing [11, 34]. Additionally, the target aircraft measures and knows the bearing of the spoofed aircraft based on the angle of arrival of reply.

4.4.2.1 Spoofed Aircraft Insertion

When the ground station sends the first reply, the spoofed aircraft inserts into the air picture of the target aircraft. The spoofed aircraft has the same reported altitude as the target aircraft. Since the spoofed aircraft is placed at the target aircraft's altitude, the additional distance from the ground station to the target aircraft adds to the x and y positioning of the inserted aircraft. The position updates based on the 4 quadrant x and y plane, using the algorithm 1. x_1 and y_1 are the x and y coordinates of the target aircraft. x_2 and y_2 are the coordinates of ground station, (0,0) respectively. Bearing represents the projected bearing of the spoofed aircraft.

The relative bearing of the ground station to the target aircraft determines the bearing. The $distanceDifference$ is the distance from the ground station to the target aircraft minus the distance between the target aircraft and an object at the same altitude as the target aircraft situated at $x = 0$ and $y = 0$. The computation for $distanceDifference$ is:

$$\begin{aligned} D_{GtoT} &= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \\ D_{GtoT-SameAlt} &= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \\ distanceDifference &= D_{GtoT} - D_{GtoT-SameAlt} \end{aligned} \tag{6}$$

Algorithm 1 Spoofed Aircraft Insertion

function MODIFIEDPOSITION($x_1, y_1, x_2, y_2, bearing, distanceDifference$)
  $bearingMod = mod(bearing, 90)$
  if $x_1 > 0\ and\ y_1 > 0$ **then**
    $x = x_2 - distanceDifference * sin(bearing)$
    $y = y_2 - distanceDifference * cos(bearing)$
  else if $x_1 > 0\ and\ y_1 < 0$ **then**
    $x = x_2 - distanceDifference * sin(bearing)$
    $y = y_2 + distanceDifference * cos(bearing)$
  else if $x_1 < 0\ and\ y_1 > 0$ **then**
    $x = x_2 + distanceDifference * sin(bearing)$
    $y = y_2 - distanceDifference * cos(bearing)$
  else if $x_1 < 0\ and\ y_1 < 0$ **then**
    $x = x_2 + distanceDifference * sin(bearing)$
    $y = y_2 + distanceDifference * cos(bearing)$
  else if $x_1 = 0\ and\ y_1 > 0$ **then**
    $y = y_2 - distanceDifference$
  else if $x_1 = 0\ and\ y_1 < 0$ **then**
    $y = y_2 + distanceDifference$
  else if $x_1 > 0\ and\ y_1 = 0$ **then**
    $x = x_2 - distanceDifference$
  else if $x_1 < 0\ and\ y_1 = 0$ **then**
    $x = x_2 + distanceDifference$
  else
    $Target\ Aircraft\ is\ Overhead$
  end if
end function

4.5 Implementation of Required Tests

The following section discusses the implementation of the required tests and limitation checks that occur during the receipt and processing of an interrogation reply. The section discusses the tests and limitations in order of processing. The tests include the received signal power test, the range test, and the altitude test. The bearing constraint check occurs after three received replies. To trigger an RA, these must be satisfied.

4.5.1 Received Signal Power Test

TCAS requires a received signal strength of greater than -74 dBm or -74 milliwatts to accept and process an interrogation reply [31]. The simulation assumes the attacker has an antenna and equipment with enough power and gain to meet the minimum requirement. The TCAS minimum antenna gain is 0 dBi. If the gain is not 0 dBi, TCAS adjusts the required received signal strength by adding or subtract the gain from the -74 dBm requirement. The power and gain chosen for the attacker are 50 dBm and 5 dBi, respectively. The maximum range considered is 30 miles. The altitude difference between the target aircraft and the ground station maximum is 45,000 feet. The maximum range and maximum altitude give a maximum distance of 31.1871 miles. When determining the minimum power received by the target aircraft, the program uses the maximum distance. The program uses the Friis equation [35] to determine the power received by the attacker and if that power meets the specified requirement of -74 dBm. The Friis equation implemented is below with all values in decibels:

$$Rx_P = Tx_P + Tx_G + Rx_G - FSPL \tag{7}$$

Rx_P is receive power and Tx_P is the transmit power. Tx_G is the transmit gain and Rx_G is the receiver gain. FSPL is the free-space path loss. Free space path loss is the amount that a signal disperses over the length of distance that it travels [36]. The equation for free space path loss is:

$$FSPL = 20 * \log_{10}\left(\frac{4 * pi * R}{\lambda}\right) \tag{8}$$

R is the range or distance between the antennas. λ is the wavelength of the signal. The reply sends at 1090 MHz. Wavelength is the speed of light (c) divided by the frequency of the signal in hertz. The FSPL equation further expands to the equation below:

$$FSPL = 20 * \log_{10}\left(\frac{4 * pi * R * f}{c}\right) \tag{9}$$

Using the frequency and furthest distance in the simulation, the FSPL is:

$$\begin{aligned} FSPL &= 20 * \log_{10}\left(\frac{4 * pi * 31.1871\, miles * 1090 MHz}{c}\right) \\ &= 127.2\, dBm \end{aligned} \tag{10}$$

With the path loss known, Rx_P is below.

$$\begin{aligned} Rx_P &= Tx_P + Tx_G + Rx_G - FSPL \\ &= 50 + 5 + 0 - 127.2 \\ &= -72.2\, dBm \end{aligned} \tag{11}$$

The lowest power that is received is -72.2 dBm. It is higher than the required sensitivity of -74 dBm. These settings always satisfy the received power test, so this test is complete.

4.5.2 Bearing Constraints

The bearing error constraint of TCAS is plus or minus 10 degrees from the estimated bearing [11, 37]. If a bearing measurement exceeds the bearing error constraint, the track possibly coasts or drops. TCAS takes the first three bearing readings and averages them together. TCAS creates a projected path for the tracked aircraft by using the bearing average.

The program takes the first three bearing measurements and averages them together using the following equation:

$$Bearing\ Average = \frac{1st\ Bearing + 2nd\ Bearing + 3rd\ Bearing}{3} \tag{12}$$

With the bearing average, the program establishes a projected path for the spoofed aircraft. Since the spoofed aircraft signals come from the ground station, the spoofed aircraft bearing changes from one reply to the next. If the bearing change exceeds the projected bearing by more than plus or minus 5 degrees from the projected bearing, the program terminates with an error. The simulation uses plus or minus 5 degrees, rather than 10 degrees since TCAS's bearing estimate has a standard deviation of 5 degrees [11]. Additionally, if the target aircraft turns left or right, the program adds the bearing change to the bearing average. This accounts for the target aircraft movements and the effect on the reported bearings from the spoofed aircraft.

4.5.3 Range Test

There are two requirements with the range test [11]. They are the TAU calculation and the diverging requirement.

4.5.3.1 Diverging Requirement

To successfully satisfy the range test and not have the aircraft track potentially dropped, the spoofed aircraft must not diverge from the target aircraft. The simulation program measures this requirement by calculating the range rate using the equation below [38]:

$$Range\ Rate = Spoofed\,Velocity * cos(\theta_1) + Target\,Velocity * cos(\theta_2) \tag{13}$$

θ_1 is the measured angle between the spoofed aircraft's heading and the closing vector between the spoofed aircraft and target aircraft. Since the spoofed aircraft's signal is coming from a stationary object with an omnidirectional antenna, the heading and closing vectors are equivalent. Therefore, θ_1 will remain 0 at all times. θ_2 is the measured angle between the target aircraft's heading and the closing vector between the target aircraft and the spoofed aircraft. θ_2 continuously changes from each reply to the next. Figure 9 provides a visual for the scenario described above. The calculation for θ_2 is below:

$$Bearing\ Difference = |180 - Target\ Heading + Spoofed\ Heading| \tag{14}$$

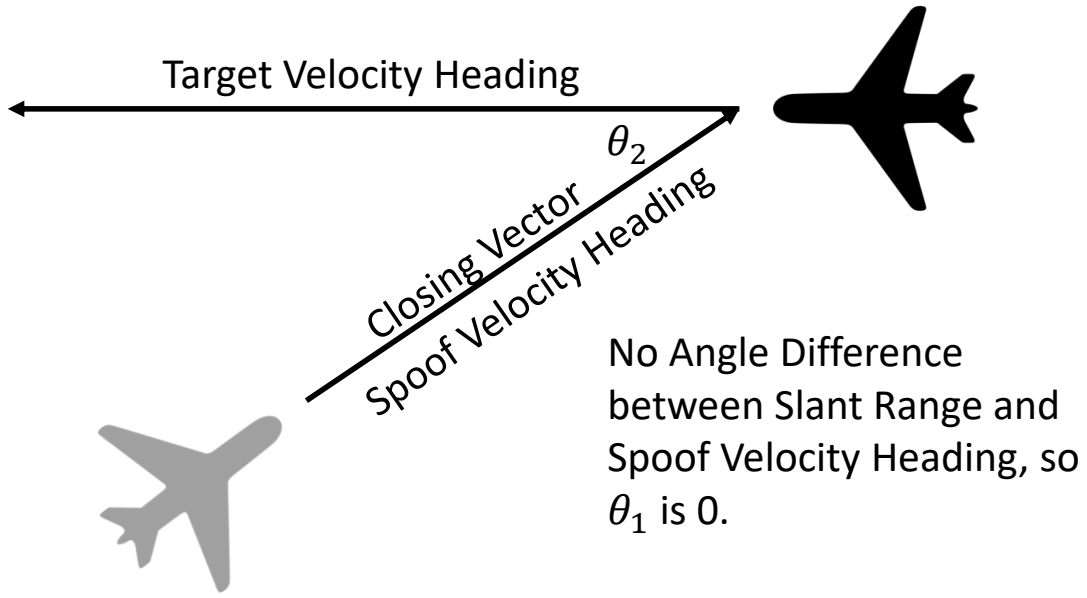

Figure 9: Closing vector: A visual to show the angles between the spoofed and target aircraft headings.

With θ_1 and θ_2, the range rate equation is as follows:

$$\begin{aligned} Range\ Rate = Spoof\ Velo * cos(0) + Target\ Velo * cos \\ (|180 - Target\ Heading + Spoofed\ AC\ Heading|) \\ = Spoof\ Velo + Target\ Velo * cos \\ (|180 - Target\ Heading + SpoofAC\ Heading|) \end{aligned} \tag{15}$$

The range rate calculation compares to 0. If the range rate is 0 or positive, the program maintains the target and spoofed aircraft as converging. The target aircraft continues to maintain the track of the spoofed aircraft since the aircraft remain converging. Contrarily, if the range rate is negative, the aircraft are diverging or separating. Diverging aircraft cannot have a RA reported [31]. Additionally, a diverging aircraft track possibly drops from the target aircraft's TCAS system.

4.5.3.2 TAU Calculation

As previously discussed, TAU is the measurement that determines when a TA or RA is necessary from a horizontal aspect. TAU gives the number of seconds until the impact or closest point of approach. The programs uses the following equation to calculate TAU with each reply [11, 39]:

$$TAU = \frac{r - \frac{SMOD^2}{r}}{rdot} * 3600 \tag{16}$$

r is the range between the target and the spoofed aircraft. SMOD is listed as a "distance surveillance modifier," and it is equivalent to 3 NMI [11]. Rdot is the range rate. The denominator in the equation below determines the range rate. Using range

rate and the SMOD modifier, the TAU calculation in the program is below:

$$TAU = \frac{r - \frac{SMOD^2}{r}}{rdot} * 3600$$
$$= \frac{r - \frac{9}{r} * (3600)}{Spoof\ Velo + Target\ Velo * cos(|180 - Target\ Heading + Spoof\ Heading|)} \quad (17)$$

The program compares the TAU calculation to the mandated TAU value of 35 seconds. If TAU is less than the 35 second threshold, the ground attacker successfully meets the range requirement, allowing the trigger of an RA. If TAU is greater than the 35 second threshold, the process of Uplink Format (UF) and Downlink Format (DF) 0 interrogations and replies continue.

4.5.4 Altitude Test

The altitude test compares the altitude of the target aircraft and the spoofed aircraft. If the altitude comparison has an altitude difference of less than or equal to 700 feet, the spoofed aircraft meets the altitude requirement for an RA.

The program copies the altitude of the target aircraft into the altitude field of the spoofed aircraft reply. If the altitude changes from one interrogation to the next, the altitude adjusts to match the target aircraft's altitude. This ensures the altitude test maintains a true and satisfied reading. With the altitude test always satisfied, the attacker only needs to focus on the range test, power test, and bearing constraints.

4.6 TCAS Interrogations and Reply Timing Implementation

The program uses 2 TCAS interrogation and reply types: All-Call interrogations and replies and Short TCAS interrogations and replies. Short TCAS interrogations are the same as UF-0 interrogations and DF-0 replies. An all-call interrogation is the

first interrogation received during the establishment of a track in the program. An all-call reply follows the interrogation. All following communications are short TCAS interrogations and replies.

4.6.1 All-Call Interrogations/Replies

The All-Call interrogation is the first interrogation received by the ground station attacker. The program uses the speed of light to determine the arrival time of the interrogation to the ground. The following equation represents the calculation of arrival time:

$$Arrival\ From\ Target = PulseTime + \frac{Bits}{BPS} + \frac{D}{c} \tag{18}$$

D is the distance between the target and the ground station. c is the standard speed that RF signals travel at, the speed of light. $PulseTime$ is the additional time needed to send P_1, P_2, and the rest of P_6. Figure 10 shows a Mode S interrogation timing layout [11]. The standard for UF-11 and UF-0 interrogations is 56 bits [30].

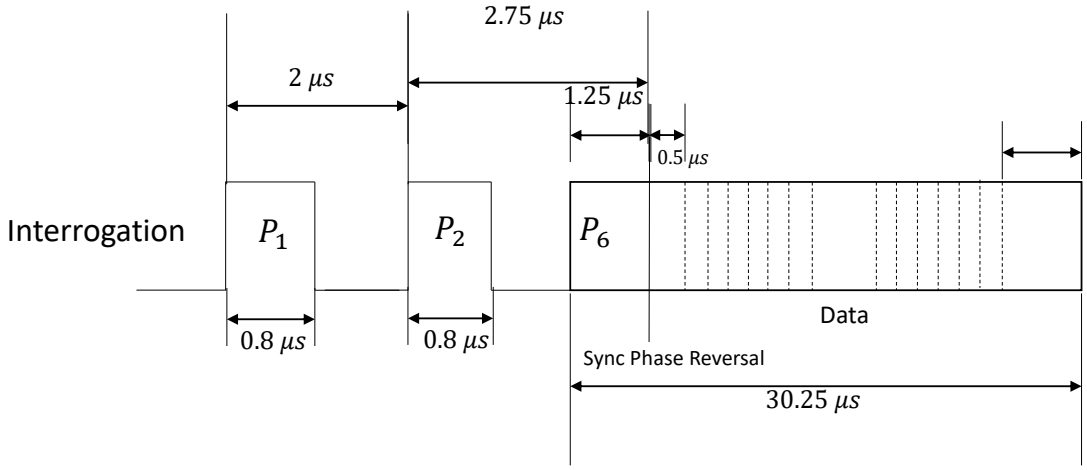

Figure 10: Mode S Interrogation Format: Layout and timing for Mode S interrogations [30].

The bits send during the P_6 pulse. Additionally, the transmission rate for Mode S interrogations is 4 Mbps [34]. Using those, the equation further reduces to:

$$\begin{aligned} Arrival\ From\ Target &= 5.75\mu s + \frac{56\ bits}{\text{4e-6}\ bps} + \frac{D}{c} \\ &= 5.75\text{e-}6s + 14\text{e-}6s + \frac{D}{c} \\ &= 19.75\text{e-}6s + \frac{D}{c} \end{aligned} \tag{19}$$

Mode S requires systems to wait 128 microseconds from the phase sync reversal of an interrogation until the rising edge of the replies first pulse [30]. There are 4.75 microseconds from the first pulse of the interrogation to the phase sync reversal of the interrogation [30]. This gives a total of 132.75 microseconds from interrogation received to first pulse of reply. Figure 11 illustrates the timing of a Mode S reply. The ground station sends the all-call reply after the mandated 132.75 microsecond data processing period. The reply arrives to the target aircraft using the following equation:

$$Arrival\ To\ Target = Preamble + \text{132.75e-}s + \frac{bits}{bps} + \frac{New\ D}{c} \tag{20}$$

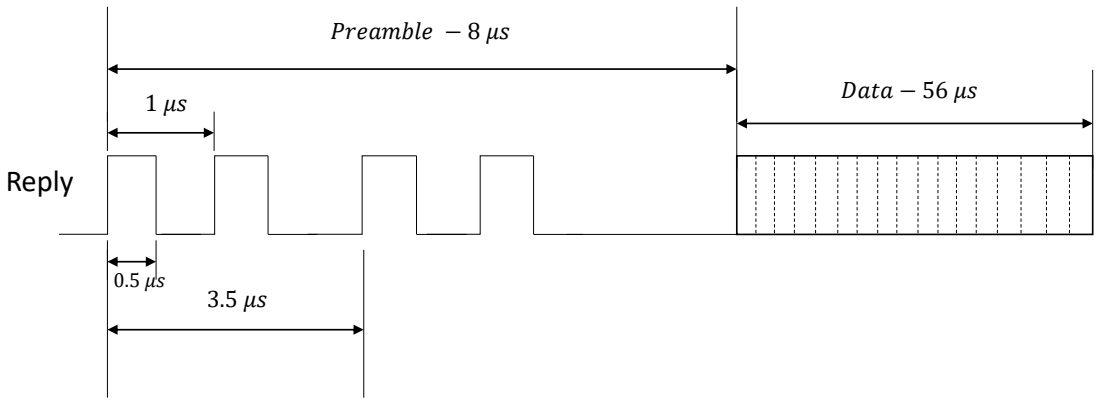

Figure 11: Mode S Reply Format: Layout and timing for Mode S replies [30].

All-Call replies have 56 bits in the reply. The reply bit rate is 1 Mbps [11]. $NewD$ is the new distance since receiving the interrogation. c remains the speed of light. $Preamble$ is the time before the bits process. For replies, it is $8\mu s$ [30]. The reply from ground station equation updates to:

$$\begin{aligned} Arrival\,To\,Target &= \text{8e-6}s + \text{132.75e-6}s + \frac{56\,bits}{\text{10e6}\,bps} + \frac{New\ D}{c} \\ &= 196.75E-6s + \frac{New\ D}{c} \end{aligned} \tag{21}$$

This formula gives the program the arrival time of the reply to the target aircraft.

4.6.2 Short TCAS Interrogations/Replies

Once the All-Call interrogation and reply complete, the simulation begins the short TCAS interrogation and reply sequence. The equations from the all-call interrogations remain implemented for short TCAS interrogation. The timing of short TCAS interrogations depends on the TAU calculation of an interrogation reply. If TAU is greater than 60, then TCAS and the program interrogates every 5 seconds. If TAU is less than or equal to 60, then the program interrogates every 1 second. The jitter is plus or minus 10 percent from the time values. Table 4 lists the program's range for short TCAS interrogation timing: All-Call and short TCAS interrogations/replies have the same transmission rate and bit length. The most important simulation aspect of short TCAS interrogations/replies is the difference between the arrival of the interrogation to the ground attacker and the spoofed aircraft location. Additionally,

Table 4: Jitter Timing Ranges

TAU	Timing	Jitter	Timing Range
TAU $>$ 60	5s	$\pm$ 10%	4.5s-5.5s
TAU $\leq$ 60	1s	$\pm$ 10%	0.9s-1.1s

the time of reply from the ground station adjusts to account for the difference in location of the ground station and spoofed aircraft. The 132 microsecond delay between a received interrogation and expected reply allows the simulated attacker a window to send the reply early. The equation below determines when the reply must send to correctly position the spoofed aircraft:

$$Needed\ Reply\ Time = ATG + 0.00013275s - (Time\ Diff) - (DG/c) \tag{22}$$

ATG is the arrival time to ground. Arrival time to ground is the time the interrogation arrives at the ground station. $132.75\mu s$ is the delay between a Mode S interrogation and reply. $TimeDiff$ is the difference between when the interrogation arrives at the ground and when it arrives at the spoofed aircraft location. DG is the distance the spoofed aircraft gains during the interrogation travel time and the $132.75\mu s$ expected delay. That is divided by the speed of light to determine the time added to the reply time.

4.7 Program Details and Parameters

The program runs a set of 500 simulations with the same parameters. Testing revealed the statistical difference was non-existent when using 1000 and 2000 simulations from 500 simulations. After the set of 500 simulations completes, the starting relative bearing from the target aircraft to the ground station changes. After 37 sets with different starting bearings, the altitude, range, or altitude and range change. In total, there are 92,500 simulations run at each range with different altitudes. There are 111,000 simulations run at each altitude with differing ranges. The following subsections discuss the details of the parameters

4.7.1 Range

The starting range for the target aircraft changes throughout the sets of simulations. The ranges used by the program are 30 miles, 25 miles, 20 miles, 15 miles, 10 miles, and 5 miles. 30 miles is the max range considered, as the maximum distance of TCAS is 35 miles [40].

4.7.2 Altitude

The starting altitude for the target aircraft changes throughout the sets of simulations. The program uses altitudes of 45,000 feet, 40,000 feet, 35,000 feet, 30,000 feet, and 25,000 feet. This includes the most common cruising altitude of aircraft, 35,000 feet [32].

4.7.3 Starting Relative Bearing

The starting relative bearing of the target aircraft changes after each set of 500 simulations. The starting relative bearing from the target to the ground station starts at 90 degrees. After each set of 500, it lowers by 5 degrees. Once at 0 degrees, it then lowers to 355 degrees on the next set. The 5 degree decrease occurs 37 times and ends at 270 degrees relative bearing. The range is [90-0] and [355-270]. This range of relative bearings lies within the visual identification window of the pilot. This is important to ensure the pilot maintains the capability to verify the spoofed aircraft doesn't exist. Algorithm 2 shows the process for conducting all trials.

Algorithm 2 Program Simulations

```
1: altitude = 25,000ft
2: range = 5m
3: while altitude ≤ 45,000ft do
4:     while range ≤ 30m do
5:         while relativeBearing ≤ 90||relativeBearing ≥ 270 do
6:             Run 500 simulations
7:             relativeBearing = mod(relativeBearing − 5, 360)
8:         end while
9:         range = range + 5m
10:        relativeBearing = 90
11:    end while
12:    altitude = altitude + 5000ft
13:    range = 5m
14: end while
```

4.8 Validation and Verification

This section presents simulations that test the program's capability to correctly end tracking when tests or constraints are exceeded. Additionally, this section verifies and validates the program's ability to accurately track aircraft, update their position, and measure the distance between them.

4.8.1 Positioning and Tracking

The program simulates with a starting distance of 30 miles and 45,000 feet. The (x, y, z) coordinates are (112005.71414, 112005.71414, 45000). The exact starting position is arbitrary but produces the same value from other positions. The starting bearing is 270 degrees. The initial reply arrives with the spoofed aircraft inserted with a bearing of approximately 45 degrees, as expected. After a 5.416566 second interrogation period, including jitter, the target aircraft turned left 1 degree. That interrogation period is due to a TAU of greater than 60 and the time for the interrogation to arrive. The total time at this point is 5.417301 seconds. The aircraft spends 0.000735 seconds with a bearing of 270 and 5.416566 with a bearing of 269. With the

```
Next interrogation begins sending from Target Aircraft at 5.417117e+00 seconds.
 Target Aircraft is 1.613490e+05 feet from Ground Attacker
```

Figure 12: Positioning and Tracking Verification: Printout from simulation detailing timing and distance data.

original 0.000735s, mathematically, the position updates to:

$$\begin{aligned} x &= 112005.71414 + (888 ft/s * 0.000735s * sin(270)) \\ &= 112005.06146 \\ y &= 112005.71414 + (888 ft/s * 0.000735s * cos(270)) \\ &= 112005.71414 \end{aligned} \tag{23}$$

Next, the 5.416566 seconds of a bearing of 269 degrees updates the position:

$$\begin{aligned} x &= 112005.06146 + (888 ft/s * 5.416566s * sin(269)) \\ &= 107195.8834 \\ y &= 112005.06146 + (888 ft/s * 5.416566s * cos(269)) \\ &= 111921.7696 \end{aligned} \tag{24}$$

Using the new (x, y, z) coordinates the the distance between target aircraft and the ground station is computed:

$$\begin{aligned} distance &= \sqrt{(107195.8834 - 0)^2 + (111921.7696 - 0)^2 + (45000 - 100)^2} \\ &= 161348\ feet \end{aligned} \tag{25}$$

The program code produced the same value, shown in Figure 12. This shows the program accurately tracks and updates aircraft positioning based on speed, time, and bearing.

```
Interrogation will arrive to Where False Aircraft should be positioned at 1.566139e+01 seconds.
    New Bearing of False Aircraft is 3.705223e+01 degrees.
```

Figure 13: Bearing Constraint Failure: Printout from simulation showing bearing failure when appropriate.

4.8.2 Bearing Constraint

The bearing constraint verification and validation test uses the same simulation parameters from the positioning and tracking test. The program illustrates its accuracy in tracking aircraft, updating position, and measuring bearing. The bearing measurements are accurate. The verification and validation of the bearing constraint ensures the program stops when a bearing reporting exceeds $\pm$ 5 degrees from the average of the first three bearing reports. The first bearing is 44.9999 degrees. The second bearing is 42.4739 degrees. The third bearing reporting is 39.8848. The average of the bearings is 42.4529. The next reported bearing is 37.05223. It exceeds the bearing constraint of $\pm$ 5 degrees. As shown in Figure 13, the bearing exceeds the constraint.

4.8.3 Range Test Failure

Using the same (x, y, z) as the previous simulations, the verification and validation of the range test occurs. The bearing changes to 45 degrees, so the target aircraft moves away from the ground station. The test sets the target aircraft speed greater than the spoofed aircraft. After the third reply, the next reply must not have a range rate of less than 10 ft/s. The target aircraft moves away at a faster rate than the

```
 Spoofed Aircraft is 1.646746e+05 feet from TargetAircraft
Aircraft are diverging and range test fails
```

Figure 14: Diverging Simulation Failure: The code readout after two aircraft are diverging.

spoofed aircraft, so it is diverging. Figure 14 illustrates the program terminating due to diverging aircraft.

V. Results and Analysis

5.1 Requirements for Success

This section presents the requirements for simulation success. Altitude is not included as a requirement for success, as the attacker's altitude reflects that of the target. The spoofed aircraft maintains an altitude that successfully meets the altitude test throughout each simulation.

5.1.1 Interrogation and Reply Requirements

Bearing and TAU measurements are necessary for false injection capabilities. For bearing and TAU calculations to occur, Traffic Collision Avoidance System (TCAS) requires 3 rounds of interrogation and replies. Those 3 rounds provide a bearing estimation for comparison. After 3 interrogation and reply rounds, with the next interrogation and reply cycle, the target aircraft calculates the TAU and bearing for RA determination. Thus, for success, the simulation must not fail on or before the fourth interrogation cycle.

5.1.2 Range Requirements

The two success requirements of the range test in the simulation are the diverging test and the TAU calculation. If at any point the spoofed aircraft and the target aircraft have a range closure rate of less than 10 feet per second, the simulation terminates. Additionally, the simulation is successful if TAU is less than 35 seconds. After 3 interrogation and reply sequences, if TAU is under 35s, the simulation is successful.

5.1.3 Bearing Requirements

The simulation is successful if the spoofed aircraft bearing change is less than 5 degrees from the projected bearing path. If a bearing change over 5 degrees occurs, the simulation terminates. If TAU is not below 35 seconds when the termination occurs, the simulation is not successful. Table 5 displays the truth table for simulation success at the end of the simulation.

5.2 General Results and Analysis

As noted from the above subsections, whenever TAU ($\leq$ 35s) is true, the simulation is successful. This section discusses the initial results of the simulations including flight paths and TAU averages.

5.2.1 Flight Paths

Flight paths differ from each simulation to the next. The flight path is randomly chosen from one simulation to the next. The aircraft turn left, turn right, or maintain close to their starting bearing from each simulation.

5.2.2 TAU Average

Each simulation calculates the final TAU value upon its termination. The program writes the TAU value for each of the 500 simulations in a set. The average of the ending TAU values is taken for each set and measured against the 35 second threshold. The sets with an average TAU value less than or equal to 35 seconds is successful. The overall success of the 555,000 trials is 32.6305%. For further analysis, the most useful variables in displaying simulation success are range and starting relative bearing. Figure 15 displays the TAU averages. The x-axis is the starting relative bearing between the target aircraft and the ground station. Each set of 5 lines represents

a different starting range. The different colors represent different altitudes at each range. Table 6 discusses the altitude scheme for Figure 15. In Figure 15, the horizontal black line indicates the TAU threshold of 35 seconds. Where an individual line goes below the threshold indicates a starting relative bearing, altitude, and range that successfully satisfies all required TCAS tests over 50 percent of the simulations.

Table 5: Figure 15 Color Legend

Altitude	Color
45,000 ft	Black
40,000 ft	Yellow
35,000 ft	Green
30,000 ft	Red
25,000 ft	Blue

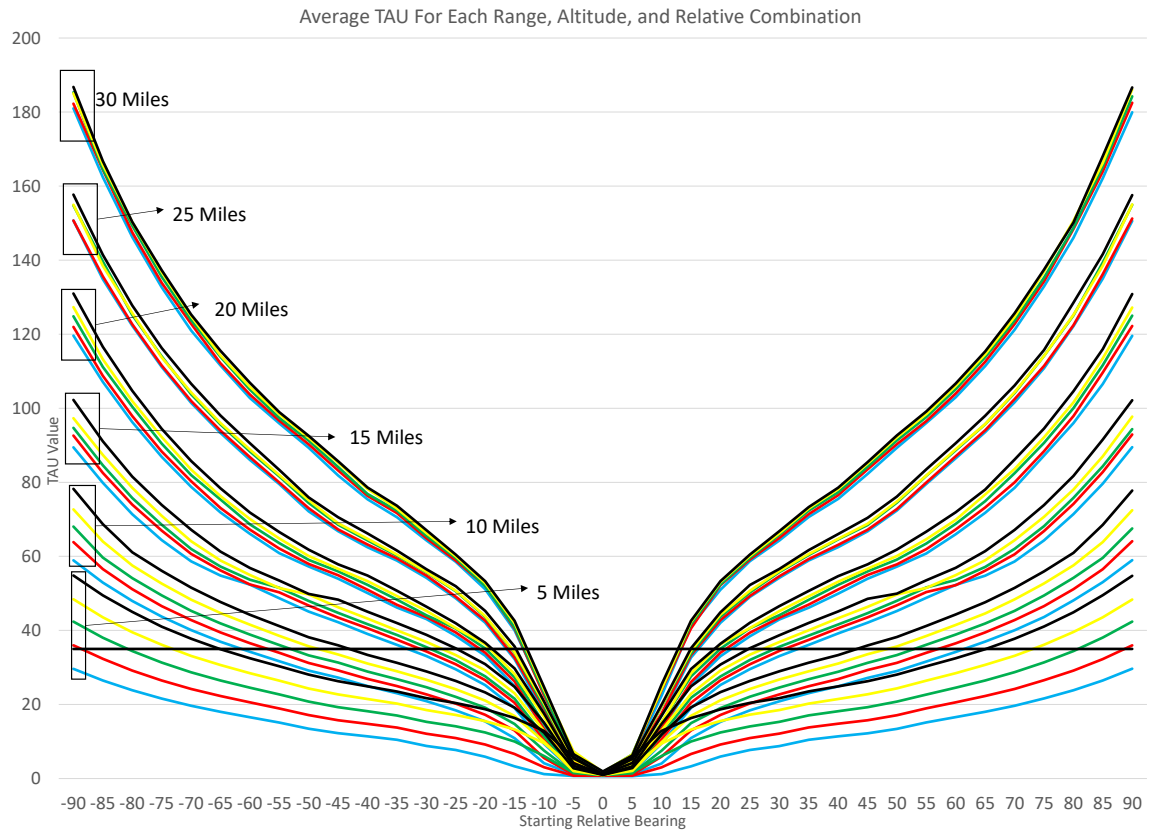

Figure 15: First-Look Tau Values: Each line represents a different range and altitude pair. The lines represents the TAU value as relative bearing increases and decreases.

Most TAU values fall above the maximum 35 second TAU threshold, as evident by the chart. TAU decreases and success increases as altitude and range lowers.

5.3 In-Depth Analysis

The previous section focused on a statistical average TAU calculation with a hard comparison against the TAU limit. The following section looks at the in-depth statistical values of each set of 500 simulations. The section overviews the skewness, kurtosis, standard deviation, and percentage of success for each altitude, range, and starting relative bearing combination.

5.3.1 Skewness

Skewness is the representation of the asymmetry within a data set [41]. A perfectly symmetric data distribution, normally distributed, has a skewness value of 0. If the skewness value is negative, the data distributes more to the left of the mean. Additionally, the tail of the left side is longer than the right side. In contrast, if the skewness value is positive, the data distributes more to the right of the mean and the right tail is longer. Figure 16 provides a visual for negative, positive, and zero value skewness distribution curves. West [42] set the skewness guidelines for normally distributed data as 0 ± 2.1. The equation for skewness is:

$$Skewness = \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^3}{N}}{\sigma^3} \tag{26}$$

To accommodate for the sample size and provide better a understanding of the data skewness, the equation is:

$$Skewness = \frac{\sqrt{N * (N-1)}}{N-2} \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^3}{N}}{\sigma^3} \tag{27}$$

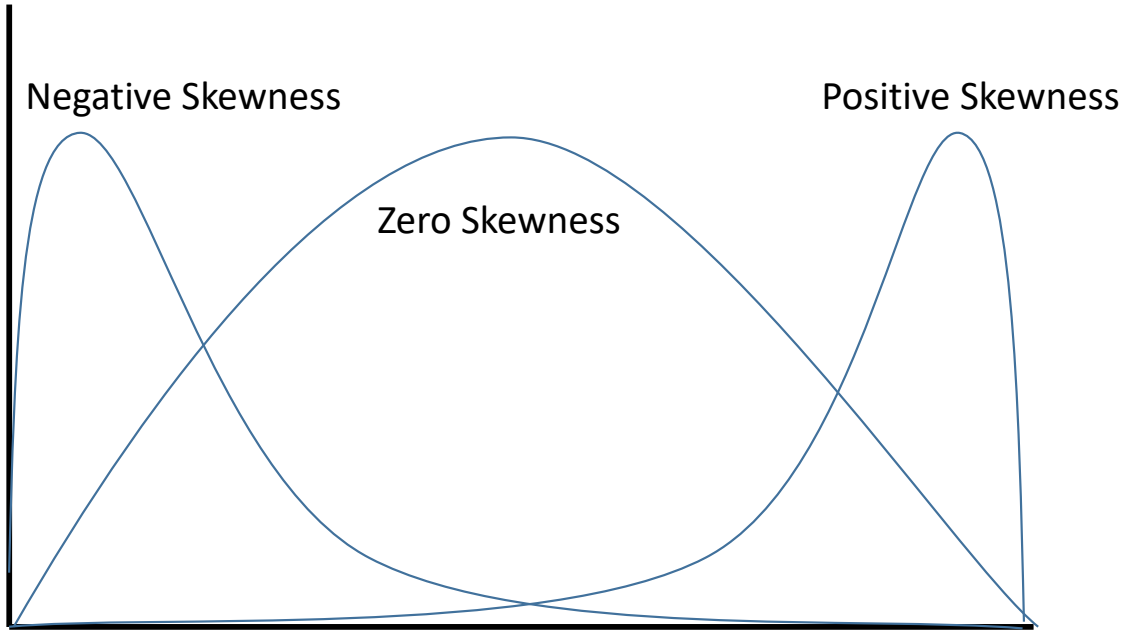

Figure 16: Positive, Negative, and Zero Skewness graphical representations [41].

Detailed analysis provides the skewness value for each set of 500 simulations. Figure 17 shows all skewness values with the thresholds of -2.1 and 2.1. There are 28 data sets over the skewness limits.

5.3.2 Kurtosis

Kurtosis is the fourth sample moment about the mean, and regarding shape, it describes if data is heavy-tailed or light-tailed compared to an even normal distribution [43]. A kurtosis value of greater than 3 represents leptokurtic data. This implies that the distribution tails are heavy compared to normal distribution. A kurtosis value of less than 3 represents playtkurtic data. This implies that the distribution tails are thinner compared to a normal distribution curve. The kurtosis value for normal distribution is 3 and known as mesokurtic. Figure 18 provides a visual for playtkurtic, leptokurtic, and mesokurtic distribution. The following equation calculates the kurtosis of data:

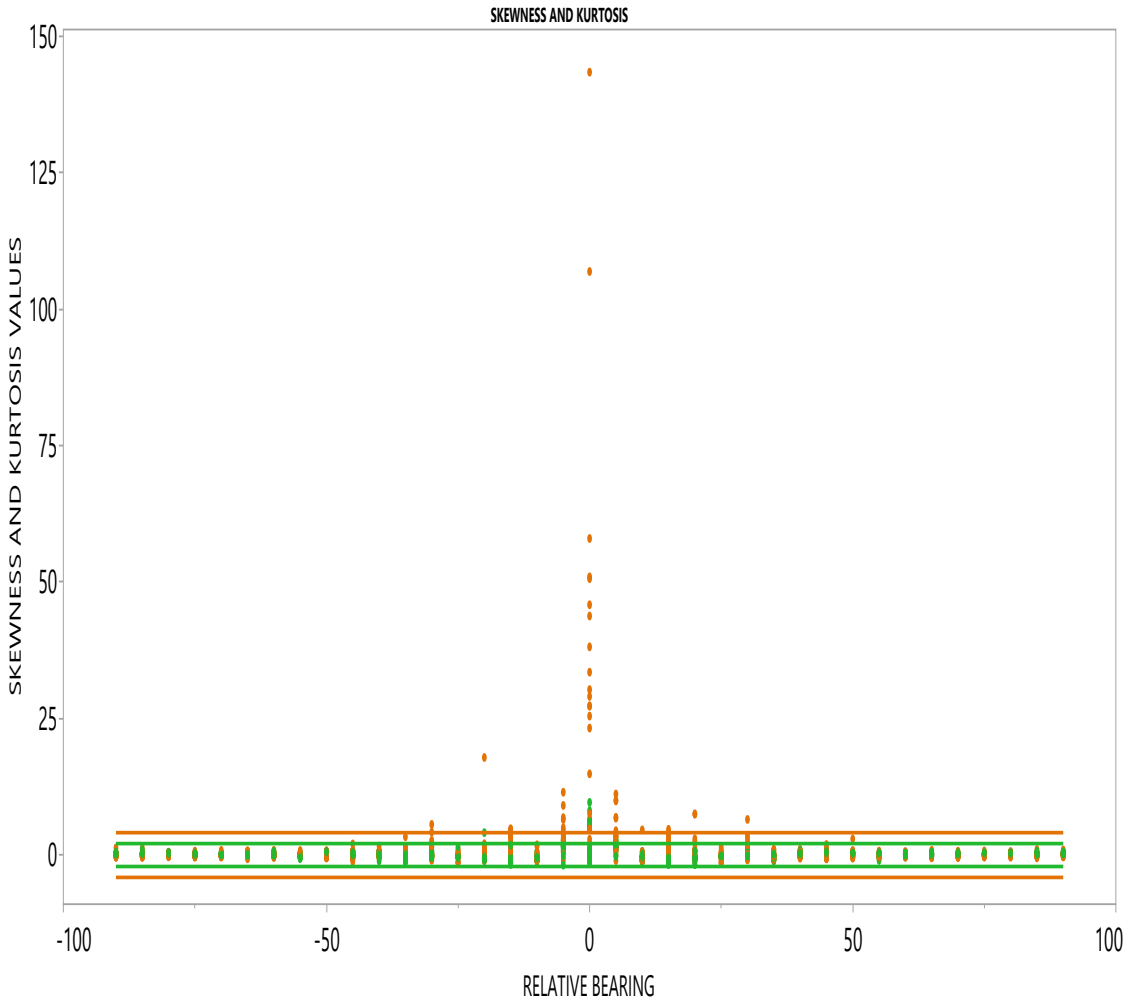

Figure 17: Original Kurtosis and Skewness Values: Orange represents kurtosis values and green represents skewness values.

$$Kurtosis = \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^4}{N}}{\sigma^4} \tag{28}$$

In data that has occasional data outliers, excess kurtosis is the standard measurement. The excess kurtosis value for normal distribution is 0 [44]. Leptokurtic is then all positive values and playtkurtic is all negative values. Additionally, the analysis accomodates for sample size, so the excess kurtosis equation is:

$$Kurtosis = \frac{N(N+1)}{(N-1)(N-2)(N-3)} \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^4}{N}}{\sigma^4} - \frac{3(N-1)^2}{(N-2)(N-3)} \tag{29}$$

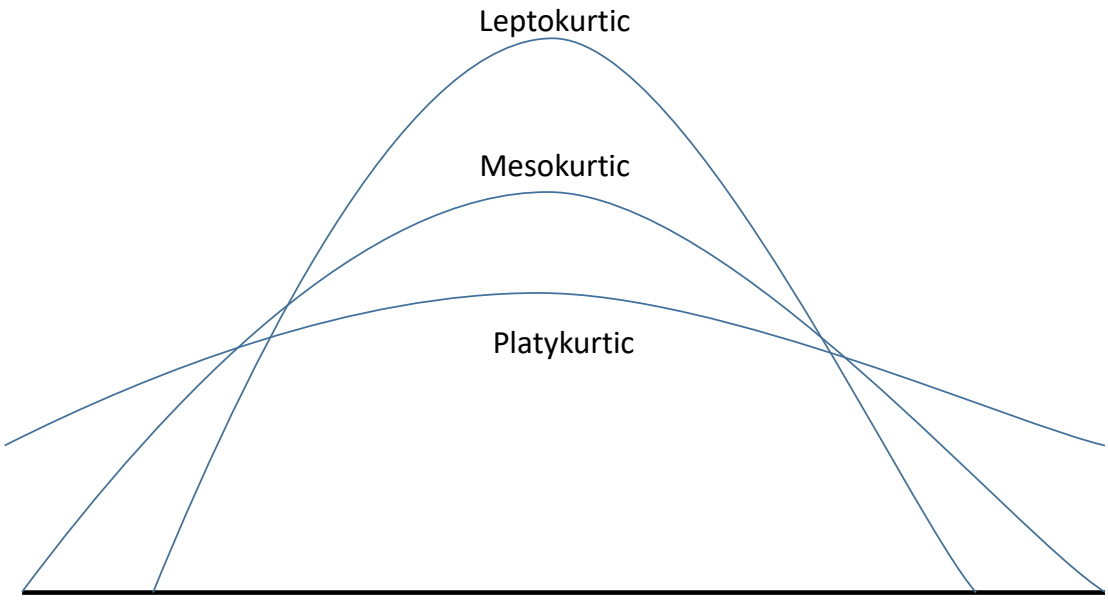

Figure 18: Visual Kurtosis Representations: Leptokurtic, Mesokurtic, and Platykurtic kurtosis graphical representations [43].

West [42] set the kurtosis guidelines for normally distributed data as 3 ± 4.1. That range is for proper kurtosis. The range for excess kurtosis is 0 ± 4.1. The kurtosis value for each set of 500 simulations is measured. Figure 17 shows all computed kurtosis values and the normal distribution thresholds of -4.1 and 4.1. There are 42 simulations with kurtosis values that exceed the threshold. Those data sets require manipulation.

5.3.3 Box Cox Transformation

Sets of data that have kurtosis or skewness values that exceed recommended thresholds require transformation. [45] recommends using the Box-Cox transformation as it provides multiple transformation options for data, choosing the option that best transforms your data from non-normal to normal distribution. [45] provides the

equation used to transform each data point:

$$Box - Cox\,Transform = \frac{x^{\lambda} - 1}{\lambda} \tag{30}$$

λ is determined by testing various values for λ in the equation with each data point [45]. The λ value chosen is the one that provides the skewness and kurtosis values closest to 0, as they are the most normally distributed. Different λ values provided different transformations, such as $\lambda = 0.5$ gives the following transformation for each value:

$$\begin{aligned} Box - Cox\,Transform &= \frac{x^{0.5} - 1}{0.5} \\ &= \frac{x^{0.5}}{2} - 2 \end{aligned} \tag{31}$$

This is considered a square root transformation [45]; whereas, other λ values give other types of transformations.

This Box-Cox transformation is applied to data sets of 500 that do not adhere to the skewness and kurtosis values. After the Box-Cox transformation, all outlier data sets transform to sets that meet normality considerations. Figure 19 is the new graph with all transformed data sets.

5.3.4 Standard Deviation Analysis

Normally distributed data sets present probability analysis capabilities. The key statistics used from each data set are the mean and standard deviation. Additionally, the target TAU value is ≤ 35 seconds. The following equation uses the mean, standard deviation, and X value (TAU) to calculate a z-score.

$$Z = \frac{X - \mu}{\sigma} \tag{32}$$

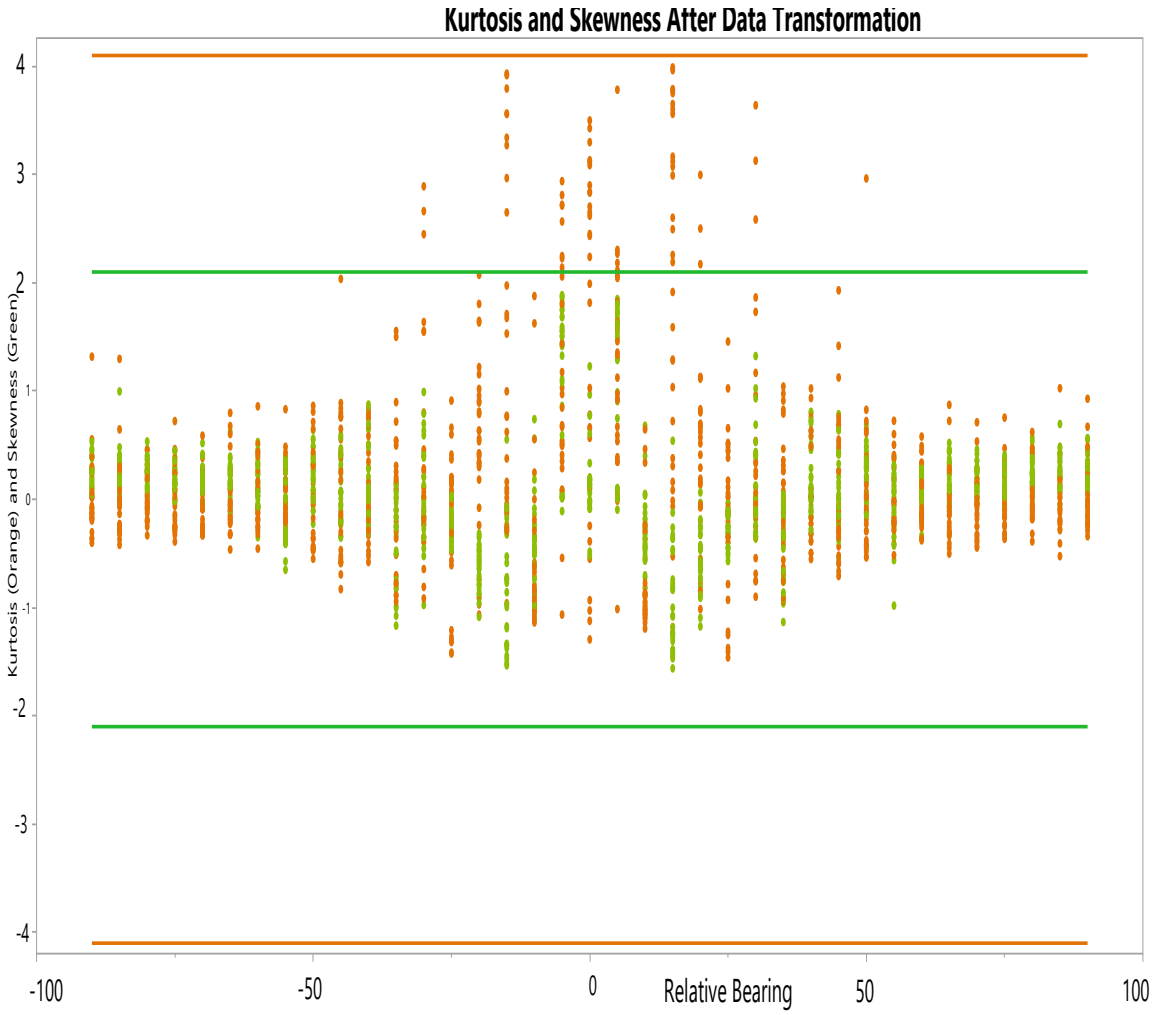

Figure 19: Kurtosis and Skewness After Data Transformation: Orange represents kurtosis values and green represents skewness values.

This Z-score represents the probability that TAU is $\leq$ 35 seconds. The equation is further clarified to:

$$P(TAU \leq 35) = \frac{35 - \mu}{\sigma} \tag{33}$$

The Z-score calculated compares to a Z-table that list the appropriate probability for the Z-score. They give an accurate depiction of successful false injection probabilities from a certain distance, altitude, and relative bearing.

5.3.5 Threat Map

The false injection probabilities allow the creation of an accurate threat map for potential aircraft. The color and percentage legend for the threat maps is:

- Highly Possible (Probability of Success $\geq$ 70%) - Red areas represent ranges and relative bearings that false injection attacks are highly successful.
- Moderately Possible(40% $\geq$ Probability of Success $<$ 70%) - Yellow areas represent ranges and relative bearings that false injection attacks are moderately successful.
- Not Likely Possible (Probability of Success $\leq$ 40%) - Green areas represent ranges and relative bearings that false injection attacks are likely to be unsuccessful.

Figures 20-24 represent the threat maps for aircraft. Each figure is a threat map for each different simulated altitude. Aircraft that appear and maintain a track in green areas of the threat map project as real aircraft. Conversely, aircraft that appear and maintain a track within red areas cannot be validated as real or falsely injected until visual identification occurs.

The figures provide pilots with an accurate understanding of the distances, altitudes, and relative bearings vulnerable to a false injection attack. In the event of a TCAS anomaly in flight, the maps provide the pilot an extra tool in the determination between system failure due to outside influence or just mechanical system failure. Also, the maps show that a false injection is quite possible in certain circumstances. This show of success requires specific attention to possible solutions for this particular attack and possibly other attacks mentioned in the threat taxonomy.

One major note from the maps is that a 0 degree relative bearing from the target aircraft to the ground-based attacker presents the perfect scenario for false injection.

As long as the attacker times the Mode S responses correctly, false injection attacks are always successful with a 0 degree relative bearing.

Additionally, another major note is that the closer an attacker is horizontally to the target aircraft, the more successful the false injection attack is. Since the aircraft is closer, the TAU calculation always falls within the window of RA issuance, ≤ 35 seconds.

The last major takeaway from the maps is the increase in success of attack at lower altitudes. As the altitude decreases, the success of false injection attacks broadens across different relative bearings. The occurs due to the reduction in distance and therefore a decrease in the TAU calculation.

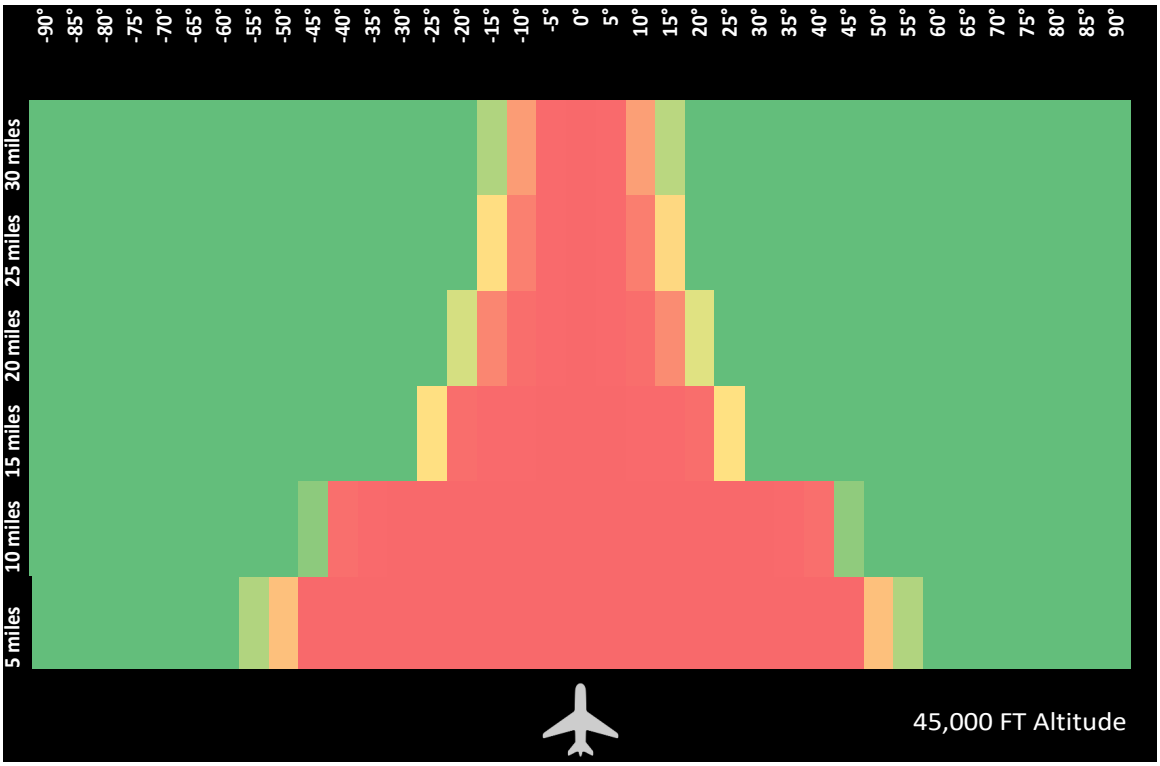

Figure 20: 45,000 feet Threat Map: Threat map for ranges and relative bearings at 45,000 feet.

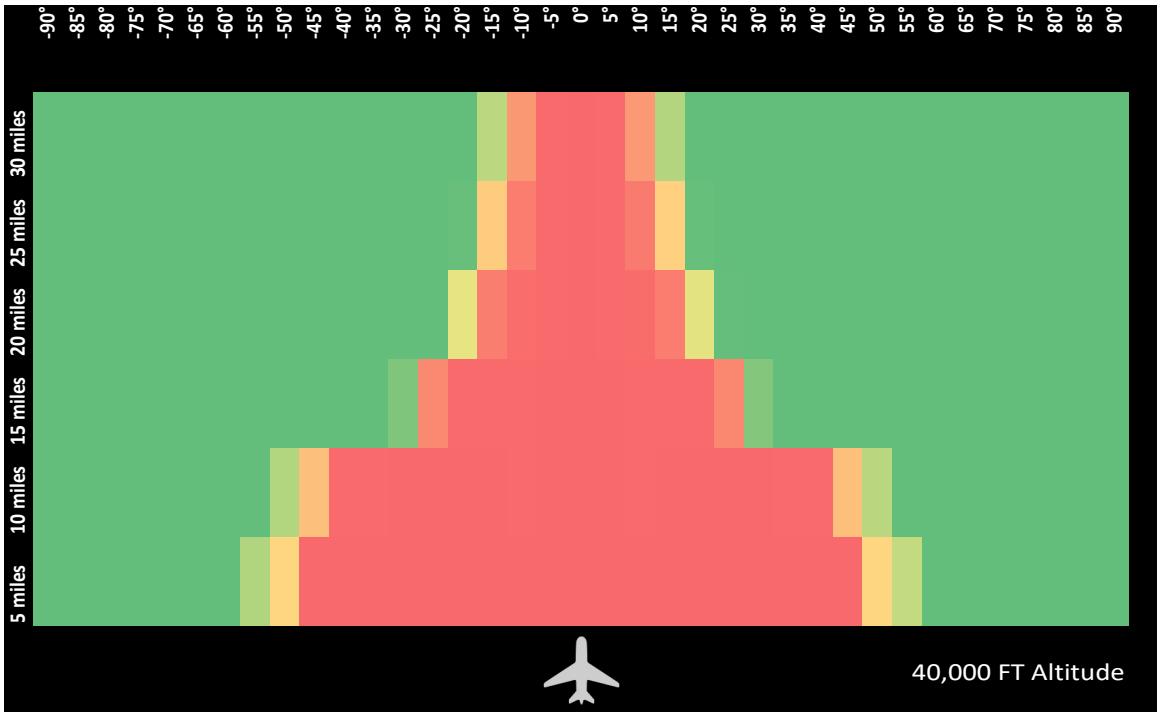

Figure 21: 40,000 feet Threat Map: Threat map for ranges and relative bearings at 40,000 feet.

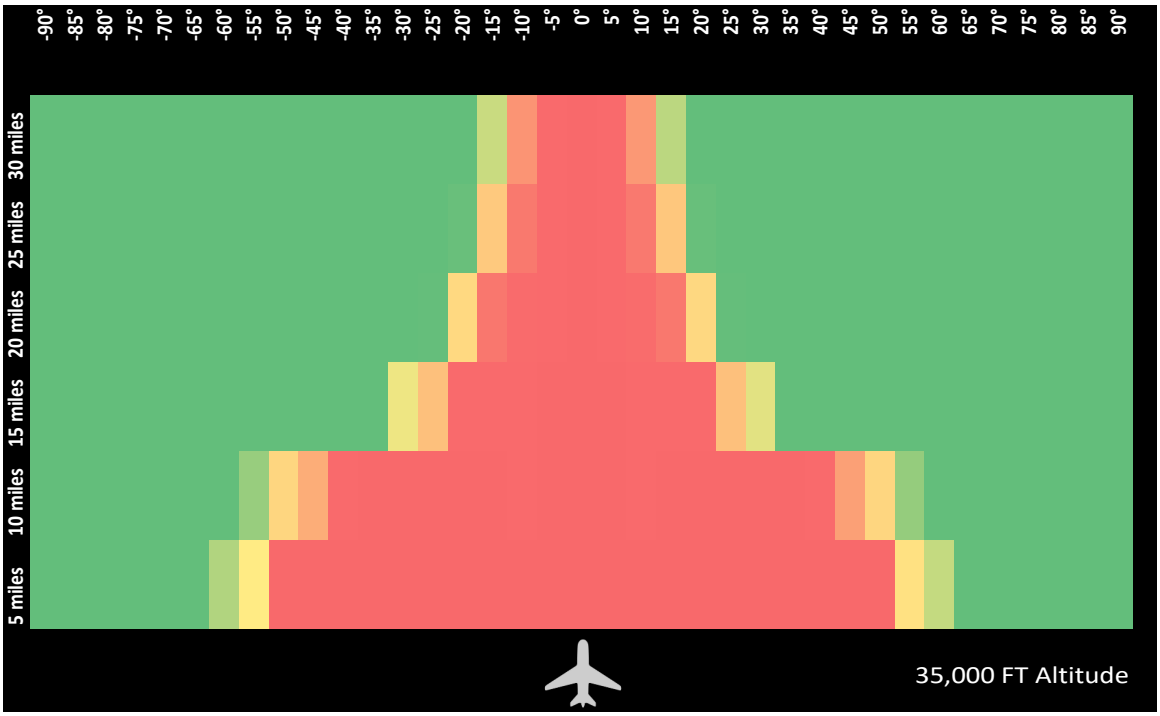

Figure 22: 35,000 feet Threat Map: Threat map for ranges and relative bearings at 35,000 feet.

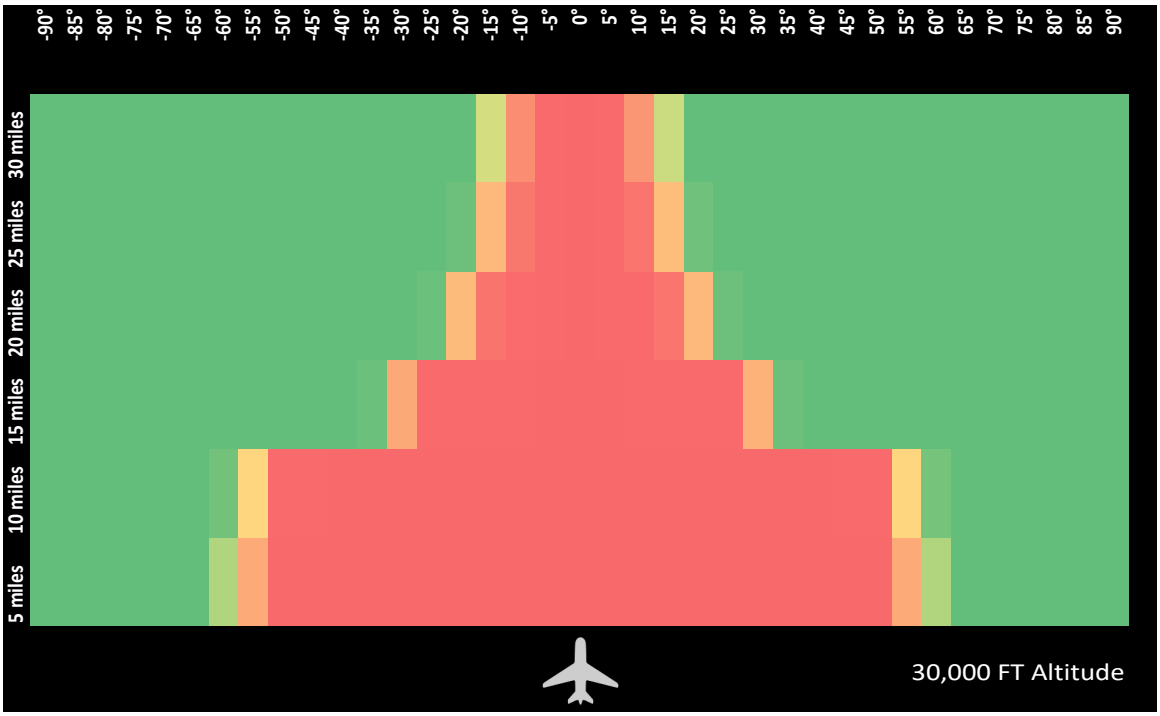

Figure 23: 30,000 feet Threat Map: Threat map for ranges and relative bearings at 30,000 feet.

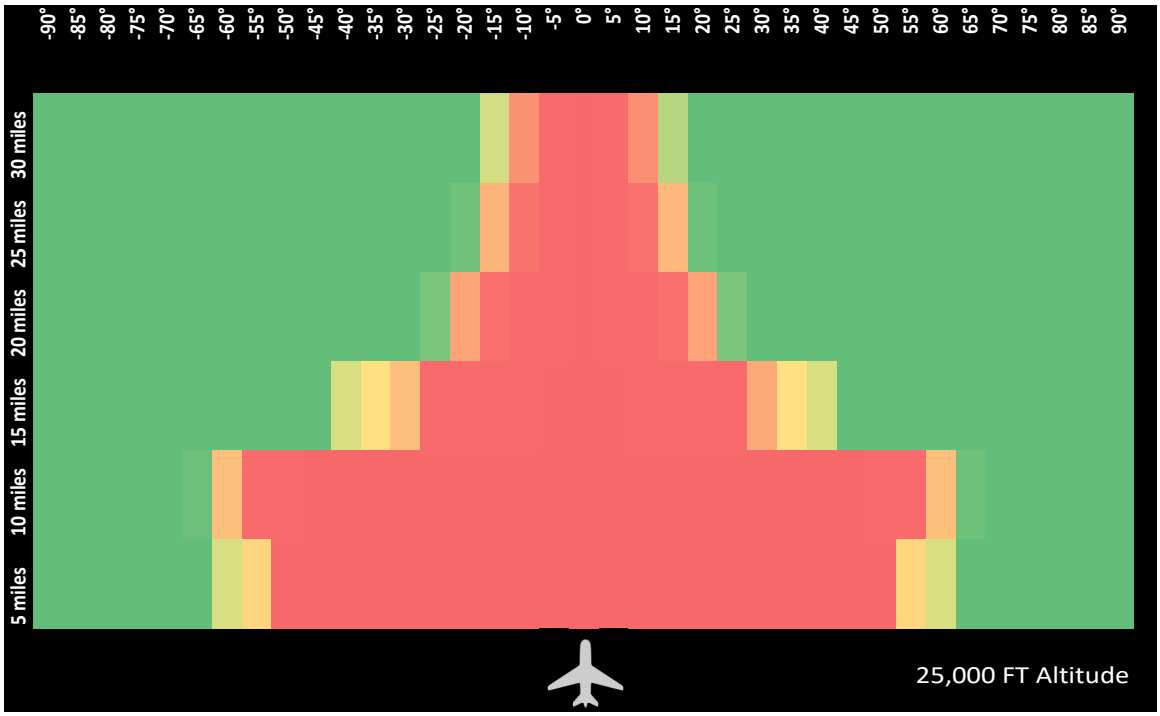

Figure 24: 25,000 feet Threat Map: Threat map for ranges and relative bearings at 25,000 feet.

VI. Conclusion

This academic thesis presented a comprehensive overview of threat actors and a Traffic Collision Avoidance System (TCAS) threat taxonomy. Additionally, the thesis constructed a dynamic simulation, focused on timing interrogation responses while satisfying varying TCAS tests and constraints. Upon simulation completion, the thesis described a detailed analysis of security vulnerabilities. The thesis's goal is to enhance the TCAS security knowledge of companies and agencies that rely on the use of TCAS. Additionally, the thesis aspires to drive research into TCAS vulnerability solutions, specifically the spoofing vulnerability. Moreover, the thesis provides aircraft pilots with a potential threat landscape while operating the aircraft. The impact that TCAS has on government and citizen safety warrants clear knowledge of threats and developed countermeasures.

This thesis provides a general landscape of threat actors, their capabilities, and their potential attacks. Additionally, the thesis further studies the requirements for the false injection attack and then performs a simulation to understand the success rate of it. The simulation procedures include several steps. First, a threat actor model is created, and with open-source documents, a vulnerability assessment is developed for TCAS. Second, the requirements for interrogation timing, the range test, the altitude test, the power test, and bearing constraints are discovered. Next, using MATLAB, a simulation that calculates the required timing for TCAS interrogation responses while satisfying all of the required tests is completed. Fourth, the analysis of the results creates a probability of success for certain regions in a flight path and a threat map for pilots. Lastly, a discussion of the results and the future work in the TCAS security occurs.

6.1 Security Impact

[4] proposed and successfully created TCAS Mode S messages. This thesis orchestrated the remaining requirements for a successful false injection attack. The ability to create TCAS Mode S messages paired with known flight paths that successfully satisfy range, altitude, power, and bearing requirements present a true attack vector for adversaries discussed in this thesis. The success plausibility of this attack presents doubt, even if minute, in the integrity of a TCAS screen. Doubt in integrity creates distrust for pilots. A system responsible for numerous lives, necessitates complete pilot trust, so solutions to this attack capability require exploration.

6.1.1 Proposed Solutions

A solution to the false injection vulnerability requires addressing the capability of creating TCAS messages. Additionally, addressing the simplicity of the TCAS tests and constraints further strains false injection capabilities.

TCAS accepts any TCAS message received from a correctly addressed aircraft [46]. TCAS does not have an aircraft confirmation capability. A potential solution is having TCAS systems communicate their current air picture. Discrepancies between multiple TCAS systems require further investigation and the ability to discern real and false aircraft. Further, this allows the verification of aircraft positioning data, further enhancing the viability of a particular aircraft's current TCAS picture.

Specifically addressing the viability of a ground-based attacker triggering a false injection attack, the altitude processing of TCAS requires exploration. TCAS uses altitude provided in Mode S messages during the placement of aircraft in its surrounding airspace. A plausible solution requires aircraft to verify altitude by a vertical angle of arrival verification. The reported altitude and measured vertical angle of arrival comparison gives TCAS an additional verification tool on determining requirements

for RA issuance. Without a trusted altitude, aircraft cannot trigger an RA, only a TA [11].

6.2 Future Work

In addition to future work in a security solution, the proposed false injection attack requires additional research. The next two areas of focus are interrogation and reply periodicity, or how often and dispersed are interrogations and their replies with operational TCAS systems. Additionally, the TCAS message creation paired with the timing and threat maps require real-world experimentation.

6.2.1 Interrogation/Reply Periodicity

Interrogations and replies have mandated timelines according to [30]. The delay mandate of 132.75 microseconds between the first interrogation pulse and the first interrogation reply pulse requires confirmation from active TCAS systems. The reply delay allows the false injection to occur, and without the delay or jitter in the expected delay, the false injection becomes less likely and most improbable. Measuring the delay requires the monitoring of two operational TCAS systems communicating. The delay becomes observable during the communication process.

6.2.2 Real-World Implementation

In addition to verification of interrogation and reply periodicity, the developed timing capabilities and threat maps require validation with real-world systems. This thesis provided threat maps based on publicly available information about TCAS. The developed simulation provides TAU measurements for each range, altitude, and relative bearing. Additionally, the simulation provides the required timing for each message. An operational software-defined radio (SDR), antenna, and target TCAS

afford the capability to test the threat maps and timing developed. The best course of action requires starting with a stationary aircraft to verify the ability to trigger an RA from different ranges, altitudes, and starting bearings.

Bibliography

1. Federal Aviation Administration. "Air Traffic By Numbers", 2020.

2. Matthew Smith, Martin Strohmeier, Jon Harman, Vincent Lenders, and Ivan Martinovic. "Safety vs. Security: Attacking Avionic Systems with Humans in the Loop". May 2019.

3. Sheryl L Chappell, Charles E Billings, and Thomas E Kozon. "Pilots' Use of a Traffic Alert and Collision-Avoidance System (TCAS II)in Simulated Air Carrier Operations Volume I: Methodology, Summary, and Conclusions", 1989.

4. Paul M Berges and Jeffrey H Reed. "Exploring the Vulnerabilities of Traffic Collision Avoidance Systems (TCAS) Through Software Defined Radio (SDR) Exploitation", 2019.

5. J Oestergaard. "An Overview of the U.S. Commercial Aircraft Fleet", Nov 2018.

6. Emily Chang, Roger Hu, Danny Lai, Richard Li, Quincy Scott, and Tina Tyan. "The Story of Mode S". *MIT*, Dec 2000.

7. Ken Hoke. "TCAS: Preventing Mid-Air Collisions", Nov 2015.

8. "Product Focus: TCAS", Apr 2002.

9. Vincent A. Orlando. "The Mode S Beacon Radar System". *The Lincoln Laboratory Journal*, 2:345–362, 1989.

10. Wes Stamper. "Understanding Mode S Technology: How Does the Interrogation and Reply Actually Work?". *Aircraft Engineering and Aerospace Technology*, 76:18, 2005.

11. Radio Technical Commission for Aeronautics. "Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System (TCAS), Version 1", Jun 2008.

12. Mica Workshop. "Mode S Surveillance Principle". 2019.

13. James K Kuchar and Ann C Drumm. "The Traffic Alert and Collision Avoidance System". *Lincoln Laboratory Journal*, 16:277–296, 2007.

14. Federal Aviation Administration. "Introduction to TCAS II", Feb 2011.

15. César Muñoz, Anthony Narkawicz, and James Chamberlain. "A TCAS-II Resolution Advisory Detection Algorithm". Aug 2013.

16. Sushrut Vaidya and Taha Khot. "Analysis of the Tau Concept Used in Aircraft Collision Avoidance through Kinematic Simulations". IEEE, Jan 2017.

17. Camilo Andres and Pantoja Viveros. "Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts", 2016.

18. Savio Sciancalepore and Roberto Di Pietro. "SOS - Securing Open Skies", 2018.

19. Xuhang Ying, Joanna Mazer, Giuseppe Bernieri, Mauro Conti, Linda Bushnell, and Radha Poovendran. "Detecting ADS-B Spoofing Attacks using Deep Neural Networks", 2019.

20. Peter Aldhous. "We Trained a Computer To Search For Hidden Spy Planes: This is What We Found", Aug 2017.

21. United States Government Accountability Office. "AVIATION SECURITY: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals Report to Congressional Requesters", Feb 2020.

22. Kayvan Faghih Mirzaei, Bruno Pessanha De Carvalho, Patrick Pschorn, Kayvan Faghih, Mirzaei Bruno, and Pessanha De Carvalho. "Easychair Preprint Security of ADS-B: Attack Scenarios Security of ADS-B: Attack Scenarios". *EasyChair*, 2019.

23. International Civil Aviation Organization. "ADS-B IMPLEMENTATION AND OPERATIONS GUIDANCE DOCUMENT INTERNATIONAL CIVIL AVIATION ORGANIZATION ASIA AND PACIFIC OFFICE", 2014.

24. Surendra Khadka, M S Anuradha, and Ch Padmasree. "Study of the Effect of Barrage and Deception Jamming on a Radar System along with their Mitigation Technique". *International Journal of Science and Research*, 4:2319–7064, 2013.

25. Celine Hacobian. "Here's How High Planes Actually Fly, According to Experts", Jun 2018.

26. Krishna Sampigethaya, Radha Poovendran, and Linda Bushnell. "Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes Measures to Protect Safety and Business Viability are Important in the Operation, Control and Maintenance of Aircraft and Air Traffic Enabled by Advanced Information Systems". *IEEE*, 96:1992–2007, 2018.

27. Donald L McCallie. "EXPLORING POTENTIAL ADS-B VULNERABILITIES IN THE FAA'S NEXTGEN AIR TRANSPORTATION SYSTEM GRADUATE RESEARCH PROJECT AIR FORCE INSTITUTE OF TECHNOLOGY", 2011.

28. Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "Understanding Realistic Attacks on Airborne Collision Avoidance Systems". Oct 2020.

29. Suresh Mikkili, Anup Kumar Panda, and Jayanthi Prattipati. "Review of Real-Time Simulator and the Steps Involved for Implementation of a Model from MATLAB/SIMULINK to Real-Time". *Journal of The Institution of Engineers (India): Series B*, 96, Jun 2015.

30. Federal Aviation Administration. "U.S. NATIONAL AVIATION STANDARD FOR THE MODE SELECT BEACON SYSTEM (MODE S)", Jan 1983.

31. W H Harman. "TCAS: A System for Preventing Midair Collisions". *The Lincoln Laboratory Journal*, 2:437–458, 1989.

32. Boeing. "The Boeing Next-Generation 737 Family – Productive, Progressive, Flexible, Familiar", Jun 2014.

33. Paul Illman. Principles of flight, 1980.

34. J D Welch and V A Orlando. "Traffic Alert and Collision Avoidance System (TCAS): A Functional Overview of Minimum TCAS II", Apr 1983.

35. Joseph A. Shaw. "Radiometry and the Friis Transmission Equation". *American Journal of Physics*, 81, Jan 2013.

36. Christian Wolff. "Free-Space Path Loss (FSPL)".

37. M L Wood. "TCAS II ATCRBS Surveillance Algorithms", Jan 1985.

38. Kirt Blatenberger. "Electronic Warfare and Radar Systems Engineering Handbook - Doppler Shift".

39. C. Livadas, J. Lygeros, and N.A. Lynch. "High-Level Modeling and Analysis of the Traffic Alert and Collision Avoidance System (TCAS)". *Proceedings of the IEEE*, 88, Jul 2000.

40. John Van Dongen and Leo Wapelhorst. "Data Link Test and Analysis System/T-CAS Monitor User's Guide", Feb 1991.

41. David P. Doane and Lori E. Seward. "Measuring Skewness: A Forgotten Statistic?". *Journal of Statistics Education*, 19, Jul 2011.

42. S West, J Finch, and P Curran. "Structural Equation Models with Non-Normal Variables: Problems and Remedies", 1995.

43. Lawrence T Decarlo. "On the Meaning and Use of Kurtosis". *Psychological Methods*, 2:292–307, 1997.

44. Hae-Young Kim. "Statistical Notes for Clinical Researchers: Assessing Normal Distribution Using Skewness and Kurtosis". *Restorative Dentistry & Endodontics*, 38, 2013.

45. Jason Osborne. "Improving Your Data Transformations: Applying the Box-Cox Improving your Data Transformations: Applying the Box-Cox Transformation". *Practical Assessment, Research, and Evaluation*, 15:12, 2010.

46. J. Hannah, R. Mills, and R. Dill. "Traffic Collision Avoidance System: Threat Actor Model and Attack Taxonomy". In *2020 New Trends in Civil Aviation (NTCA)*, pages 17–26, 2020.

Acronyms

AC Altitude Code. 11

ACAS Aircraft Collision Avoidance System. 1

ADS-B Automatic Dependent Surveillance - Broadcast. 18, 20, 21, 22, 24, 31, 32

APT advanced persistent threat. 20, 30, 31

ATC air traffic control. 6, 13

ATCRBS Air Traffic Control Radar Beacon System. 7

CAASD Mitre Center for Advanced Aviation System Development. 7, 8

CIA confidentiality, integrity, and availability. 23

DABS Discrete Address Beacon System. 7

DF Downlink Format. 8, 10, 11, 49

DoS Denial-of-Service. 24, 26

FAA Federal Aviation Administration. 1, 7, 8, 13

IC interrogator code. 10

ICAO International Civil Aviation Organization. 8, 10, 11, 27, 28

IFF Identification Friend or Foe. 6

MIT-LL Massachusetts Institute of Technology - Lincoln Laboratory. 7

NASA National Aeronautics and Space Administration. 1

RA resolution advisory. 13, 14

RAC resolution advisory complement. 28

RI reply information. 10

RTT round-trip travel time. 28

SDR software-defined radio. 2, 21, 24, 26, 27, 32, 74

TA traffic alert. 13, 16

TCAS Traffic Collision Avoidance System. iv, x, 1, 2, 3, 4, 34, 36, 37, 38, 44, 45, 46, 48, 49, 50, 52, 54, 59, 61, 72, 73, 74

TSA Transport Security Administration. 21

UF Uplink Format. 8, 10, 11, 13, 49

VS vertical status. 10

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
19–03–2021	Master's Thesis	Sept 2019 — Mar 2021

4. TITLE AND SUBTITLE

A CYBER THREAT TAXONOMY AND A VIABILITY ANALYSIS FOR FALSE INJECTIONS IN THE TRAFFIC COLLISION AVOIDANCE SYSTEM (TCAS)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

John W. Hannah

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-21-M-045

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

NONE

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis provided background information on the Traffic Collision Avoidance System (TCAS). Additionally, the thesis developed a threat taxonomy for TCAS, resulting in the determination that a false injection attack presents the most comprehensive risk. Moreover, the thesis presents the development of a program to determine what ranges, altitudes, and relative bearings are most vulnerable to a false injection attack. The program includes test for all requirements of a successful false injection. Furthermore, the thesis presents an analysis of results and creates threat maps as situational awareness tools. Lastly, the thesis discusses potential solutions to the false injection attack, covers future work in the areas of TCAS vulnerabilities, and concludes the thesis.

15. SUBJECT TERMS

TCAS, Vulnerability, False Injection, Threat Map

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Captain John W. Hannah, AFIT/ENG
U	U	U	UU	94	19b. TELEPHONE NUMBER *(include area code)* (404) 709-7278; john.hannah@afit.edu