The Journal of Supercomputing (2021) 77:12666–12689
https://doi.org/10.1007/s11227-021-03766-9

Traffic collision avoidance system: false injection viability

John Hannah[1] · Robert Mills[1] · Richard Dill[1] · Douglas Hodson[1]

Accepted: 19 March 2021 / Published online: 12 April 2021

Abstract

Safety is a simple concept but an abstract task, specifically with aircraft. One critical safety system, the Traffic Collision Avoidance System II (TCAS), protects against mid-air collisions by predicting the course of other aircraft, determining the possibility of collision, and issuing a resolution advisory for avoidance. Previous research to identify vulnerabilities associated with TCAS's communication processes discovered that a false injection attack presents the most comprehensive risk to veritable trust in TCAS, allowing for a mid-air collision. This research explores the viability of successfully executing a false injection attack against a target aircraft, triggering a resolution advisory. Monetary constraints precluded access to a physical TCAS unit; instead, this research creates a novel program, TCAS-False Injection Environment (TCAS-FIE), that incorporates real-world distributed computing systems to simulate a ground-based attacker scenario which explores how a false injection attack could target an operational aircraft. TCAS-FIEs' simulation models are defined by parameters to execute tests that mimic real-world TCAS units during Mode S message processing. TCAS-FIE simulations execute tests over applicable ranges (5–30 miles), altitudes (25–45K ft), and bearings standard for real-world TCAS tracking. The comprehensive tests compare altitude, measure range closure rate, and measure signal strength from another aircraft to determine the delta in bearings over time. In the attack scenario, the ground-based adversary falsely injects a spoofed aircraft with characteristics matching a Boeing 737-800 aircraft, targeting an operational Boeing 737-800 aircraft. TCAS-FIE completes 555,000 simulations using the various ranges, altitudes, and bearings. The simulated success rate to trigger a resolution advisory is 32.63%, representing 181,099 successful resolution advisory triggers out of 555,000 total simulations. The results from additional analysis determine the required ranges, altitudes, and bearing parameters to trigger future resolution advisories, yielding a predictive threat map for aircraft false injection attacks. The resulting map provides situational awareness to pilots in the event of a real-world TCAS anomaly.

✉ John Hannah
jchannah1021@gmail.com

[1] Air Force Institute of Technology, Dayton, USA

Keywords TCAS · False injection · Threat map

1 Introduction

The focus of the aviation industry is passenger safety during flight. Airlines have to continually balance passenger safety with customer satisfaction. Mid-air collisions from cyber capabilities are more than theoretical, but rather a possible occurrence given the current communications technology, specifically with a software-defined radio (SDR). SDRs are inexpensive radios capable of creating, sending, receiving, and processing Mode S signals. SDRs are easily accessible, further expanding the number of potential threats [1]. The safety risk to TCAS includes over 1 billion travelers each year [2].

TCAS is a critical cyber-physical system designed to prevent mid-air collisions between aircraft. The current version of TCAS in use is TCAS II, and it is the focus of this paper. Specifically, TCAS uses Mode S communications to exchange distance, altitude, and bearing information. TCAS processes this information and determines the feasibility of a mid-air collision, warning the pilot if necessary [3].

1.1 Motivation

The National Aeronautics and Space Administration (NASA) conducted a study [4] to determine the necessity of an automated system to prevent mid-air collisions. NASA tested 16 aircrews (48 individuals in total). The results showed that four declared near mid-air collisions (less than 1000 feet horizontal and 200 feet vertical separation) would have occurred during 32 total flights [4]. With an operational TCAS, there were zero near mid-air collisions in 96 flights. TCAS reduces the probability of a near mid-air collision by approximately 87 percent.

If an adversary targets and successfully denies, degrades, or destroys an operational TCAS, the possibility of a mid-air collision increases. For passenger safety, all attack possibilities against TCAS require examination. Previous research into TCAS vulnerabilities determined that a false injection attack is plausible [1, 5]. The false injection attack presents a risk to the safety and security of passengers. This research quantifies the inherent risk of a successful false injection attack against an aircraft's TCAS by creating a novel false injection environment, TCAS-FIE. TCAS-FIE uses simulation models to determine all possible locations of a successful false injection attack. Determining false injection viability informs pilots and industry of the actual operational risk during flight.

1.2 Organization

Section 2 provides an overview of TCAS communication security issues and its warning notifications, a background of Mode S timing properties, and a review of previous research. Previous research results lead to the requirement for a model and simulation of a ground-based attacker targeting an operational TCAS. Section 3

presents the development of a MATLAB simulation environment, TCAS-FIE, that models an adversary targeting a TCAS unit by timing Mode S messages. The environment includes distributed computing systems, the ground-based attacker/equipment and the TCAS unit. Each TCAS reply from the adversary faces a range of TCAS tests and requirements for a successful, false injection attack. Tedious exploration of the technical specifications and pseudocode for TCAS provided the knowledge for creating the TCAS-FIE simulations. Section 4 overviews the process of validating and verifying the processes within TCAS-FIE. Section 5 presents the simulations' results and provides a predictive threat map for auspicious false injection attacks against TCAS.

2 Background

2.1 TCAS system overview

Traffic Collision Avoidance System is the certified collision detection system used on aircraft within the United States [6]. It pairs with an aircraft's Mode S transponder to conduct collision detection communications with surrounding aircraft. TCAS performs its communications using an interrogation and reply process. The interrogating aircraft sends an all-call interrogation to all surrounding aircraft within 30 miles; the interrogating aircraft receives the reply, processes the reported altitude, and measures the aircraft's bearing. Additionally, the interrogating aircraft determines the aircraft's distance by measuring the round-trip travel time of an interrogation and reply sequence. With the altitude, range, and bearing, TCAS creates a track of the responding aircraft. After the initial reply, TCAS continues to interrogate the responding aircraft, until the aircraft no longer poses a threat.

For the communication process, TCAS includes several system components.

- *Computer Unit*: The Federal Aviation Administration (FAA) describes the computer unit as the brains of TCAS [3]. It performs all necessary TCAS actions: threat detection, threat tracking, collision avoidance determination. After determining a collision avoidance maneuver, the computer unit creates and displays a Traffic Advisory (TA) or Resolution Advisory (RA), alerting the pilot of imminent danger and offers a remedial solution.
- *Mode S Transponders*: The Mode S [7] transponder allows communication between aircraft.
- *Control Panel*: The control panel is an interactive Mode S transponder control switch for pilots. Settings include on, off or standby [3].
- *Antennas*: TCAS uses four antennas to communicate with nearby aircraft [7]. The antennas dually support TCAS and Mode S communications. Modern-day TCAS systems have two 1030 MHz omnidirectional antennas, located above and below the aircraft, that perform all Mode S communications.
- *Displays*: Two TCAS displays [3] show real-time traffic and advisories to provide situational awareness to the pilot. The RA display only alerts when an aircraft enters an imminent threat zone, representing an approach that could yield a

collision. Also, the RA display gives vertical speed and pitch recommendations to avoid a mid-air collision.

2.2 TCAS warning notifications

TCAS has two notifications: TA and RA [3]. TAs give potential threat warnings, while RAs refer to imminent threats.

The TCAS computer unit develops a TA or RA from algorithmic calculations of the interrogated aircraft's TCAS messages. The two major calculations are for the sensitivity thresholds, horizontal TAU and vertical TAU. Horizontal TAU measures the closest time to impact on the horizontal plane, or range [8], while vertical TAU measures the closest time to impact on the vertical plane, or altitude. If both of the TAU measurements exceed set thresholds, a TA or RA triggers.

In addition to the TAU calculations, TCAS monitors reported altitude from aircraft and calculates the overall range. Altitude is a field within Mode S replies [9]. Vertical or altitude separation is also known as ZTHR. TCAS measures range by calculating the round-trip time for an interrogation and reply sequence. Range is also referred to as DMOD. Issuance of a TA or RA occurs when one of the following threshold combinations are exceeded:

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

Figure 1 provides a visual representation for the two warnings. The red represents the immediate danger area around the aircraft, when an RA is necessary. The yellow area represents a potential risk to the aircraft, when a TA is necessary.

2.2.1 Traffic advisory (TA)

TCAS issues a TA once an aircraft becomes a plausible threat to the host aircraft [3]. A TA provides situational awareness for the pilot. Additionally, the TA readies the pilot for a potential RA issuance. When a TA occurs, TCAS marks the intruder yellow on the traffic display and provides an auditory warning to the pilot.

To determine the necessity of a TA, first, TCAS measures the round-trip travel time between its interrogation and the intruder's reply. Next, TCAS calculates

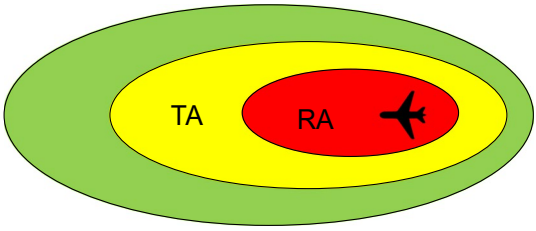

Fig. 1 TA and RA visual: Visual representation showing when TCAS issues an RA or TA to the pilot [10] (color figure online)

ZTHR, DMOD, Horizontal TAU, and Vertical TAU. If those values exceed the thresholds in Table 1, TCAS issues a TA [3].

2.2.2 Resolution advisory (RA)

The final step in the TCAS protective measures is the issuance of an RA. TCAS issues an RA once an intruding aircraft becomes an imminent threat to the safety of the aircraft [7]. There are different types of RAs; however, they all alert when a collision is imminent. TCAS marks the intruder on the RA display as a red dot. Additionally, TCAS provides an auditory warning to the pilot, as well as avoidance maneuver instructions for the pilot [7]. These instructions ensure a safe encounter between the two aircraft.

Similar to the TA process, for RA issuance, TCAS measures the round-trip travel time of the interrogation response. From that measurement, TCAS calculates DMOD, ZHTR, vertical TAU, and the horizontal TAU. TCAS compares the calculated values against the threshold limits listed in Table 1. If the calculated value exceeds the thresholds, TCAS issues an RA.

2.3 Mode S timing

TCAS uses two interrogation and reply types: All-Call interrogations/replies and Short TCAS interrogations/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 TCAS. An all-call reply follows the interrogation.

2.3.1 All-call interrogations/replies

The All-Call interrogation is the first interrogation received by an aircraft. Figure 2 shows a Mode S interrogation timing layout [7].

The standard for all-call interrogations is 56 bits [10]. The bits send during the P_6 pulse. Additionally, the transmission rate for Mode S interrogations is 4 Mbps [11]. Mode S requires systems to wait for 128 microseconds from the phase sync reversal of the interrogation until the rising edge of the replies first pulse [10].

Table 1 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

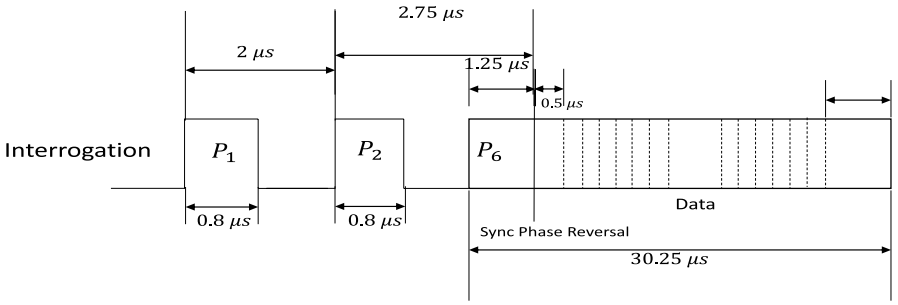

Fig. 2 Mode S Interrogation Format: Layout and timing for Mode S interrogations [7]

There are 4.75 microseconds from the first pulse of the interrogation to the phase sync reversal of the interrogation [10]. This gives a total of 132.75 microseconds from interrogation received to the first pulse of the reply. Figure 3 illustrates the timing of a Mode S reply. All-Call replies have 56 bits in the reply. The reply bit rate is 1 Mbps [7].

2.3.2 Short TCAS interrogations/replies

Once the All-Call interrogation and reply sequence completes, TCAS begins short interrogations and replies. The timing of short TCAS interrogations depends on the TAU calculation of an interrogation reply. If TAU is greater than 60, TCAS interrogates every 5 seconds. If TAU is less than or equal to 60, then TCAS interrogates every second. TCAS has a timing jitter of ± 10 percent from the time values.

All-Call and short TCAS interrogations/replies have the same transmission rate and bit length. One notable aspect is that the 132-microsecond delay between a received interrogation and expected reply allows a window for a potential adversary to falsely inject into an aircraft.

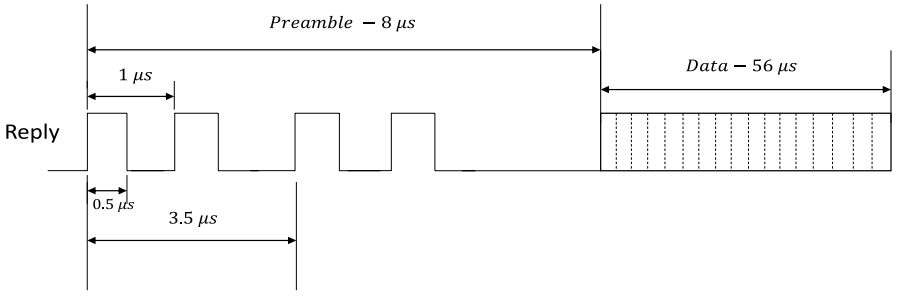

Fig. 3 Mode S Reply Format: Layout and timing for Mode S replies [10]

2.4 Previous TCAS security research

For a critical system, there is little research on protecting and preserving TCAS integrity and its communication processes. The lack of TCAS research motivated the authors to understand how an adversary would attack TCAS, so that counter measures could be implemented. Berges et al. focused on creating malicious Mode S responses [1]. Hannah et al. discovered and described possible TCAS threats [5]. Both of these authors showed the possibility of a successful false injection onto a target TCAS screen, but neither implemented them, which is the focus of this paper.

2.4.1 TCAS mode S message creation

Berges et al. [1] focused on the processing and creating of TCAS Mode S messages. Ultimately, the research showed the successful development of TCAS responses. The messages included all required data fields for a TCAS unit to process. Additionally, the author processed Mode S interrogations. The ability to process and create TCAS messages is key to false injection presented in Sect. 3.

2.4.2 TCAS threat taxonomy

Hannah et al. [5] presents a TCAS threat taxonomy that determined a false injection vulnerability presents the highest risk to TCAS integrity, yielding mid-air collision, and pilot distrust. It was the only vulnerability to have two significant impacts.

- *Pilot Distrust* A verifiable false RA creates a distrust in TCAS's accuracy.
- *Near Mid-Air Collision* A false RA could alter a pilot's course that interferes with the path of another aircraft.

This taxonomy and the message creation research projects reinforced the necessity for a false injection simulation. The works led directly to the development of TCAS-FIE, providing the capability to test false injections against TCAS.

3 Methodology of false injection viability

This section details the design of the novel Traffic Collision Avoidance System-False Injection Framework (TCAS-FIE), founded in MATLAB, to simulate a ground station adversary attacking an operational aircraft. The authors deciphered the technical specifications and pseudocode to determine requirements for a successful false injection attack and RA trigger. In the environment, TCAS-FIE determines an attacker's viability to successfully time Mode S responses that satisfy all required TCAS tests and constraints, triggering an RA. It also tests aircraft at different ranges, altitudes, and relative bearings.

The 132-microsecond delay between a received TCAS interrogation and the reply [10] yields an opportunity for an adversary to introduce malicious data, subverting TCAS integrity and trust. TCAS-FIE simulates how an adversary would exploit this vulnerability to put aircraft at risk.

3.1 TCAS-FIE environment

The authors created TCAS-FIE exclusively within MATLAB. TCAS-FIE implements several real-world distributed computing systems within its one environment. TCAS-FIE contains implementations of a ground-based attack paired with an SDR, processing equipment, and antenna. Additionally, it implements a spoofed aircraft with realistic flight profiles. Most importantly, TCAS-FIE imitates a real-world TCAS system, with tests and requirements from the TCAS pseudocode [7] implemented and fully operational within the environment. The imitated TCAS system also sends interrogations within nanoseconds of a comparative real-world TCAS system.

Furthermore, the authors developed TCAS-FIE on a 64-bit Windows-based operating system with an Intel Xeon E3-1535M Computer Processing Unit (CPU) with 32 GigaBytes (GB) Random Access Memory (RAM). Each simulation takes approximately 0.02 seconds. For a set of 500 simulations, the total runtime is 10 seconds. The set is ran a total of 500 times (8.33 minutes) to ensure the results are accurate over multiple trials. The CPU usage during simulations approached 99%. For future simulations, graphics processing units (GPU) offer much faster processing time for the simulations. For real-world situations, the results need to be instantaneous and provide an accurate average. 8.33 minutes is too long for a potential mid-air collision situation. The results of TCAS-FIE determine where RA issuance is possible from a ground-based attacker.

3.2 Assumptions

TCAS-FIE simulates an air operational environment with the following assumptions:

3.2.1 Flat earth

Using the flat earth model and associated (x,y,z) coordinates suffice for this simulation. The minimum altitude considered is 25,000 feet. With a ground-based attacker, the smallest line of sight is 228.218 miles. The farthest range implemented is 30 miles, only 13 percent of the visual identification distance possible.

3.2.2 Terrain and weather

The terrain is flat, and the weather is clear. Non-flat land presents a risk for a potential reflection of signals, while adverse weather limits pilots' visual identification range. This simulation is operationally consistent, since pilots require clear weather to verify the existence of an aircraft visually.

3.2.3 Aircraft speed and altitude

The spoofed and targeted aircraft are Boeing 737–800s, the most used commercial aircraft in the world [12]. Both aircraft travel within ± 10 feet per second of their cruising speed. Additionally, TCAS-FIE assumes the target aircraft maintains its cruising altitude ± 700 feet from one TCAS interrogation to the next.

3.3 Antenna and transmitter requirements

TCAS-FIE assumes the ground-based attacker has the appropriate equipment to satisfy the signal requirements. TCAS has specific antenna and signal strength requirements to accept interrogation replies. Table 2 lists the signal profile for TCAS. [7, 13].

3.4 Aircraft implementation

TCAS-FIE simulates two B737-800s; one is spoofed, and the other is the target aircraft.

3.4.1 Aircraft speed and altitude

The cruise speed of the B737-800 is 0.789 mach or 887.88 feet per second [12]. For simulation variance, the aircraft cruising speed varies ± 10 feet per second.

Additionally, the cruising altitude of the B737-800 is 35,000 feet [12]. The altitude varies over different simulations to test all possible range, altitude, and relative bearing combinations.

3.4.2 Turning capability

To provide realistic flight paths, the aircraft turn during the simulations. The target aircraft turns left or right, altering its course. TCAS-FIE also allows the target aircraft to maintain its current trajectory. The spoofed aircraft mirrors the movements of the target aircraft turns.

The aircraft's speed and the bank angle determine how many degrees the aircraft turns, left or right, in one second. The maximum bank angle without putting the

Table 2 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

passenger's safety at risk is 25 degrees [14]. With the cruising speed and bank angle known, the standard rate of turn is 1 degree per second as shown in Eq. 1:

$$\begin{aligned} \text{Bank Angle} &= 25 \text{ degrees} \\ \text{Velocity} &= \frac{887 \text{ ft/s}}{1.688} / 1.688 = 525.533 \text{ knots} \\ \text{Rate of Turn} &= \frac{1091 * \tan(\text{Bank Angle})}{\text{Velocity}} \\ &= .97 \text{ degrees per second} \end{aligned} \tag{1}$$

3.5 Program overview

TCAS-FIE runs sets of 500 simulations with the same parameters. After a set completes, the starting relative bearing from the target aircraft to the ground station increases by 5 degrees. After 37 sets with different starting bearings, the altitude, range, or altitude and range change. In total, the authors ran 555,000 simulations, with 111,000 simulations at each altitude with differing ranges. The following subsections discuss the details of the parameters.

3.5.1 Range

There is variation in the starting range for the target aircraft. The variants are 5– 30 miles in 5-mile increments. Thirty miles is the max range as the maximum distance of TCAS is 35 miles [15].

3.5.2 Altitude

There is variation in the altitude for the target aircraft and spoofed aircraft. The variants are 25,000– 45,000 ft in 5000 ft increments. This includes the most common cruising altitude of aircraft, 35,000 feet [12].

3.5.3 Starting relative bearing

The starting relative bearing of the target aircraft changes after each set of 500 simulations. The original starting relative bearing from target to ground is 90 degrees. After 500 simulations, the relative bearing decreases by 5 degrees. Once at 0 degrees, the next change is relative bearing is to 355 degrees. The final relative bearing is 270 degrees. The range is [90–0] and [355–270]. This relative bearing change gives the pilot the possibility of visual identification of an RA inducing aircraft. In this attack, there is no actual aircraft, potentially causing the pilot confusion and distrust.

3.5.4 Spoofed aircraft insertion

After the ground station replies to the first interrogation, the spoofed aircraft appears on the appropriate TCAS display. The spoofed aircraft has the same reported altitude as the target aircraft. To account for the delta in distance from the ground versus the distance from a same-altitude aircraft, TCAS-FIE places the spoofed aircraft further away on the (x,y) plane.

3.6 Tests implementation

This section presents the implementation of the required tests and limitation checks of TCAS. The order of tests follows TCAS's order of processing. The implemented tests and constraints are the received signal power test, bearing constraint check, the diverging range test, the TAU range test, and the altitude test.

3.6.1 Received signal power test

TCAS requires a received signal strength of > -74 dBm to accept an interrogation reply [13]. The TCAS minimum antenna gain is 0 dBi. The power and gain chosen for the attacker are 50 dBm and 5 dBi, respectively. These are conservative values, as individuals have many choices for power and gain capabilities, some much stronger than 50 dBm and 5 dBi. TCAS-FIE uses the Friis equation [16] to determine the power received by the attacker and if that power meets the specified requirement of -74 dBm. TCAS-FIE uses the Friis equation, shown in equation 2:

$$Rx_P = Tx_P + Tx_G + Rx_G - \text{FSPL} \tag{2}$$

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 deteriorates over the length of distance that it travels [17]. Equation 3 shows the implemented equation for free-space path:

$$\text{FSPL} = 20 * \log_{10}\left(\frac{4 * pi * R}{\lambda}\right) \tag{3}$$

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 divided by the frequency of the signal in hertz.

3.6.2 Bearing constraints

TCAS's bearing constraint error is $\pm$ 10 degrees from the estimated bearing [7, 18]. If a bearing measurement exceeds the bearing error constraint, the track coasts or drops. The bearing estimate from TCAS is the average of the first three

bearing reportings. From that bearing estimate, TCAS develops a track for the intruding aircraft.

With the interrogation replies sent from a ground station, the spoofed aircraft bearing reflects the ground station's relative bearing to the target aircraft. If the bearing change exceeds the 5 degrees threshold from the projected bearing, the simulation terminates with a constraint failure. The simulations use $\pm$ 5 degrees due to TCAS's bearing estimate standard deviation of 5 degrees [7]. Additionally, the simulations add the bearing change to the bearing average if the target aircraft turns left or right. This accounts for the target aircraft movements and the effect on the reported bearings from the spoofed aircraft.

3.6.3 Diverging range test

There are two requirements with the range test [7]. The first is the diverging range test.

The spoofed aircraft must not diverge from the target aircraft or TCAS drops the intruding aircraft. TCAS-FIE program measures this requirement by calculating the range rate using Eq. 4 [19]. Essentially, the aircraft must always gaining distance on one another versus separating.

$$\text{Range Rate} = \text{Spoofed Velocity} * \cos(\theta_1) + \text{Target Velocity} * \cos(\theta_2) \quad (4)$$

θ_1 is the measured angle between the spoofed aircraft's heading and the closing vector between the spoofed aircraft and target aircraft. θ_1 is always zero, as the ground station's signal takes the most direct path to the target. 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 changes at each measurement. Figure 4 provides a visual for this measurement process.

If the range rate is 0 or positive, TCAS-FIE marks the aircraft as converging. The target aircraft continues tracking the spoofed aircraft. Contrarily, if the range rate is negative, the individual simulation ends in error. Diverging aircraft cannot have an RA reported [13]. Additionally, a diverging aircraft track possibly drops from the target aircraft's TCAS system.

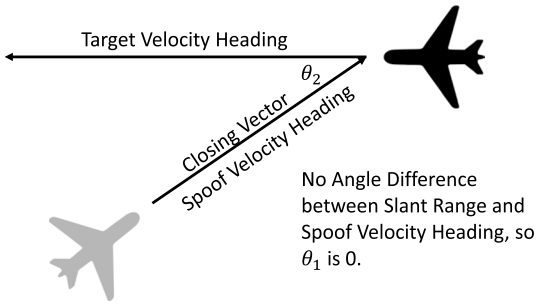

Fig. 4 Closing vector: A visual to show the angles between the spoofed aircraft (gray) and target aircraft (black) headings (color figure online)

3.6.4 TAU range test

The next range test is the TAU range test. TAU is the horizontal measurement that determines the necessity of a TA or RA. TAU is the number of seconds until the impact or closest point of approach. TCAS-FIE uses Eq. 5 to calculate TAU with each reply [7, 20]:

$$\text{TAU} = \frac{r - \frac{\text{SMOD}^2}{r}}{rdot} * 3600 \tag{5}$$

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 [7]. *rdot* is the range rate. Using range rate and the *SMOD* modifier, the TAU calculation in TCAS-FIE is:

$$\begin{aligned}\text{TAU} &= \frac{r - \frac{\text{SMOD}^2}{r}}{rdot} * 3600 \\ &= \frac{r - \frac{9}{r}}{\text{Spoof Velo} + \text{Target Velo} * \cos(|180 - \text{Target Heading} + \text{Spoof Heading}|)} * 3600\end{aligned} \tag{6}$$

If the TAU calculation is less than the 35-second threshold, the ground attacker successfully meets the range requirement, and TCAS triggers an RA. If TAU is greater than the 35-second threshold, the process of UF and DF 0 interrogations and replies continue.

3.6.5 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. This is always true as the ground attacker copies the altitude of the target aircraft from each reply.

4 Validation and verification

This section presents simulations that focus on the validation and verification of the processes and tests within TCAS-FIE. The simulation tests include the positioning/tracking process, the bearing constraint check, and the range test failure requirement.

4.1 Positioning and tracking

The following example of positioning and tracking accuracy is for one particular set of variables; however, it maintains across all sets. This simulation has a starting distance of 30 miles and 45,000 feet altitude. The (x,y,z) coordinate set for this example is (112005.71414, 112005.71414, 45000). These coordinates are arbitrary, and the

process is identical despite the starting location. The starting bearing is 270 degrees. The initial reply arrives with the spoofed aircraft inserted with a bearing of approximately 45 degrees. After a 5.416566 second interrogation period, the target aircraft turns left 1 degree. 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 original 0.000735s, mathematically, the position updates to:

$$\begin{aligned} x &= 112005.71414 + (888\text{ft/s} * 0.000735\text{s} * \sin(270)) \\ &= 112005.06146 \\ y &= 112005.71414 + (888\text{ft/s} * 0.000735\text{s} * \cos(270)) \\ &= 112005.71414 \end{aligned} \tag{7}$$

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

$$\begin{aligned} x &= 112005.06146 + (888\text{ft/s} * 5.416566\text{s} * \sin(269)) \\ &= 107195.8834 \\ y &= 112005.06146 + (888\text{ft/s} * 5.416566\text{s} * \cos(269)) \\ &= 111921.7696 \end{aligned} \tag{8}$$

Using the new (x,y,z) coordinates, the distance between the target aircraft and the ground station is 161348 feet. TCAS-FIE's code produces the same value, shown in the code readout below, demonstrating that it accurately tracks and updates aircraft positioning based on speed, time, and bearing. constraint.

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

4.2 Bearing constraint

The bearing constraint verification/validation test uses the same relative location as the positioning/tracking test. The bearing measurements are accurate, as shown by the verified and validated tracking process. The bearing constraint's verification and validation ensure TCAS-FIE stops when a bearing reporting exceeds ± 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 ± 5 degrees. The following code printout from TCAS-FIE shows the bearing exceeds the constraint.

```
Interrogation will arrive to False Aircraft position at 1.566139e+01 seconds.
    New Bearing of False Aircraft is 3.705223e+01 degrees
    Projected Bearing Exceeded
```

4.3 Range test failure

Using the same coordinates as the previous simulations, the range test's verification and validation occur. The bearing changes to 45 degrees, simulating an aircraft moving away. 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, so it is diverging. The code printout below illustrates the simulation terminating due to diverging aircraft.

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

5 Results and analysis

This section details the overall results of the 555,000 simulations. The analysis includes general statistics and more in-depth descriptive statistics to gain a proper understanding of false injection viability. Lastly, with detailed analytical results, the section presents a threat heat map of locations representing the highest risk of a successful, false injection attack.

5.1 Requirements for success

The following subsection details the simulation success requirements. These include interrogation/reply, range, and bearing requirements. Altitude is not a requirement for success because the spoofed aircraft's altitude reflects that of the target's reported altitude.

5.1.1 Interrogation and reply requirements

Bearing and TAU measurements are necessary for false injection success. Bearing and TAU calculation require at least three interrogations and subsequent replies. After three interrogations and replies, the target aircraft calculates TAU and bearing for RA determination. Thus, for success, the simulation requires at least four interrogations and replies.

5.1.2 Range requirements

The two success requirements of the range test in the simulation are the diverging range test and the range TAU calculation. If a range closure rate of fewer than 10 feet per second occurs, the simulation terminates. Additionally, the simulation is successful if TAU is less than 35 seconds, there are at least four interrogations and replies.

5.1.3 Bearing requirements

A successful simulation occurs if the spoofed aircraft bearing change is less than 5 degrees from the projected bearing path until RA issuance. If a bearing change over 5 degrees occurs, the simulation terminates.

5.2 Initial results

This subsection discusses the simulations' initial results with a focus on the end of simulation TAU calculations.

5.2.1 TAU average

Each simulation calculates the final TAU value upon failure. TCAS-FIE writes the TAU value for each of the 500 simulations in a set. Further processing averages the ending TAU values for each set. The sets with an average TAU value $\leq$ to 35 seconds are successful. The overall success of the 555,000 trials is 32.6305%. Upon inspection, the most useful variables in displaying simulation success are range and starting relative bearing. Figure 5 displays the TAU averages. The x-axis is the starting relative bearing between the target aircraft and the ground station. Table 3 shows the altitude scheme for each line in Fig. 5.

In Fig. 5, the horizontal black line indicates the TAU threshold of 35 seconds. Lines below this threshold indicate a starting relative bearing, altitude, and range combination that 50% of the time successfully satisfy all required TCAS tests. Most TAU values fall above the minimum 35-second TAU threshold, as evident by the chart. TAU decreases and success increases as altitude and range lower.

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 in-depth analyses each set's descriptive statistics: skewness, kurtosis, and standard deviation. Lastly, the

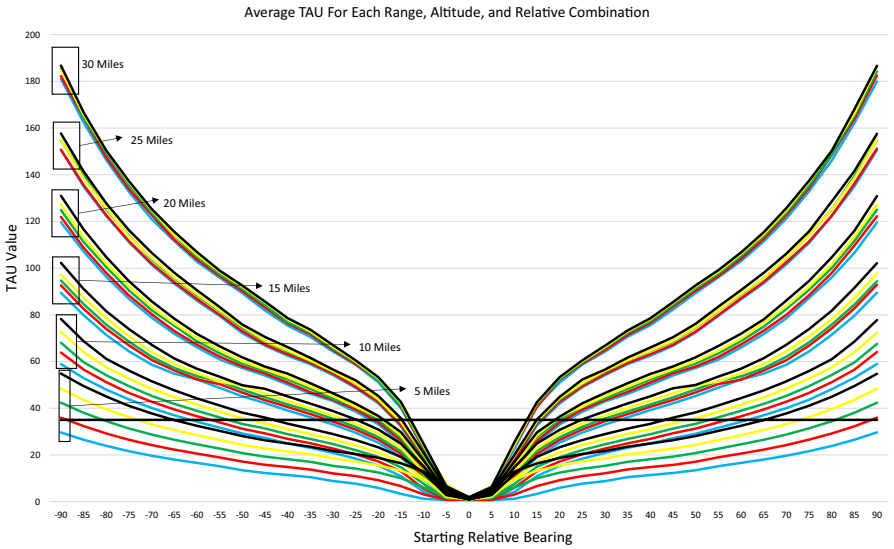

Fig. 5 First-Look TAU Values: Each line represents a different range and altitude pair. The lines represents the TAU value as relative bearing increases and decreases (color figure online)

Table 3 Figure 5 color legend

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

section discusses the transformation of non-normal data sets to meet normal distribution criteria.

5.3.1 Skewness

Skewness is the representation of the asymmetry within a data set [21]. A normally distributed data set has a skewness value of 0. If the skewness value is negative, the data distribute more to the mean's left. Additionally, the tail of the left side is longer than the right side. In contrast, if the skewness value is positive, the data distribute more to mean's right, and the right tail is longer.

West et al. [22] set the skewness guidelines for normally distributed data as 0 ± 2.1. Equation 9 shows the equation for skewness.

$$\text{Skewness} = \frac{\sqrt{N * (N-1)}}{N-2} \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^3}{N}}{\sigma^3} \tag{9}$$

The detailed analysis determines the skewness value for each set of 500 simulations. Figure 6 shows all skewness values with the thresholds of [-2.1, 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 it describes the tail heaviness compared to an even normal distribution [23]. A kurtosis value greater than 3 represents leptokurtic data, implying that the distribution tails are heavy compared to normal distribution. A kurtosis value of less than 3 represents playtkurtic data, implying that the distribution tails are thinner compared to a normal distribution curve. The kurtosis value for normal distribution is three and known as mesokurtic. Equation 10 calculates the kurtosis of data.

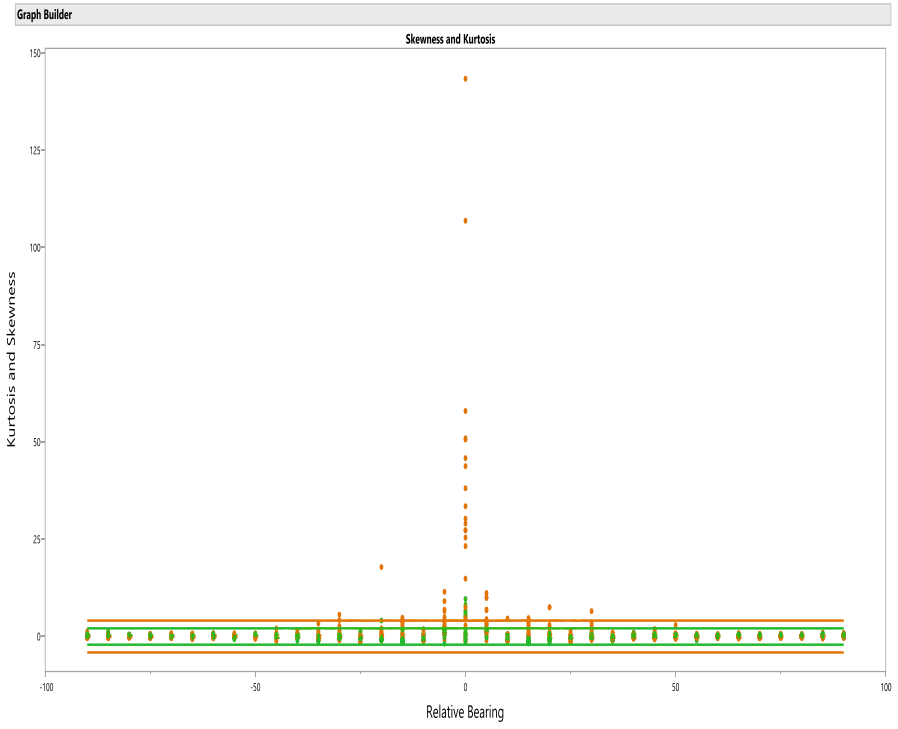

Fig. 6 Original Kurtosis and Skewness values: orange represents kurtosis values, and green represents skewness values (color figure online)

$$\text{Kurtosis} = \sum_{i=1}^{N} \frac{\frac{(X_i - \bar{X})^4}{N}}{\sigma^4} \tag{10}$$

In data that has occasional data outliers, excess kurtosis is the standard measurement. The excess kurtosis value for normal distribution is 0 [24]. West et al. [22] 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 detailed analysis determines the kurtosis value for each set of 500 simulations. Figure 6 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 with kurtosis or skewness values that exceed recommended thresholds require transformation. Osborne recommends using the Box-Cox transformation as it provides multiple transformation options for data, choosing the option that best transforms the data from non-normal to normal distribution [25]. He provides Eq. 11, the equation used to transform each data point:

$$\text{Box-Cox Transform} = \frac{x^{\lambda} - 1}{\lambda} \tag{11}$$

The detailed analysis determines λ by trial and error of different λ values [25]. The λ value chosen is the one that provides skewness and kurtosis values closest to 0.

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 outliers transform to data sets that meet normality considerations. Figure 7 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.

$$\text{P(TAU} \leq 35) = \frac{35 - \mu}{\sigma} \tag{12}$$

The Z-score calculated compares to a Z-table that lists the appropriate probability for the Z-score. The Z-score accurately depicts the successful false injection probabilities from a certain distance, altitude, and relative bearing.

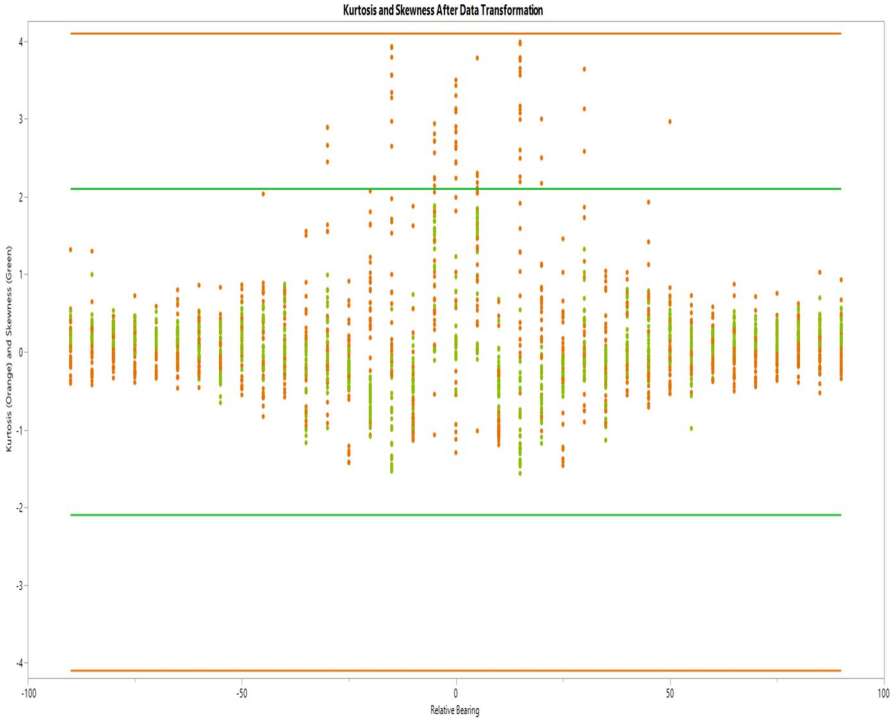

Fig. 7 Kurtosis and Skewness After Data Transformation: Orange represents kurtosis values, and green represents skewness values (color figure online)

5.3.5 Threat map

The false injection probabilities allow the creation of an accurate threat heat 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.

Figure 8 represents the threat map for an aircraft at 45,000 feet. 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 threat heatmap provides pilots with an accurate understanding of the distances and relative bearings vulnerable to a false injection at 45,000 feet altitude.

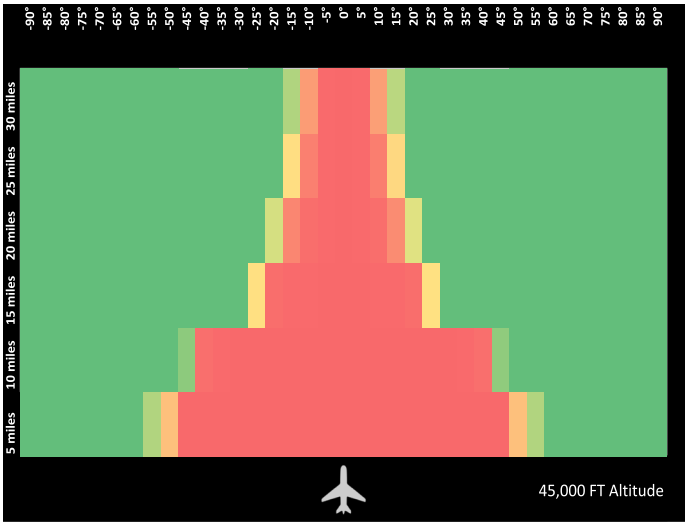

Fig. 8 45,000 feet Threat Map: Threat map for ranges and relative bearings at 45,000 feet (color figure online)

In the event of a TCAS anomaly in flight, the maps provide the pilot an extra tool to determine between system failure due to outside influence or just mechanical system failure.

A bearing specific aspect from the map is that a 0-degree relative bearing from the target aircraft to the ground-based attacker presents the perfect scenario for false injection. If the attacker times the Mode S responses correctly, false injection attacks are always successful with a 0-degree relative bearing.

A range specific aspect from the map is the closer, an attacker is horizontal to the target aircraft, the more successful the false injection attack is. If an aircraft is close enough, i.e., 5 miles out, the TAU calculation always falls within the ≤ 35 seconds RA issuance window.

6 Discussion

The following section discusses the overall security impact of a false injection attack against aircraft. Additionally, the authors present solutions to mitigate the vulnerability and capability for an attacker to successfully complete a false injection attack.

6.1 Security impact

Berges et al. [1] proposed and successfully created TCAS Mode S messages. Following on, the authors of this paper orchestrated the requirements to use those messages 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 paper. 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. The future work subsection explores possible solutions for future research.

7 Conclusion

This research introduced a novel method for a ground-based adversary to attack an operational aircraft's critical safety system (TCAS). The research goal is to time Mode S messages, simulating a moving aircraft, resulting in the insertion of a spoofed aircraft onto the target's TCAS. The ultimate goal, triggering an RA, requires the spoofed aircraft to adeptly satisfy the received signal power test, the range test, the altitude test, and the bearing constraint requirements. Additionally, the spoofed aircraft needs four successful replies. TCAS-FIE covers a variance of ranges, altitudes, and starting relative bearings.

After the completion of 555,000 simulations, Sect. 5 provided fundamental and detailed descriptive statistics analysis yielding the predictive threat heat maps for each altitude tested. These maps offer situation awareness to pilots in time of uncertainty with the TCAS system. The results show that a false injection attack is successful under certain range, altitude, and bearing circumstances.

This paper aims to enhance the knowledge of TCAS vulnerabilities, specifically, the false injection vulnerability. Several companies and agencies rely on the use of the TCAS system with 100% integrity. Additionally, this paper aspires to drive research into TCAS false injection solutions.

7.1 Future work

The implemented false injection attack creates the foundation and should provide the motivation for additional research. The next three research areas should be on possible solutions proposed by the authors, interrogation/reply periodicity, and verification of the created threat maps with the discussed time between interrogations and replies.

7.1.1 Proposed solutions

A mitigation strategy for the proposed false injection vulnerability requires securing the TCAS message generation process. The TCAS specification requires the system to accept any received message from a correctly addressed aircraft [5]. A method to increase integrity and message security would rely on a distributed voting algorithm, where the sender communicates its current air picture, to include aircraft positioning data, to surrounding aircraft. Any discrepancies would require actions to validate the

sender's authenticity. Further, this allows the verification of aircraft positioning data, further enhancing the viability of a particular aircraft's current TCAS picture.

A potential area of exploration to curb ground-based false injection attacks is the altitude processing by TCAS. TCAS uses the altitude reported in Mode S messages by placing the aircraft at the reported altitude. 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 [7].

7.1.2 Interrogation/reply periodicity

Interrogations and replies have mandated timelines [10]. Technical specifications for Mode S include 132.75 microseconds between the first interrogation pulse and the first interrogation reply pulse. The accuracy of this timing specification requires verification. This mandated delay allows the possibility of a false injection. Without the delay, the ability to falsely inject a spoofed aircraft becomes difficult and improbable. Accurately measuring the delay requires an operational TCAS system. The delay becomes observable during the communication process.

7.1.3 Real-world implementation

In addition to verifying interrogation and reply periodicity, the developed message timing and threat maps require validation with real-world systems. With technical specifications and other open-source documents, this paper developed threat maps. TCAS-FIE simulations calculate TAU measurements for each data set of range, altitude, and relative bearing. Additionally, TCAS-FIE calculates the required timing for each message. An operational SDR, antenna, and target TCAS can test the threat map and timing developed.

References

1. Berges Paul M, Reed Jeffrey H (2019) Exploring the vulnerabilities of traffic collision avoidance aystems (TCAS) through software defined radio (SDR) exploitation. Master's Thesis, Virginia Tech, Blacksburg, Virginia, United States
2. Federal Aviation Administration (2020) Air traffic By numbers

3. Federal Aviation Administration (2011) Introduction to TCAS II
4. Chappell Sheryl L, Billings Charles E, Kozon Thomas E (1989) Pilots' use of a traffic alert and collision-avoidance system (TCAS II)in simulated air carrier operations Volume I: Methodology, Summary, and Conclusions
5. John H, Robert M, Richard D (2020) Traffic collision avoidance system: threat actor model and attack taxonomy. In: Hanáková L, Socha V (eds) 2020 New trends in civil aviation (NTCA), Service Center, Piscataway, NJ, pp 17–26. https://doi.org/10.23919/NTCA50409.2020
6. Smith Matthew, Strohmeier Martin, Harman Jon, Lenders Vincent, Martinovic (2019) Safety vs. security: attacking avionic systems with humans in the loop
7. Radio Technical Commission for Aeronautics (2008) Minimum operational performance standards for traffic alert and collision avoidance system (TCAS), Version 1
8. Muñoz César, Narkawicz Anthony, Chamberlain James (2013) A TCAS-II Resolution advisory detection algorithm
9. Mica Workshop (2019) Mode S surveillance principle
10. Federal Aviation Administration (1983) U.S. National Aviation Standard for the mode select Beacon System (MODE S)
11. Welch JD, Orlando VA (1983) Traffic Alert and Collision Avoidance System (TCAS): A functional overview of minimum TCAS II. Lincoln Laboratory, Massachusetts Institute of Technology, Massachusetts, United States
12. Boeing, (2014) The boeing next-generation 737 family - productive. Progressive, Flexible, Familiar
13. Harman WH (1989) TCAS: a system for preventing midair collisions. Lincoln Lab J 2:437–458
14. Paul I (1999) Pilot's handbook of aeronautical knowledge, 4th edn. McGraw Hill, New York, pp 32–36
15. John VD, Leo W (1991) Data link test and analysis system/TCAS monitor user's guide
16. Shaw Joseph A (2013) Radiometry and the Friis transmission equation. Am J Phys 81:33–37
17. Wolff Christian Free-Space Path Loss (FSPL). https://www.radartutorial.eu/01.basics/Free-Space%20Path%20Loss.en.html#. Accessed 20 Oct 2020
18. Wood ML (1985) TCAS II ATCRBS Surveillance algorithms. Lincoln Laboratory, Massachusetts Institute of Technology, Massachusetts, United States
19. Avionics Department (2013) Electronic warfare and radar systems engineering handbook. 4th edn. Naval Air Warfare Center Weapons Division, Point Mugu, pp 48–52
20. Livadas C, Lygeros J, Lynch NA (2000) High-level modeling and analysis of the traffic alert and collision avoidance system (TCAS). Proceedings of the IEEE 88
21. Doane David P, Seward Lori E (2011) Measuring skewness: a forgotten statistic? J Stat Ed 19
22. West S, Finch J, Curran P (1995) Structural equation models with non-normal variables: problems and remedies
23. Decarlo Lawrence T (1997) On the meaning and use of Kurtosis. Psychol Methods 2:292–307
24. Hae-Young Kim (2013) Statistical notes for clinical researchers: assessing normal distribution using Skewness and Kurtosis. Restor Dent Endod 38(1):52
25. Osborne Jason (2010) Improving your data transformations: applying the box-cox improving your data transformations: applying the box-cox transformation. Pract Assess Res Eval 15:12