USAFTPS-TIM-19A-02

A LIMITED DEMONSTRATION OF ADS-B SECURITY

BRANDON C. BURFEIND, Capt, USAF
Project Manager & Pilot

BEN P. BOWMAN, Capt, USAF
Project WSO

BRET M. CUNNINGHAM, Maj, USAF
Project Pilot

E. KEKOA CABERTO, Capt, USAF
Project Engineer

RYAN M. FORYSTEK, Capt, USAF
Project Pilot

J. ADAM MCKENZIE, Capt, USAF
Project Engineer

NOVEMBER 2019

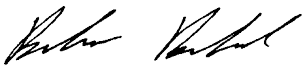
TECHNICAL INFORMATION MEMORANDUM

412TH TEST WING
EDWARDS AIR FORCE BASE, CALIFORNIA
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

This technical information memorandum (USAFTPS-TIM-19A-02, *A Limited Demonstration of ADS-B Security*) was submitted under job order number MT19A200 by the Commandant, USAF Test Pilot School, Edwards Air Force Base, California 93524-6843.

Approved for public release: distribution unlimited.

Prepared by:

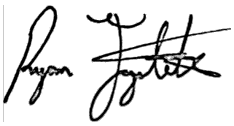


BRANDON C. BURFEIND
Capt, USAF
Project Manager / Project Pilot

BRET M. CUNNINGHAM
Maj, USAF
Project Pilot

BEN P. BOWMAN
Capt, USAF
Project WSO

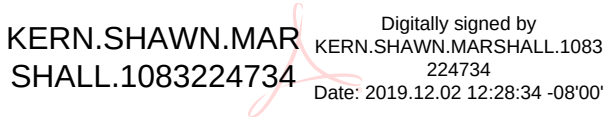
E. KEKOA CABERTO
Capt, USAF
Project Engineer



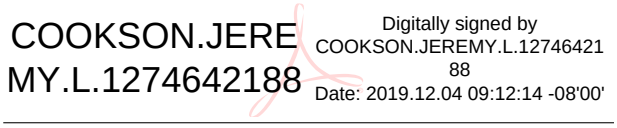
RYAN M. FORYSTEK
Capt, USAF
Project Pilot

J. ADAM MCKENZIE
Capt, USAF
Project Engineer

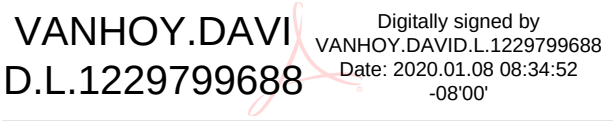
This memorandum has been reviewed and is approved for publication:



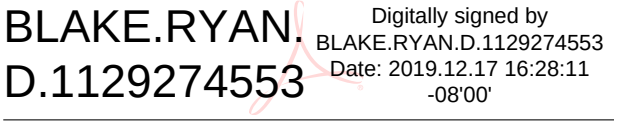
SHAWN M. KERN
NH-IV, DAF
Staff Advisor, USAF Test Pilot School



JEREMY L. COOKSON
NH-IV, DAF
Technical Expert, USAF Test Pilot School



DAVID L. VANHOY
NH-IV, DAF
Technical Director, USAF Test Pilot School



RYAN D. BLAKE
Col, USAF
Commandant, USAF Test Pilot School

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
30–11–2019	Technical Information Memorandum	17 Sep 2019 — 19 Sep 2019

4. TITLE AND SUBTITLE

HAVE CRYPTO
A Limited Demonstration of ADS-B Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Brandon C. Burfeind, Project Pilot
Bret M. Cunningham, Project Pilot
Ben P. Bowman, Project WSO
E. Kekoa Caberto, Project Engineer
Ryan M. Forystek, Project Pilot
J. Adam McKenzie, Project Engineer

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

412th Test Wing
Edwards AFB CA 93524-6001

8. PERFORMING ORGANIZATION REPORT NUMBER

USAFTPS-TIM-19A-02

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

Air Force Research Laboratory
Sensors Directorate
Wright-Patterson Air Force Base, OH 45433-7320

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: Approved for Public Release; distribution unlimited.

13. SUPPLEMENTARY NOTES

SC: 012100 CA: 412th Test Wing Edwards AFB CA Print this document in COLOR.

14. ABSTRACT

This report presents the results of project Have Crypto, *A Limited Demonstration of ADS-B Security*. The lead developmental test organization was the Air Force Test Center, Edwards AFB, California. The executing test organization was the Have Crypto TMP team, part of Class 19A at the USAF Test Pilot School, Edwards AFB. Testing was conducted from 17 to 19 September 2019 and comprised of six sorties totaling 7.9 hours. Testing utilized a T-38C equipped with a RASCAL pod configured as an ADS-B transmitter, two custom receiver sites located in the San Bernardino Mountains, and multiple commercial ADS-B receivers located in the Antelope Valley. Testing was conducted in and around the R-2508 complex at altitudes from 10,000 to 30,000 feet and airspeeds between 250 and 450 knots. The first general test objective, addressing ADS-B confidentiality, was to determine the performance of a connectionless packet-switched key handoff mechanism. The second general test objective was to observe integrity vulnerabilities inherent to ADS-B.

15. SUBJECT TERMS

ADS-B, Confidentiality, Cybersecurity, Datalink, Encryption, IFF, Mode S, Spoofing, Transponder

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Bob Mills, AFIT/ENG
U	U	U	Same as Report	81	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x4527; robert.mills@afit.edu

This page was intentionally left blank.

EXECUTIVE SUMMARY

This report presents the results of project Have Crypto, *A Limited Demonstration of ADS-B Security*. The lead developmental test organization was the Air Force Test Center, Edwards AFB, California. The executing test organization was the Have Crypto test management project (TMP) team, part of Class 19A at the USAF Test Pilot School, Edwards AFB. Testing was conducted from 17 to 19 September 2019 and comprised of six sorties totaling 7.9 hours. Testing utilized a T-38C equipped with a Reconfigurable Airborne Sensor, Communication, and Laser (RASCAL) pod configured as an automatic dependent surveillance-broadcast (ADS-B) transmitter, two custom receiver sites located in the San Bernardino Mountains, and multiple commercial ADS-B receivers located in the Antelope Valley. Testing was conducted in and around the R-2508 complex at altitudes from 10,000 to 30,000 feet and airspeeds between 250 and 450 knots.

In 2019, the worldwide air traffic infrastructure was in the late stages of transition from legacy interrogate and reply based transponder systems to ADS-B based systems. ADS-B systems relied on precise position information from global navigation satellite systems and required aircraft to transmit their unique identification, state, and position. ADS-B promised the availability of high fidelity air traffic information, however, position and identification data were not secured via authentication, verification, or encryption. This lack of security in the ADS-B protocol allowed non-participants to observe and collect data on both government and private flight activity. It also caused vulnerabilities to cyber operations against air defense and air traffic control infrastructure via spoofing, deletion, and modification of ADS-B tracks.

The first general test objective, addressing ADS-B confidentiality, was to determine the performance of a connectionless packet-switched key handoff mechanism. Connectionless packet-switching involves splitting data into multiple sets and transmitting without acknowledgement from the receiver. The system under test (SUT) was the key handoff functionality of a proposed ADS-B encryption protocol. Data collected included error as a function of transmit range, destructive interference, receiver antenna type, and direction of flight. Signal density, and therefore interference, was qualitatively set by controlling line-of-sight (LOS) to the dense air traffic environment of the Los Angeles basin. Each receiver was equipped with a directional and omni-directional antenna.

While limitations prevented accomplishment of all objectives, connectionless packet switching was demonstrated. Packet error ratio (PER) and handoff error ratio (HER) were the determinants of packet switching performance. PER was the ratio of incorrectly received packets to the total number of packets transmitted. HER was the same ratio, but for a handoff (set of 12 sequential packets). The PER for ADS-B varied from 30% at 10 nautical miles (NM) to 84% at 100 NM. Interference environment, antenna pattern, and direction of flight were significant factors in determining PER. Lower interference, outbound flight, and a directional antenna all resulted in lower PER than the alternatives. HER could not be measured directly due to transmitter and receiver limitations; it was analytically calculated using measured PER. Testing for ranges less than eight NM was not accomplished due to a restricted test timeline. The lack of data within eight NM impacts implementation decisions; many key handoffs could occur at short range.

The second general test objective was to observe integrity vulnerabilities inherent to ADS-B. The SUT was the Mode S - Extended Squitter (Mode S-ES) protocol, the most widely used implementation of ADS-B. The RASCAL pod was configured to transmit false ADS-B tracks (limited to restricted airspace) while receiver sites positioned at various locations observed the effects of spoofing-based deception operations.

The second general test objective was met; the test team successfully observed spoofing operations to include identity transfer and multi-aircraft scenarios. Observations were made by using commercial ADS-B receivers as well as crowdsourced flight tracking websites. Testing also observed that a spoofed track may appear differently depending on the technology stack used to aggregate, process, and display the data.

This page was intentionally left blank.

TABLE OF CONTENTS

This page was intentionally left blank.

LIST OF ILLUSTRATIONS

This page was intentionally left blank.

LIST OF TABLES

This page was intentionally left blank.

INTRODUCTION

This report presents the results of project Have Crypto, *A Limited Demonstration of ADS-B Security*. The lead developmental test organization was the Air Force Test Center, Edwards AFB, California. The executing test organization was the Have Crypto test management project (TMP) team, part of Class 19A at the USAF Test Pilot School, Edwards AFB. Testing was conducted from 17 to 19 September 2019 and comprised of six sorties totaling 7.9 hours. Testing utilized a T-38C equipped with a Reconfigurable Airborne Sensor, Communication, and Laser (RASCAL) pod configured as an automatic dependent surveillance-broadcast (ADS-B) transmitter, two custom receiver sites located in the San Bernardino Mountains, and multiple commercial ADS-B receivers located in the Antelope Valley. Testing was conducted in and around the R-2508 complex at altitudes from 10,000 to 30,000 feet and airspeeds between 250 and 450 knots.

BACKGROUND[1]

Basics

The worldwide air traffic infrastructure was in the late stages of transition from legacy interrogate and reply based transponder and identification friend or foe (IFF) systems. Replacing and/or supplementing the legacy systems were ADS-B based systems. ADS-B systems relied on precise position information from global navigation satellite systems (GNSSs) augmented with space-based augmentation systems (SBASs) and required aircraft to transmit position, state, and unique identification at update rates exceeding once per second. ADS-B was both an extension and subset of secondary surveillance radar (SSR) Mode S (figure 1).

ADS-B was a follow on to modes A and C, allowing selective addressing of individual aircraft via a unique International Civil Aviation Organization (ICAO) address. Mode S - Extended Squitter (Mode S-ES) was a portion of the Mode S protocol which implemented ADS-B for most aircraft and transmitted on 1090 MHz. The extended squitter (Mode S-ES) format lengthened the message from 56 to 112 bits, making space for the additional data transmitted for ADS-B. Testing focused on Mode S-ES and the term ADS-B in this document is utilized for the Mode S-ES protocol. The other subset of ADS-B, Universal access transceiver (UAT), was a portion of ADS-B utilized to relieve frequency congestion for light aircraft and was not part of this test.

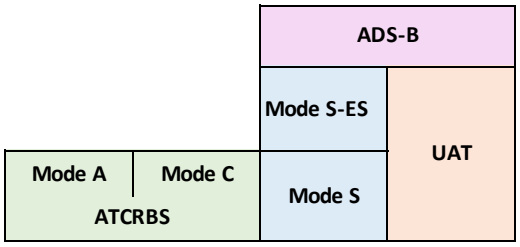


Figure 1 ADS-B Technology

A list of common definitions frequently utilized throughout this report is available in appendix I.

Motivation

ADS-B technology offered significant safety and efficiency benefits to the air transport industry. ADS-B shared identification, location, and other flight information between aircraft and ground control entities as well as between participating aircraft. ADS-B offered improvement over previous IFF systems in fidelity and scope of data transmitted.

The widespread availability of precise location and identification information for ADS-B participating aircraft created an environment ripe for exploitation. Many instances of military and intelligence missions being adversely affected by ADS-B transmissions have been documented. Figures 2-4 show various instances of sensitive missions being publicly tracked via ADS-B.

This test supported potential implementation of a confidentiality protocol for Mode S-ES. The novelty of this protocol was in the use of security principle decomposition to create a lightweight and interoperable

[1] Burfeind, Mills, Nykl, Betances, Sielski, *Confidential ADS-B*, 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2019.

scheme allowing full ADS-B participation while maintaining confidentiality and/or privacy. It used existing asymmetric and format preserving encryption (FPE) together with unidirectional key passage to enable a confidential mode of operation. Potential implementation required the receipt of multiple packets containing a portion of the encryption key. This test supported that implementation by determining the feasibility of the key handoff mechanism.

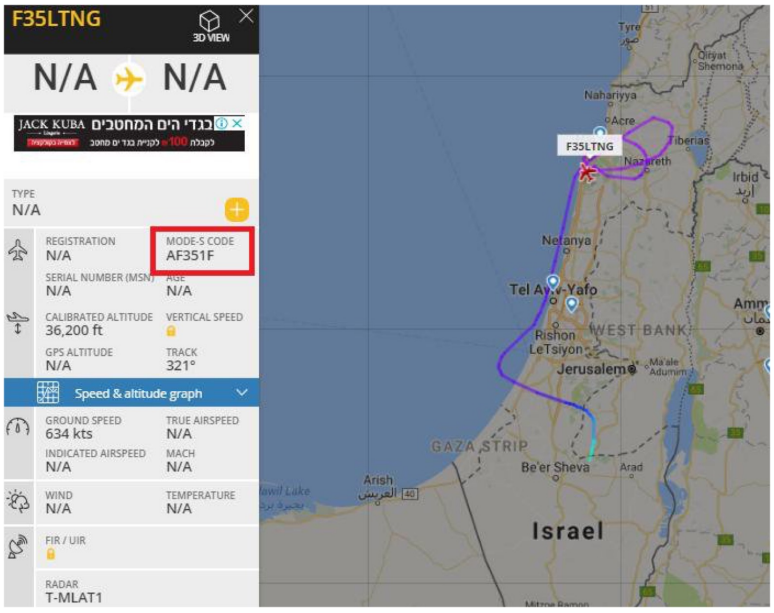


Figure 2 Israeli F-35 – US ICAO Address

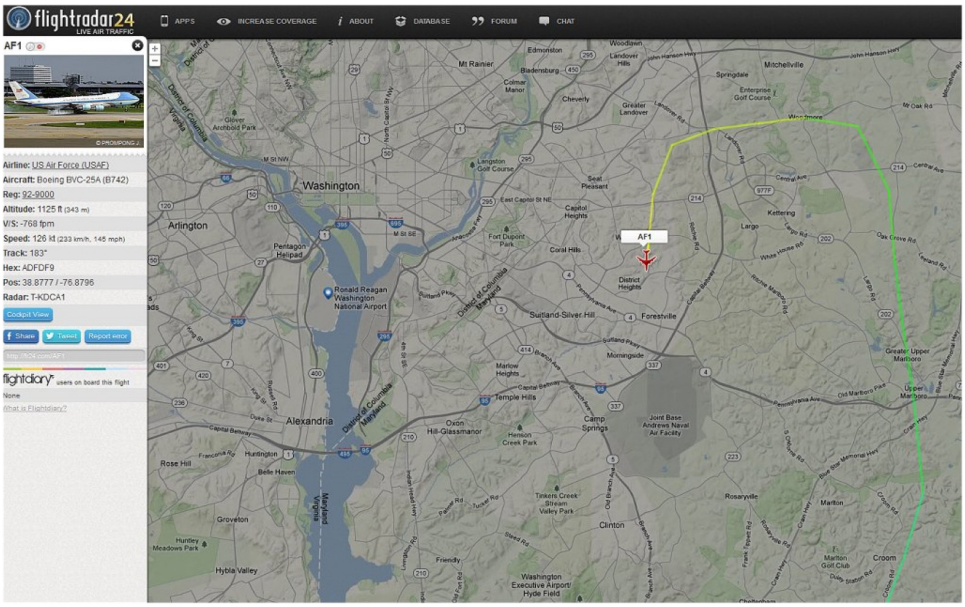


Figure 3 VC-25 – *Air Force One* Callsign

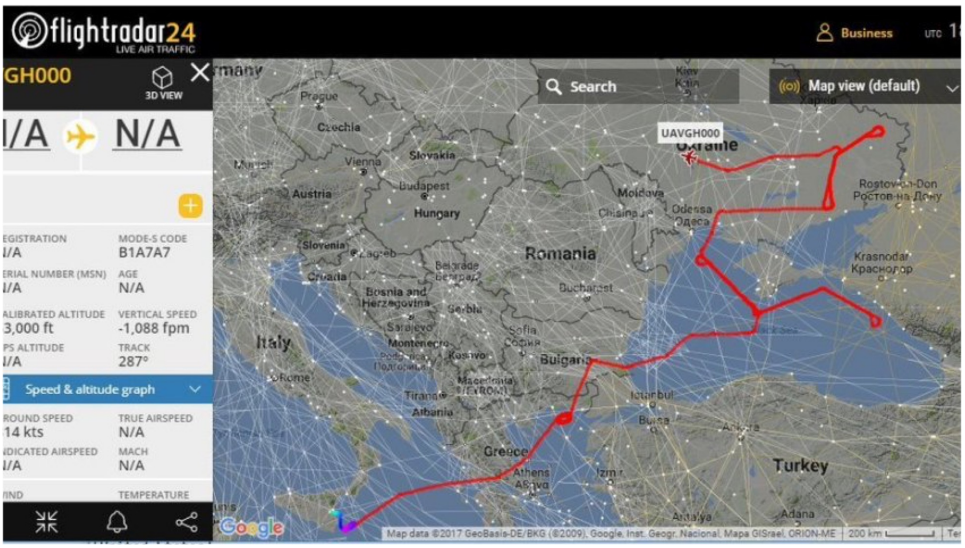


Figure 4 RQ-4 – Over the Black Sea

Security Principles

Traditional information security discussion used the *CIA Triad* to frame security best practices:

- *Confidentiality*: information accessible by entities with a 'need to know'
- *Integrity*: information originated from an authenticated source and was not tampered with, changed, or destroyed en route to the using entity
- *Availability*: the service(s) which the information serves or was part of were available to authorized users when required/desired

While ADS-B did not implement security features, figure 5 further decomposes these security principles as they might pertain to ADS-B.

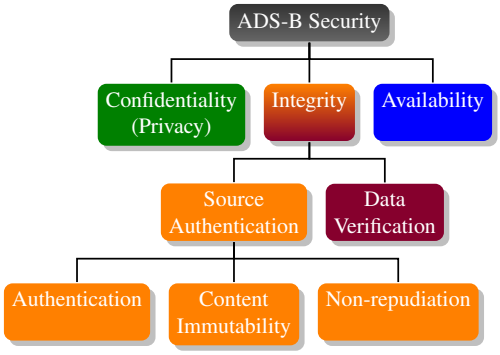


Figure 5 ADS-B Security Principles

ADS-B *confidentiality* was the concept that data would only be accessible to the intended entities. The implementation of confidentiality however did not imply authentication or verification. Dependent on system design, one could have had a confidential system in which an adversary could manipulate, remove, or insert false data.

The *integrity* of ADS-B data was uniquely decomposed into *source authentication* and *data verification*.

Source authentication ensured that data originated from, and could be attributed to a certain entity without modification. Source authentication did not give assurance that the received data was accurate. An authenticated aircraft could have inadvertently or maliciously sent false data.

Data verification was a subset of integrity discussed when using untrusted broadcast communications. Data verification ensured that the information transmitted was accurate. For example, data verification was used to ensure that the location reported by an ADS-B target was the true location of the aircraft or vehicle.

Data verification did not determine whether a message had been tampered with; it only tried to determine if the data were true.

Availability referred to assurance of service to users. Generally, ADS-B was designed to be available unless a known or scheduled outage existed.

The broadcast nature of ADS-B allowed layered independent security protocols to accomplish tailored objectives. Due to the emphasis on interoperability, this proposal for confidentiality was compatible with any number of physical layer techniques for authentication or verification.

Stakeholders, Adversaries, and Standards

Stakeholders

Various stakeholders were involved in the development, deployment, operation, and use of ADS-B. These entities had a common objective: *safe aircraft operations* regardless of aircraft type or operational objective. From that point, goals diverged and became operation or entity specific. These included efficiency, security, profitability, etc. Further stakeholder details are included in appendix B.

Adversaries

Two types of adversaries were commonly addressed in reference to ADS-B: active and passive. Active adversaries collected surveillance data directly related to a certain operation. Possible examples were foreign intelligence services tracking friendly military missions or a corporate competitor keeping tabs on a rival's movements. Passive adversaries on the other hand did not act with malicious intent, but unknowingly provided public data to those who did.

Current Standards

Radio Technical Commission for Aeronautics (RTCA) and European Organisation for Civil Aviation Equipment (EUROCAE) created, maintained, and updated standards for Mode S and ADS-B. ICAO and various civil aviation authorities (CAAs) implemented and/or augmented these standards.

Security Protocol

Data Encryption

Confidentiality of broadcast data required obfuscation via encryption. Format preserving encryption combined Advanced Encryption Standard (AES) security with the capability to handle legacy data formats of variable length. In the protocol under test, only the message field was encrypted. This allowed the system to selectively encrypt based on message type. For example, if a user was in an operating mode that masked identity, but did not deny location information, the transponder only encrypted packets that contained an *Aircraft Identification and Category* message.

ICAO Address Anonymization

Obfuscating the ICAO address required substituting a *session unique ICAO address (SUIA)* on all packets transmitted, even those not encrypted. For this implementation, a SUIA was randomly generated from a set of ICAO addresses set aside for this purpose. The SUIA implementation was intended to last for a single session, which was, at most, a single flight from avionics initialization to engine shutdown.

SUIA & Session Key Handoff

The use of symmetric encryption and unique identifiers required a method of sharing both an SUIA and a session symmetric key (SSK) between the participating aircraft and ground-based surveillance infrastructure. Given that ADS-B often had a high packet error ratio (PER) and was connectionless (no return data channel for acknowledgement), the packetized nature of the key handoff segment presented

a communications challenge. One solution was to resend the handoff packets a certain number of times, resulting in a high probability of successful segment reassembly.

Ground Infrastructure

A *secure software module* acted as a filter for incoming Mode S packets. Any packet that had a normal ICAO address and message type passed through unmodified. A packet with a SUIA had its address field replaced with the actual ICAO address. A packet that was encrypted had its address replaced and message field decrypted. This was then forwarded as a normal message to air traffic control (ATC) software.

FRUIT and PER

The aforementioned challenges of implementing a stateless key handoff demanded an in-depth analysis of connectionless packet-switching over the 1090 MHz binary pulse position modulated (PPM) channel. While all channels contain noise, 1090 MHz was unique in that there was no multiple access protocol, which meant that all transmitters could transmit at any time, in any direction, with any power. This interference was known as false replies unsynchronized in time (FRUIT), a phenomenon where overlapping waveforms caused packet errors. Especially useful to the development of the protocol under test was an analysis of how the FRUIT environment and range from antenna impacted the success of a key handoff.

Further details of the background for this test are in appendix B.

TEST ITEM DESCRIPTION

The system under test (SUT) for general test objective (GTO) 1 was the key handoff functionality of the ADS-B encryption protocol. The SUT for GTO 2 was the Mode S-ES protocol.

The test aircraft was a T-38C with a RASCAL pod attached on the centerline station. The RASCAL pod was controlled through an C-9492 electronic counter measures (ECM) panel installed in the front cockpit and a Getac tablet in the rear cockpit via an ethernet connection. The RASCAL pod contained hardware and software used to transmit ADS-B data. Details of each individual internal component of the pod are found in appendix A. The T-38C with RASCAL pod attached is seen in figure 6.

The Getac tablet computer used to control the RASCAL operated Matrix Laboratory (MATLAB) in the rear cockpit and connected to the RASCAL pod via ethernet. A MATLAB graphical user interface (GUI) provided initial setup cues and real-time functionality notifications in flight and allowed for testers to change spoofing parameters as desired for different scenarios. The tablet computer allowed testers to manipulate the content of ADS-B packets while ensuring the transmitted waveform was compliant with RTCA, DoD and air traffic control radar beacon system (ATCRBS), IFF, Mark XII/XIIA system program office (SPO) (AIMS) specifications. This flexibility allowed the test team to gather data regarding Mode S-ES PER and manipulate packets to execute spoofing operations. Aircraft location for range data was determined using a Dual XGPS160 SkyPro GPS Receiver connected to the Getac tablet via Bluetooth and integrated with MATLAB via the custom GUI.

Two receiver sites were established south of R-2508. The “high” FRUIT receiver site was on top of a tower on Strawberry Peak, exposed to FRUIT from air traffic in the Los Angeles (LA) basin to the south. The “low” FRUIT reciever site was on the north side of the San Bernardino mountains, masked from the LA traffic by intervening terrain. Additional details and terrain masking profiles of the two locations can be found in appendix A. Each receiver site consisted of one directional antenna and one omni-directional antenna. Transmissions were received by a software defined radio (SDR) and processed by a MATLAB program on a laptop computer. A picture of the setup at each receiver site can be seen in figure 7.

Commercial ADS-B receivers and crowdsourced ADS-B tracking applications were utilized as the receive element for GTO 2. Tablet computers and laptops were used to observe flights from three locations. The locations were Edwards Air Force Base (AFB), Kramer Junction, and Barstow. Additional details of the receiver locations can be found in appendix A.

Figure 6 T-38C with RASCAL Pod

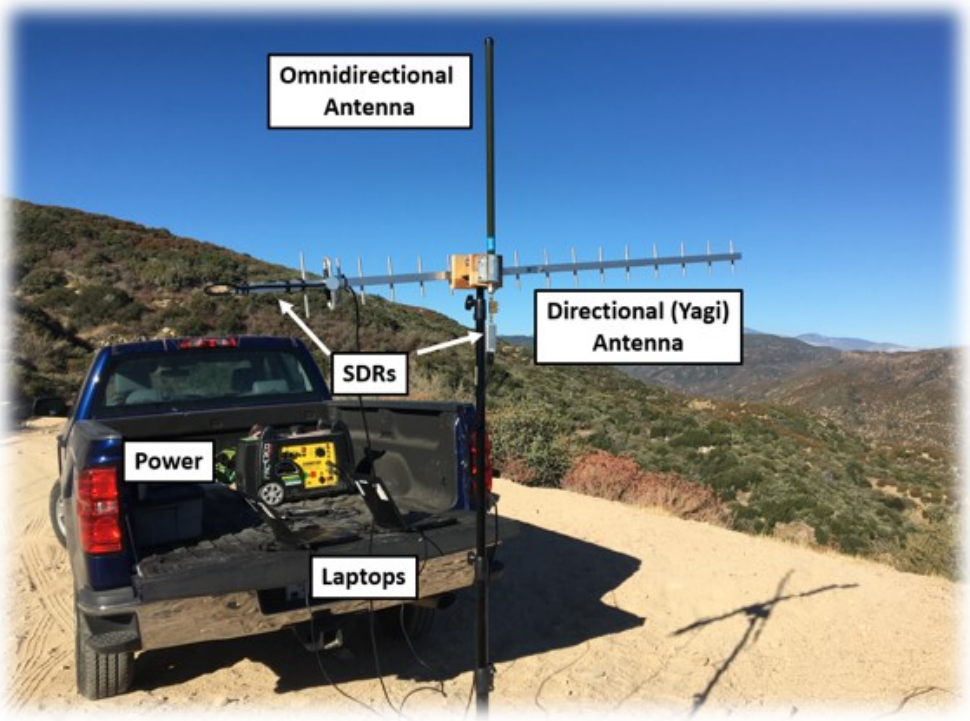


Figure 7 Receiver Site Setup

TEST OBJECTIVES

The first general test objective, addressing ADS-B confidentiality, was to determine the performance of a connectionless packet-switched key handoff mechanism. The first GTO was partially met. Specific test objectives (STOs) for GTO 1 were:

1. Demonstrate data transfer via connectionless packet switching on a binary PPM 1090 MHz channel.
2. Determine the post-cyclic redundancy check (CRC) PER of the Mode S-ES protocol in an open-air environment.
3. Determine the handoff error ratio (HER) of the secure key handoff protocol.
4. Compare analytical HER calculated from determined PER to flight-test determined HER.

The second general test objective was to observe integrity vulnerabilities inherent to ADS-B. The second GTO was met. The STO for GTO 2 was:

1. Observe the effects of real-time, airborne-transmitted Mode S-ES spoofing.

CONSTRAINTS AND LIMITATIONS

Limitations with the RASCAL pod's Getac tablet processing while running MATLAB restricted the pod's transmission rate. GTO 1 transmission rates were planned at 5, 10, and 100 packets per second to determine the effect of transmission rate on PER. The maximum sustainable transmission rate was approximately eight packets per second, therefore transmission rate could not be used as a factor for PER model creation. Performance was not determined as a function of transmission rate.

The receiver and its interaction with MATLAB were a limitation. After receiving packets for approximately one second, the receiver would process the transmissions and store the receive logs in MATLAB for approximately 0.7 seconds, during which time it would dump transmissions received in that period. This limitation, combined with the transmission rate limitation, made it impossible to receive the twelve consecutive packets required for a complete handoff. This prevented the test team from determining a twelve-packet HER and comparing the determined HER to the analytically calculated HER.

As a result of programmatic and scheduling delays, the test team was constrained to only three test days. This time constraint did not allow the test team to perform the full scope of planned ground tests which would have characterized PER from one to seven nautical miles (NM). As a result, the PER model was generated from 8 to 150 NM instead of the planned 1 to 150 NM. This is significant as many key handoffs would likely occur on the ground in the 1 to 7 NM range.

This page was intentionally left blank.

TEST AND EVALUATION

The first general test objective, addressing ADS-B confidentiality, was to determine the performance of a connectionless packet-switched key handoff mechanism. Connectionless packet-switching involves splitting data into multiple sets and transmitting without acknowledgement from the receiver. The SUT was the key handoff functionality of a proposed ADS-B encryption protocol. Data collected included error as a function of transmit range, destructive interference, receiver antenna type, and direction of flight. Signal density, and therefore interference, was qualitatively set by controlling line-of-sight (LOS) to the dense air traffic environment of the Los Angeles basin. Each receiver was equipped with a directional and omni-directional antenna.

While limitations prevented accomplishment of all objectives, connectionless packet switching was demonstrated. PER and HER were the determinants of packet switching performance. PER was the ratio of incorrectly received packets to the total number of packets transmitted. HER was the same ratio, but for a handoff (set of 12 sequential packets). The PER for ADS-B varied from 30% at 10 NM to 84% at 100 NM. Interference environment, antenna pattern, and direction of flight were significant factors in determining PER. Lower interference, outbound flight, and a directional antenna all resulted in lower PER than the alternatives. HER could not be measured directly due to transmitter and receiver limitations; it was analytically calculated using measured PER. Testing for ranges less than eight NM was not accomplished due to a restricted test timeline. The lack of data within eight NM impacts implementation decisions; many key handoffs could occur at short range.

The second general test objective was to observe integrity vulnerabilities inherent to ADS-B. The SUT was the Mode S-ES protocol, the most widely used implementation of ADS-B. The RASCAL pod was configured to transmit false ADS-B tracks (limited to restricted airspace) while receiver sites positioned at various locations observed the effects of spoofing-based deception operations.

The second general test objective was met; the test team successfully observed spoofing operations to include identity transfer and multi-aircraft scenarios. Observations were made by using commercial ADS-B receivers as well as crowdsourced flight tracking websites. Testing also observed that a spoofed track may appear differently depending on the technology stack used to aggregate, process, and display the data.

PERFORMANCE OF A CONNECTIONLESS KEY HANDOFF MECHANISM

The first general test objective, addressing ADS-B confidentiality, was to determine the performance of a connectionless packet-switched key handoff mechanism.

Overall Test Methods

Two receiver sites were established in the San Bernardino mountains at locations intended to have different FRUIT rates, such that one was a relatively “high” FRUIT while the other was “low” in relation.

FRUIT level was used as a qualitative factor due to the great difficulty in characterizing the FRUIT environment. Even with knowledge of all air traffic positions out to the horizon, it would have been necessary to determine transmit power, transmit antenna characteristics, attitude, transmit rate, and transmit timing to quantify the FRUIT environment. This was beyond the scope of this test. Each receiver site possessed an omni-directional antenna and a directional antenna aligned with the flight path of the test aircraft. SDR based receivers logged the ADS-B packets received from each antenna. Further details of the receiver sites can be found in the test item description and in appendix A.

The test aircrew flew the ground track depicted in figure 8 to vary slant range between 8 and 150 NM. After the second sortie it was determined that sufficient data had been collected at slant ranges greater than 100 NM, and on subsequent sorties the aircraft remained between 8 and 100 NM. The aircraft flew at maximum endurance airspeed to maximize sortie duration.

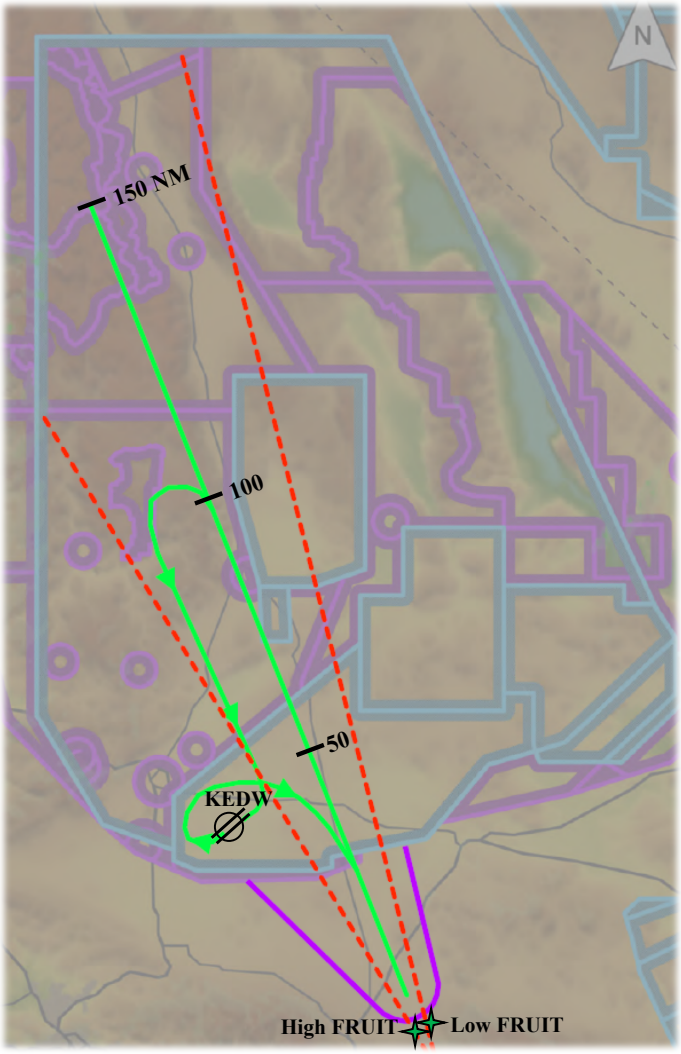


Figure 8 Test Ground Track

An overall results file containing the slant range, FRUIT environment, antenna type, direction of flight (inbound or outbound), and success/failure to receive the transmitted packet was generated by comparing the transmission log to the four receiver logs. Of note, transmitter limitations caused transmission rate to be constant, therefore results files did not account for this as a factor. A linear regression model was used to create the PER model over the range of 8 to 150 NM. The message field was decoded to extract the attempt and sequence number from each packet and determine when a complete handoff had been received. Additionally, HER was analytically computed from determined PER using the following probability based model:

$$HER = 1 - (1 - PER)^{12}$$

Further details of the data analysis are found in appendix E.

Connectionless Packet Switching

The test objective was to demonstrate data transfer via connectionless packet switching on a binary PPM 1090 MHz channel. This was designed to demonstrate that bits could be divided among multiple packets, transmitted, and each packet in a sequence could be received at a receiver site, in accordance with the above

methodology.

Test Results

During testing, data transfer via connectionless packet switching on a binary pulse position modulated 1090 MHz channel was demonstrated. Although receiver software limitations prevented reception of 12 consecutive packets in sequence, all 12 packets were received over multiple handoff attempts, as the flight data in table 1 displays. This indicated that reconstruction at the receiver was possible. The assumption was made that a production representative system would be capable of buffering received packets which would allow reconstruction once all required packets were received.

Table 1 Key Handoff Packet Receipt

Time	Attempt	Sequence
22:23:52.17	16	1
22:23:40.04	10	2
22:23:40.20	10	3
22:24:10.06	22	4
22:25:41.71	62	5
22:23:40.72	10	6
22:23:40.90	10	7
22:24:44.49	36	8
22:23:43.28	11	9
22:25:37.03	59	10
22:25:47.40	65	11
22:23:41.75	10	12

Mode S-ES Packet Error Ratio

The test objective was to determine the post-CRC PER of the Mode S-ES protocol in an open-air environment. The output of this test objective was a model which displayed PER versus range for any combination of factors which affected PER.

Test Results

A model of PER for slant ranges from 8 to 150 NM was created from the overall results file. The model analyzed PER for four different factors: range, FRUIT level, antenna type, and direction of flight. Due to previously discussed limitations, transmission rate was held constant and not considered as a factor. The results gathered during flight test had a minimum statistical confidence level of 0.9954, however due to the qualitative characterization of FRUIT, this confidence level gave an estimate of the population mean only for test day conditions. Details of statistical analysis are in appendix E.

Assumptions

Implementation of the test resulted in two factors which impacted test results: direction of flight and receiver processing delays.

Figure 9 displays the impact of direction of flight on PER results. Direction of flight was not expected to have an impact on PER as the transmit antenna was designed to transmit with equal power on all azimuths. However, the direction of flight was the most statistically significant factor for this implementation in determining PER, with a value of 0.31 at 10 NM when travelling outbound and 0.84 when flying inbound. It was unknown if this difference was caused by an asymmetric transmit pattern from the antenna or aircraft

installation interference. The issue was not a result of Doppler effects as the aircraft velocity would result in a Doppler shift of approximately 500 Hz around the 1090 MHz signal, not significant enough to create receiver issues. During spoofing test flights, the test team at receiver sites noticed that spoofed aircraft tracks, which were not present while the aircraft flew towards their location, immediately appeared after the host aircraft turned and flew outbound.

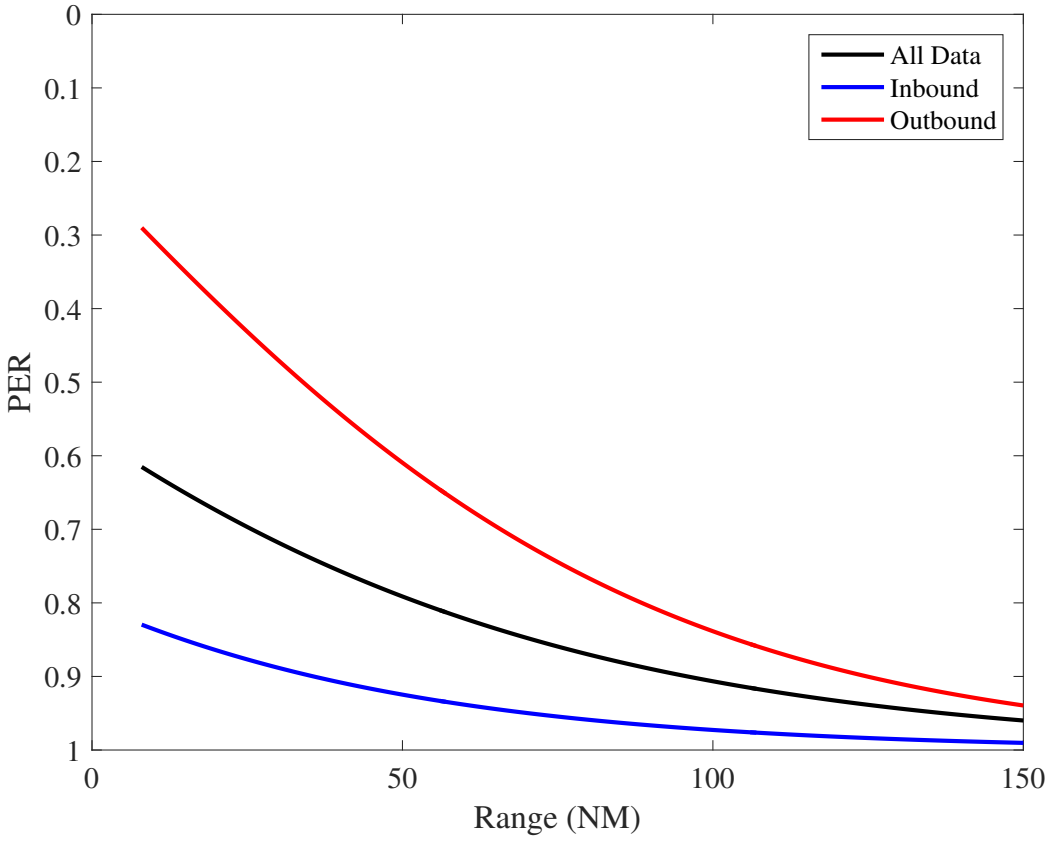


Figure 9 PER Results: Range and Direction of Flight

All additional plots and tables in this section will only include outbound data in the calculations to better represent an appropriate implementation. Plots showing overall results with inbound data included can be found in appendix D.

Receiver processing delay also impacted data. As a result of receiver processing delay, when the transmitter was directly connected to the receiver the measured PER was approximately 0.41. This occurred because the receiver collected transmissions for approximately one second, then took 0.7 seconds to process the data while receiving no other transmissions. To approximate a system without these constraints, an assumption was made that the 0.7 seconds of lost transmissions would have the same PER characteristics as the one second immediately prior. During this 0.7 second period, the aircraft travels less than 0.1 NM. This correction factor was applied to the data analysis and is reflected in all plots presented in this report, including those in appendix D.

PER Model

As seen in figure 10, the low FRUIT receivers had a better PER when compared to the high FRUIT receivers. A summary of results at select ranges is shown in table 2. These results match expectations, as the added traffic in the LA basin created more noise. For the multi-factor effect plots seen in figure 11, these

results remain similar in that for a given antenna type the low FRUIT site has a better PER than the high FRUIT site.

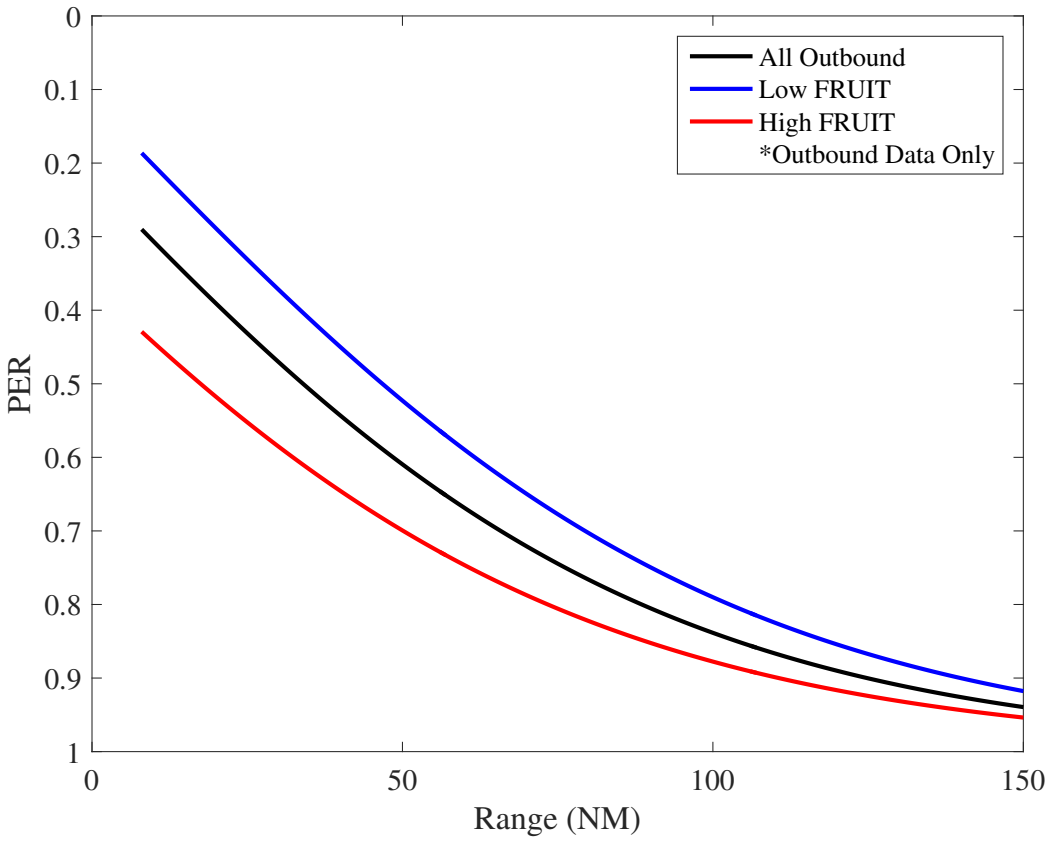


Figure 10 PER Results: Range and FRUIT

The directional antenna achieved a lower PER than the omni-directional antenna, which can be seen in figures 11 and 12 and in table 2. However, the type of antenna used for the receiver had less impact than FRUIT location. It was expected that the directional antenna would achieve better results than the omni-directional antenna, especially at the high FRUIT location. The directional antenna received signal with a higher power in the appropriate angular cone, therefore the impact of FRUIT from the LA basin was expected to be reduced for a directional antenna. While this was true to an extent, figure 11 shows that the impact of FRUIT was still high, even for a directional antenna.

The model did not extend to ranges of 1 to 7 NM due to constraints preventing ground test execution. These ranges are important as many key handoffs in any future implementation of this protocol would happen on the ground in the 1 to 7 NM range. **Conduct testing within ranges expected for initial ADS-B key handoff (R1)**.

Table 2 Packet Error Ratio for Varying Factors and Ranges

Factors	**10 NM**	**50 NM**	**100 NM**
All Outbound	0.307	0.700	0.839
Low FRUIT	0.204	0.523	0.790
High FRUIT	0.444	0.699	0.878
Omni Antenna	0.348	0.639	0.853
Directional Antenna	0.267	0.580	0.824
Low FRUIT / Omni	0.247	0.557	0.809
Low FRUIT / Dir	0.161	0.488	0.772
High FRUIT / Omni	0.482	0.724	0.889
High FRUIT / Dir	0.407	0.674	0.866

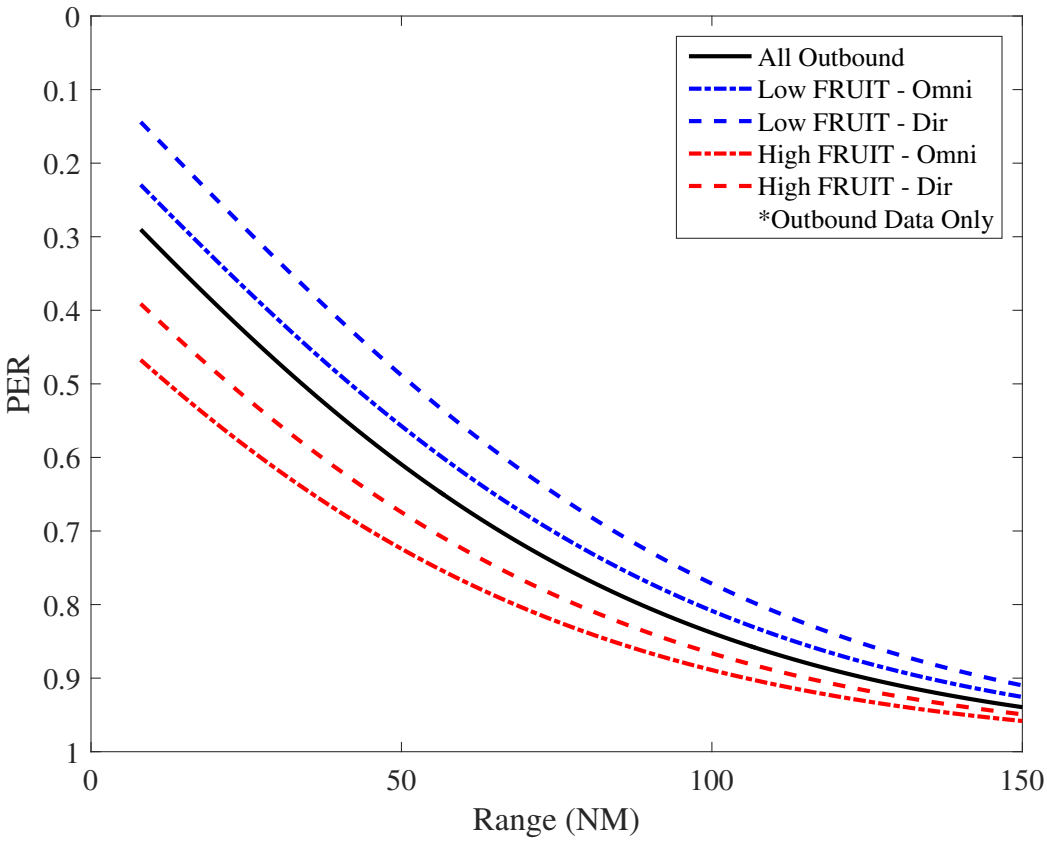


Figure 11 PER Results: Range, FRUIT, and Antenna

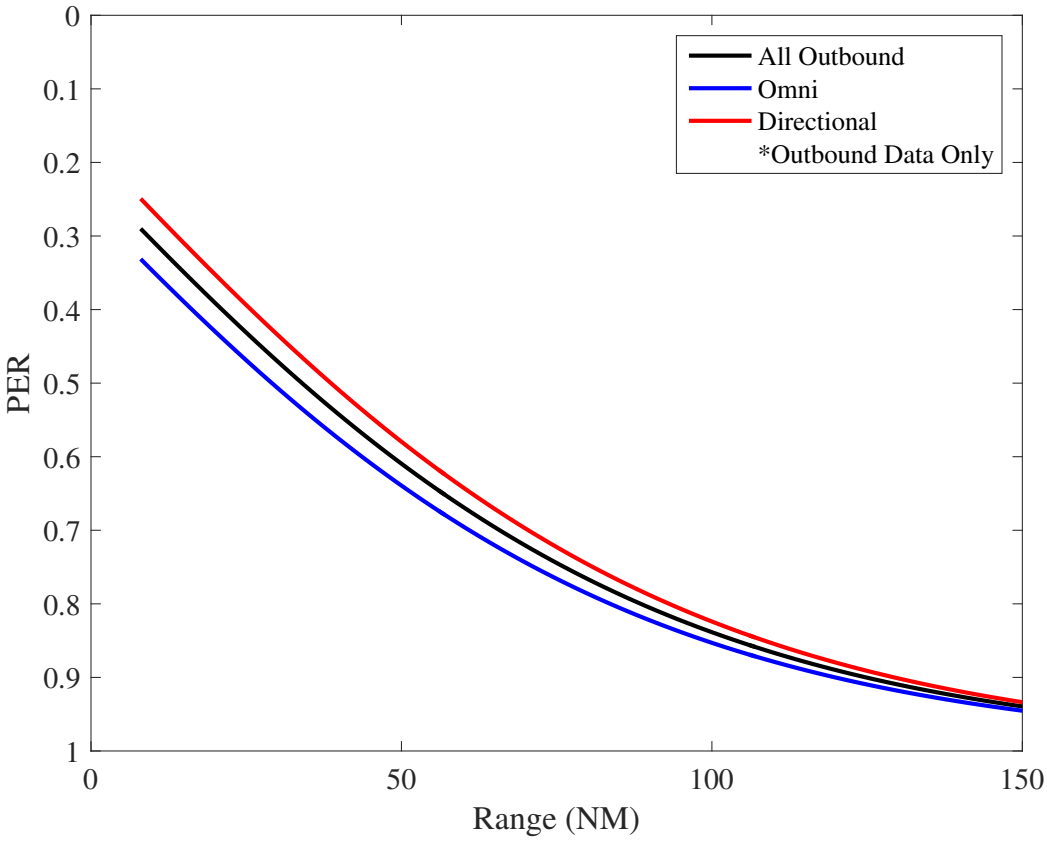


Figure 12 PER Results: Range and Antenna

Key Handoff Error Ratio

The test objective was to determine the HER of the secure key handoff protocol. A handoff was considered successful when all 12 packets were received in a single attempt.

Test Results

As a result of the previously detailed receiver processing limitations and transmission rate constraints the handoff error ratio determined from flight was 1.0. There was no occurrence where 12 consecutive packets in a sequence were received. **Reconfigure transmit and receive elements of the sytem under test to allow continuous transmission, reception, and processing of ADS-B messages (R2).**

Comparison of Analytical Handoff Error Ratio to Determined Handoff Error Ratio

The test objective was to compare analytical HER calculated from determined PER to flight-test determined HER. The flight test determined HER was calculated per the previous test objective, and analytical HER was calculated based on PER and the equation in the test methodology section.

Test Results

As the flight test determined HER was 1.0 due to test limitations, a comparison between the two methods of determining HER cannot be completed. However, the analytical HER was still calculated based on the determined PER. It is likely that the determined model would be the same as the analytical model based on statistical independence.

With the relatively high PERs, a HER of greater than 0.999 at 10 NM was calculated for all inbound results. When analyzing all outbound data, a HER of 0.988 was calculated at 10 NM, with the value improving when using low FRUIT data, as seen in figure 13. HER results at multiple ranges are shown in table 3.

These HER results highlighted an issue with the proposed implementation. Based on the HER, a large number of handoffs would likely need to be attempted in order to ensure receipt of all packets.

Table 3 Handoff Error Ratio for Multiple Factors and Ranges

Factors	**10 NM**	**20 NM**
All Outbound	0.988	0.998
Low FRUIT / Omni	0.967	0.992
Low FRUIT / Dir	0.879	0.967
High FRUIT / Omni	1.000	1.000
High FRUIT / Dir	0.998	1.000

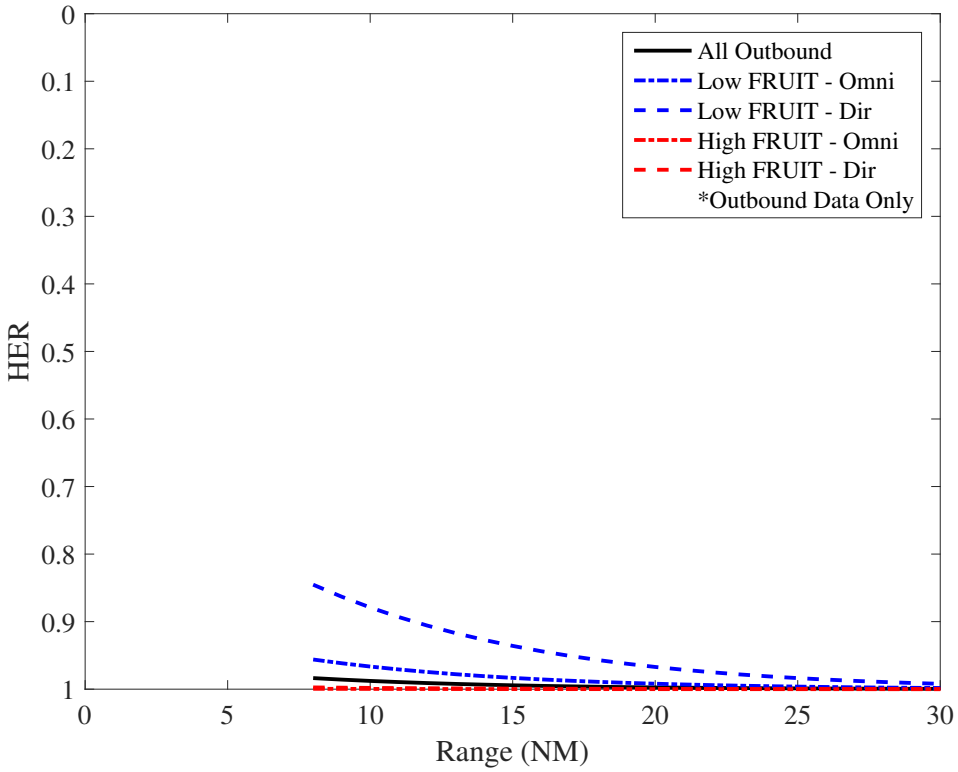


Figure 13 HER Results

INTEGRITY VULNERABILITIES INHERENT TO ADS-B

The second general test objective was to observe integrity vulnerabilities inherent to ADS-B.

Mode S-ES Spoofing

The test objective was to observe the effects of real-time, airborne-transmitted Mode S-ES spoofing.

Test Methods and Conditions

Two scenarios were utilized to observe the effects of real time ADS-B spoofing. The first scenario observed the ability of an aircraft to change its identity by utilizing divergent and convergent self-generated realistic ADS-B tracks. The second scenario observed the ability of a single ADS-B transmitter to generate multiple false tracks.

Identity Transfer

To observe an outward identity transfer by utilizing spoofed ADS-B tracks, the test aircraft flew a profile depicted in figure 14. False tracks corresponding to the flight profiles in figure 15 were generated by the transmit pod. All spoofed tracks were confined to restricted areas within the R-2508 complex with ATC coordination. Three receiver site locations within line-of-sight of the test aircraft were used to observe ADS-B spoofing. At test initiation, the host aircraft began broadcasting ownship location with the ANDY 01 identity and a spoofed ADS-B track with the BURNR 01 identity. Identity data contained both callsign and ICAO address. At the point of divergence, the host aircraft ceased ownship ADS-B transmissions and began spoofing the ANDY 01 divergent track, while continuing to broadcast the spoofed BURNR 01 track. At the desired time and location the host aircraft converged with the spoofed BURNR 01 track and began broadcasting ownship location with the assumed BURNR 01 identity.

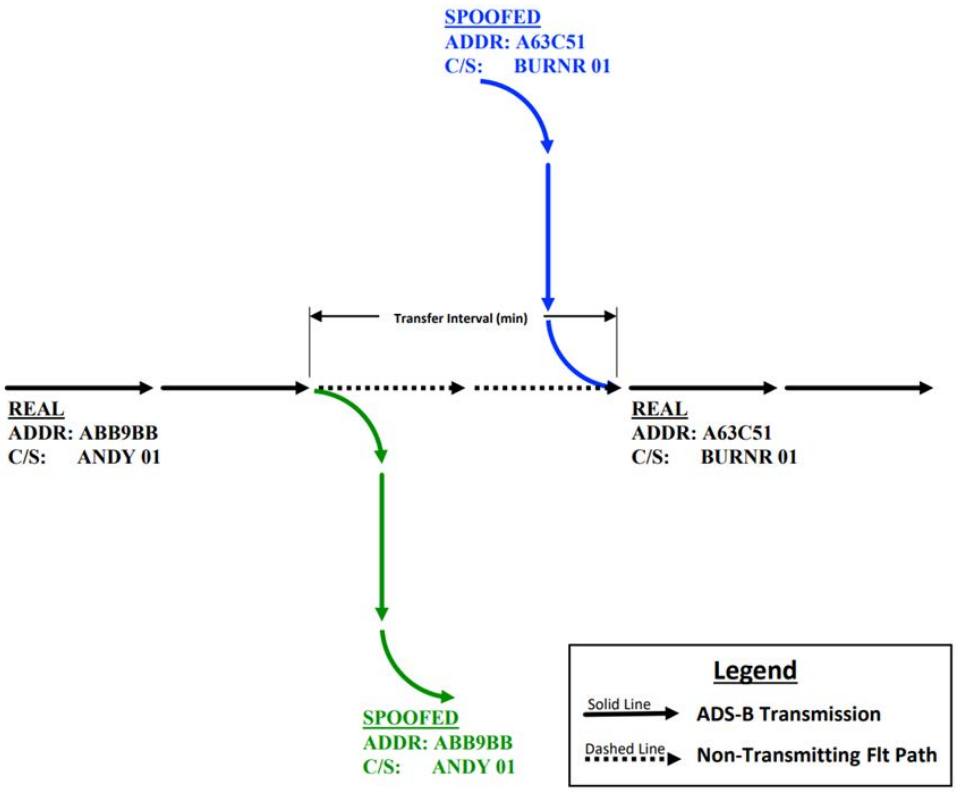


Figure 14 Spoofing Interactions Concept

Testing utilized three different transfer intervals, defined as the time from when the test aircraft ceased ownship ADS-B transmission to when it began ownship transmissions again after converging with the spoofed track. Testing occurred with intervals of 84 seconds, three minutes, or five minutes when flown at 450 knots ground speed (KGS). Additional test points were flown at speeds of 405 KGS and 360 KGS, with spoofed tracks groundspeed adjusted accordingly to account for the longer interval required at slower speeds. The test setup allowed the aircrew to choose an altitude offset for the converging spoofed track of either 2000 ft below, 3000 ft above, or no offset from initial ownship position. Testing followed the flight paths depicted in figure 15.

Multi-Aircraft Spoofing

An additional scenario, an eight-ship wall formation, was spoofed to demonstrate the ability of a single Experimental ADS-B Testbed System (EATS) pod to transmit a large number of false tracks. This test consisted of the test aircraft transmitting its ownship position as well as seven false tracks spread throughout the airspace with 2 NM spacing.

Data collection was performed by screen captures of ForeFlight™ paired with a Stratus 3 receiver. Additional screen captures were collected using FlightRadar24 and ADSBExchange on a laptop. These screen captures were recorded via native screen recording capability on each device.

Test Results

Identity Transfer

Two sorties were dedicated to spoofing scenarios. The test aircraft was able to change its identity with various false tracks used to ‘sell’ the change. The identity change scenarios are detailed in table 4.

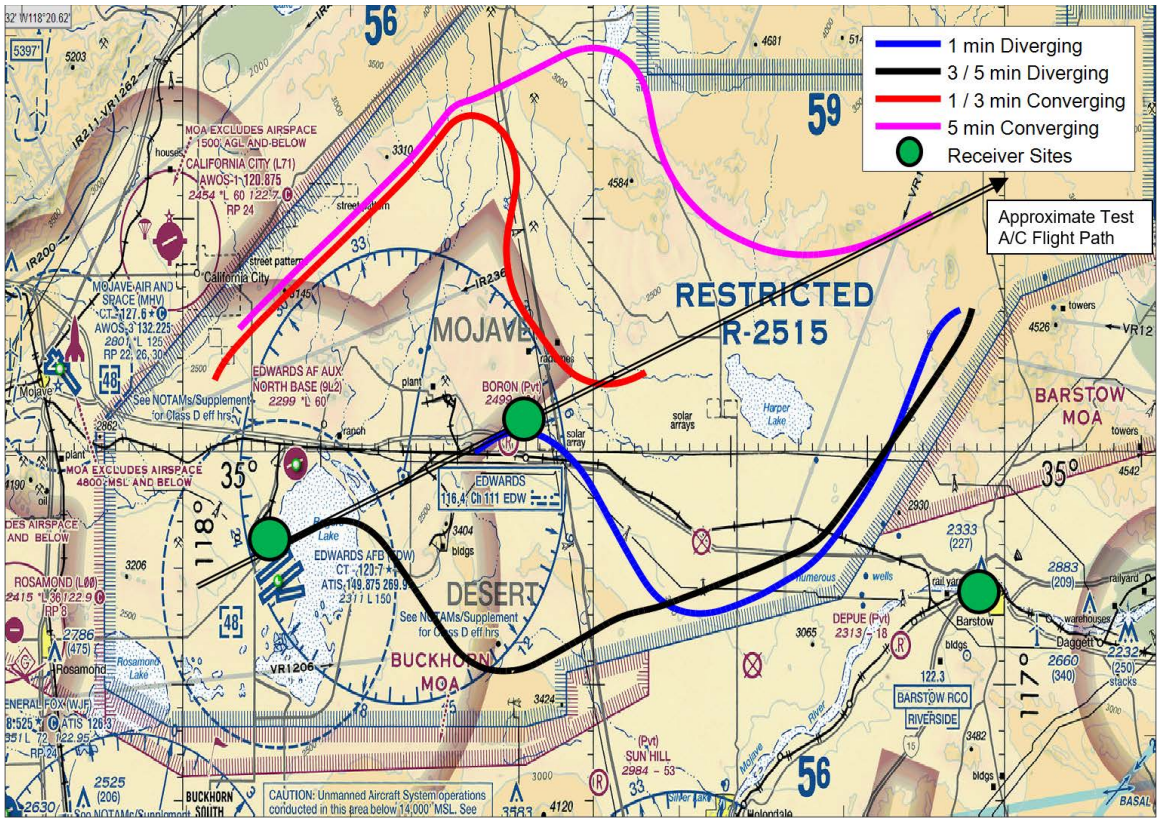


Figure 15 Spoofing Ground Tracks

Table 4 Conditions of Executed Spoofing Scenarios

Run	Convergence Interval	Average Ground Speed	Altitude Offset
1	200 sec	405 KGS	+3000
2	300 sec	450 KGS	-2000
3	93 sec	405 KGS	0
4	225 sec	360 KGS	-2000

The effects of spoofing varied between receivers. For example, ADSBExchange not only displayed the spoofed ADS-B tracks but also displayed the test aircraft's actual location when ownship position was not being transmitted. Using multilateration, ADSBExchange was capable of tracking the production transponder independently of the test ADS-B transmissions. The ADSBExchange capture in figure 17 observes this scenario as well as the successful spoofing of callsign and ICAO address. It was notable that not all systems possessed this capability, FlightRadar24 being one example. Figure 17 displays FlightRadar24 at the same time; it was only capable of displaying the spoofed tracks.

Figure 16 Identity Change: ANDY01 (top) to Not Transmitting (middle) to BURNR01 (bottom)

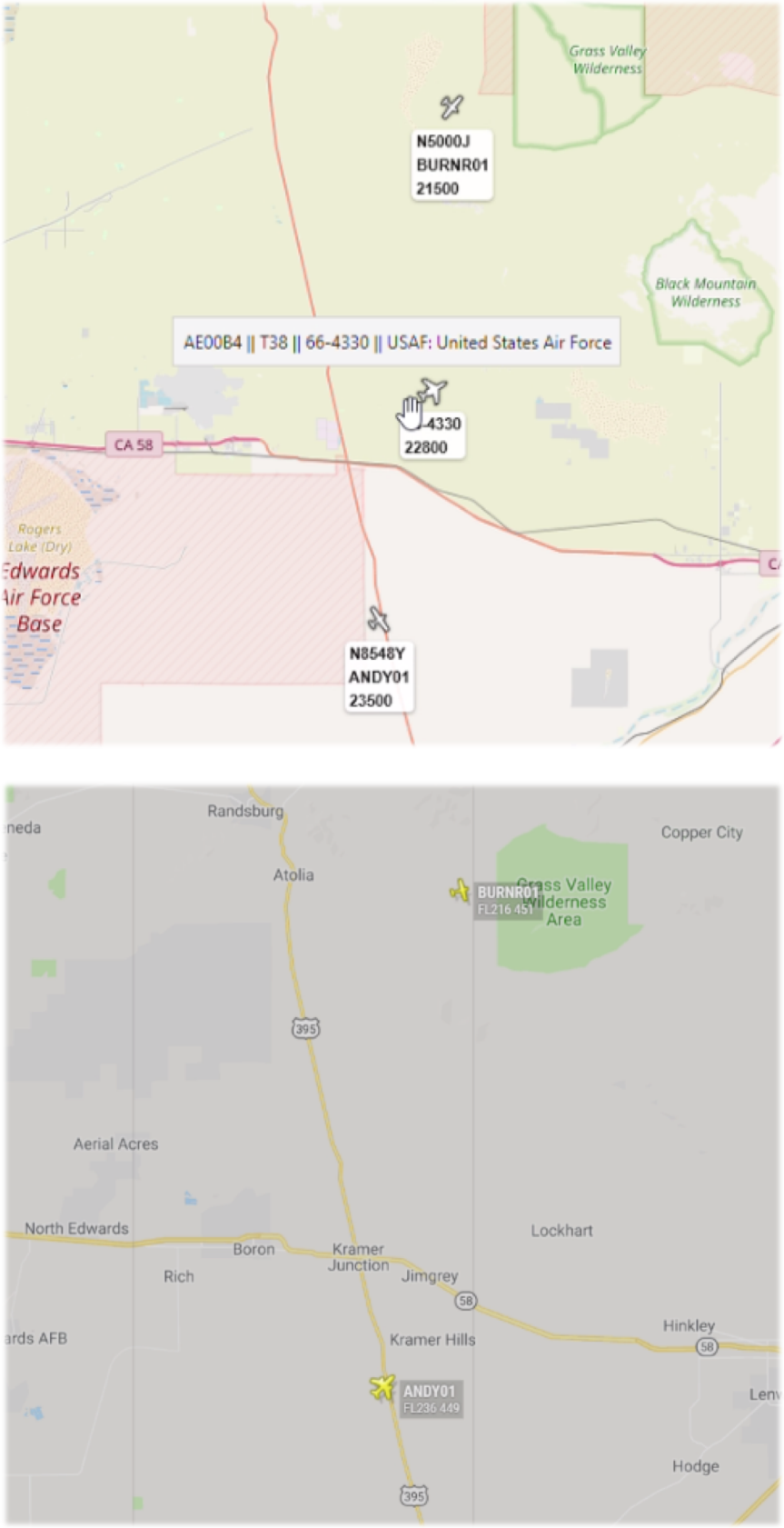


Figure 17 Comparison: ADSBExchange (top) and FlightRadar24 (bottom)

Multi-Aircraft Spoofing

The eight-ship wall scenario was executed twice by the test team. The ownship track and seven spoofed tracks were observed at the receiver sites, as shown in figure 18. With a maximum transmission rate of eight packets per second, the EATS transmitter was capable of transmitting a sufficient number of packets to credibly spoof seven additional aircraft.

Figure 18 FlightRadar24 Eight-Ship Wall

The eight-ship wall test point exposed effects of prediction algorithms used to display tracks by FlightRadar24. Figure 19 shows one member of the eight-ship wall that continued to track east (over Barstow) while the actual aircraft and other spoofed tracks flew west. This was likely an effect of intermittent reception and the prediction algorithms. There are many possible outcomes of how the spoofed track may appear depending on the technology stack used to interpret the data.

Figure 19 FlightRadar24 Location Prediction Error

This page was intentionally left blank.

APPENDIX A – DETAILED TEST ITEM DESCRIPTION

TRANSMIT COMPONENT

The Experimental ADS-B Testbed System consisted of an airborne transmitter and ground-based receiver. The EATS transmitter included a Department of Defense (DoD) AIMS compliant Mode S transmitter implemented with a SDR and integrated into a RASCAL pod for carriage on an F-16C/D, T-38C, or C-12J aircraft.

RASCAL Pod

The EATS airborne transmitter was located in a RASCAL pod. The RASCAL pod was a test asset developed by Test Pilot School (TPS) to rapidly move laboratory experiments to flight test. The RASCAL pod was a generic, unpopulated pod with power, space, communication, and control provisions for a wide variety of electro-optical (EO) and radio frequency (RF) experiments. It was designed for rapid installation and integration of sensors and equipment on location at a university or laboratory followed by flight test planning and execution. The RASCAL pod on the test T-38C can be seen in figure A1.

Test-specific components within the RASCAL pod included four NuWaves amplifiers, RF filters, couplers and splitters, an antenna, a SDR, and a power supply. Figure A2 depicts a block diagram of the EATS transmit components that were contained with the RASCAL pod.

Figure A1 T-38C with RASCAL Pod

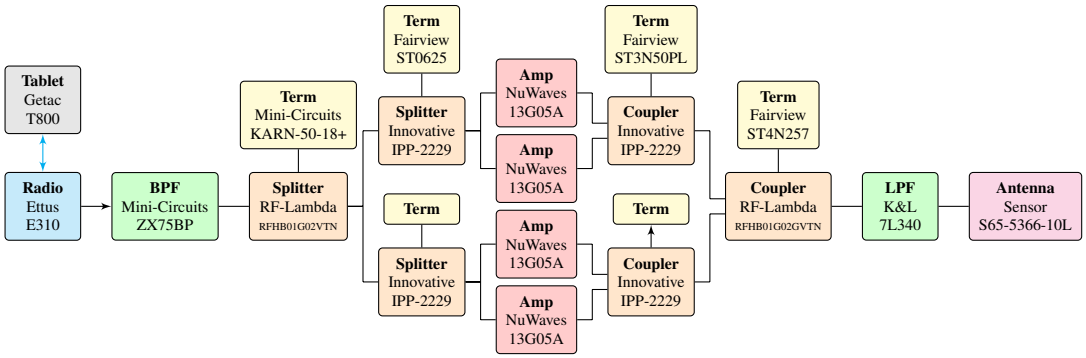


Figure A2 EATS Transmit Components

Getac Tablet

The primary RASCAL pod interface was a Getac T800 tablet in the rear cockpit connected to the pod using an ethernet cable. A MATLAB GUI provided initial setup cues and real-time functionality notifications in flight and allowed for testers to change spoofing parameters as desired for different scenarios. The tablet computer allowed testers to manipulate the content of ADS-B packets while ensuring the transmitted waveform was compliant with RTCA, DoD and AIMS specifications. This flexibility allowed the test team to gather data regarding Mode S-ES PER and manipulate packets to execute spoofing operations.

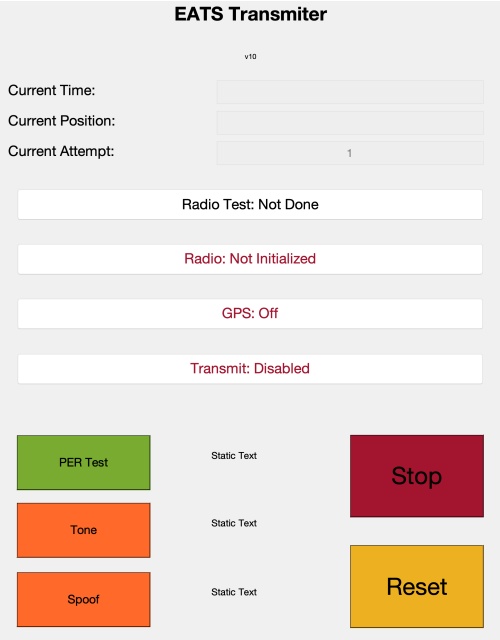


Figure A3 GTO 1 GUI

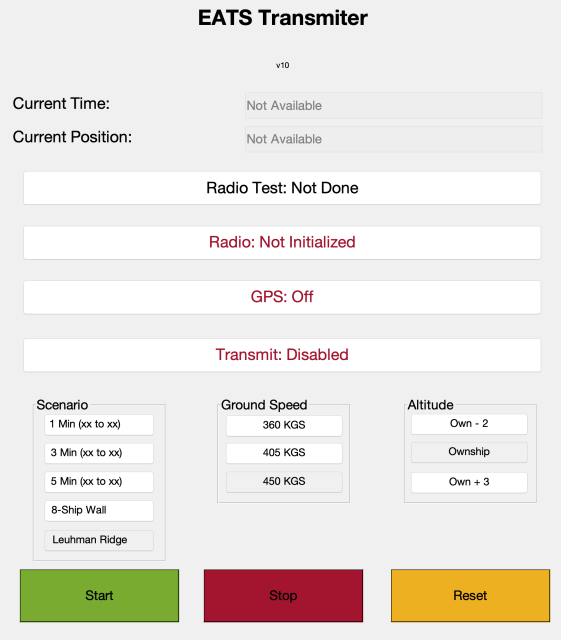


Figure A4 GTO 2 GUI

RECEIVE COMPONENT

Figure A5 depicts a block diagram of the EATS receiver components. Each receiver site had two complete receivers, one with a omnidirectional antenna (figure A6) and one with a directional antenna (figure A7). The EATS receiver utilized a SDR to allow custom, rapid data processing.

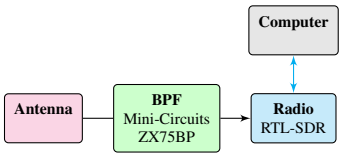


Figure A5 EATS Receive Components

Figure A6 Omnidirectional Antenna

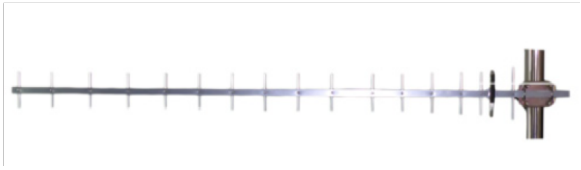


Figure A7 Directional Antenna

The first general test objective utilized two receiver sites with varying FRUIT environments, selected to provide a contrasting low and high FRUIT environment. Figure A8 is an overview map of the low and high FRUIT sites within the San Bernardino National Forest.

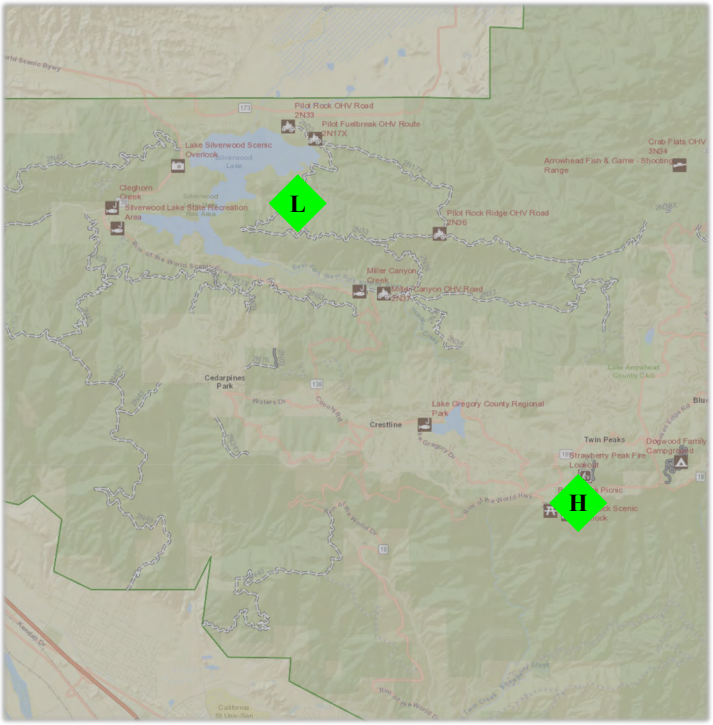


Figure A8 Low and High FRUIT Receiver Sites

Low FRUIT - Pilot Rock Trail Road

The low FRUIT receiver site was located along Pilot Rock Trail Road, also known as 2N33. There was a previously cleared section of terrain near the road where the receiver site was set up. This location provided terrain masking (figure A9) to the majority of the LA basin air traffic creating a low FRUIT environment relative to the other location.

The low FRUIT receiver site was located at the following coordinates. Multiple coordinate formats are presented for ease of use across platforms.

- 34.232091°, -117.23465°
- 34°13.93', -117°14.08'
- 34°13'56", -117°14'05"

Figure A9 shows the masking profile for the low FRUIT receiver site (shown as a purple 'x'). The orange line shows LOS to aircraft at 16,000 feet mean sea level (MSL) and above. The blue line shows the line of sight to 30,000 feet MSL and above.

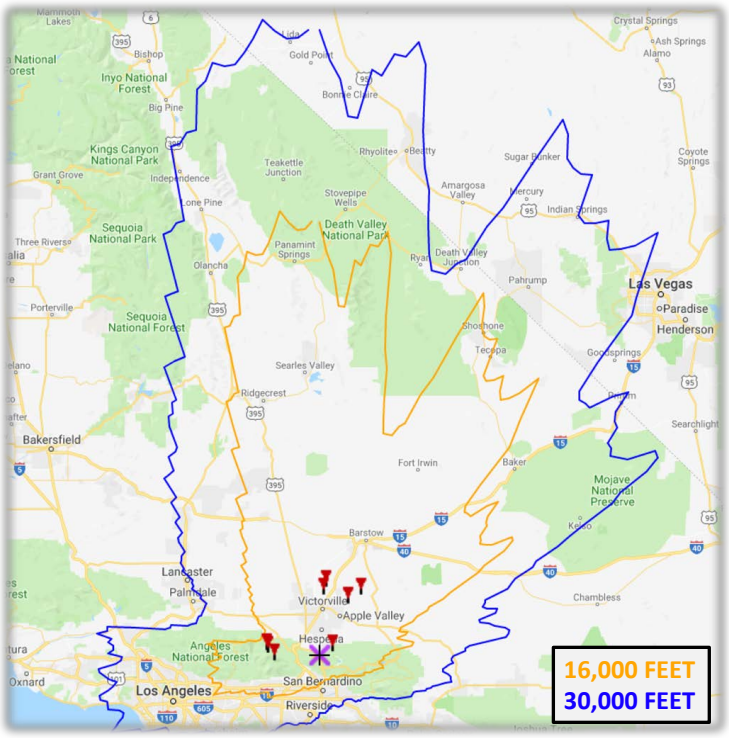


Figure A9 Low FRUIT Terrain Masking Profile

High FRUIT - Strawberry Peak Fire Tower

The high FRUIT receiver site was located at the Strawberry Peak Fire Tower. This location provided minimal terrain masking (figure A10) to the majority of the LA basin air traffic, creating a high FRUIT environment.

The high FRUIT receiver site was located at the following coordinates. Multiple coordinate formats are presented for ease of use across different platforms and systems.

- 34.232091°, -117.23465°
- 34°13.93', -117°14.08'
- 34°13'56", -117°14'05"

Figure A10 shows the masking profile for the low FRUIT receiver site (shown as a purple 'x'). The orange line shows LOS to aircraft at 16,000 feet MSL and above. The blue line shows the line of sight to 30,000 feet MSL and above.

Figure A10 High FRUIT Terrain Masking Profile

This page was intentionally left blank.

APPENDIX B – DETAILED BACKGROUND[1]

INTRODUCTION

ADS-B technology offered significant safety and efficiency benefits to the aviation industry. Its use was widespread and continued to grow as countries passed their equipage deadlines. As an extension of ATCRBS and Mode S, Mode S - Extended Squitter (Mode S-ES) was a widely used ADS-B protocol which lacked security features found in modern information systems.

A new confidentiality sub-protocol for Mode S-ES has been proposed. The novelty of this proposal lies in the use of security principle decomposition to create a lightweight and interoperable scheme which allows for full ADS-B participation while maintaining confidentiality and/or privacy. This protocol uses existing asymmetric encryption and FPE together with unidirectional key passage to enable its confidential modes of operation.

The widespread availability of accurate and precise location and identification information on air traffic creates an environment ripe for exploitation. Strohmeier, et al. explore this issue in depth, using openly available data to analyze government activity and predict potential merger and acquisition activity among corporations. In April 2017, the OpenSky research network detected over 3,000 military aircraft broadcasting plaintext ADS-B in the United States alone. Schäfer, et al. provide detailed statistics on the military and state aircraft use of Mode S and ADS-B. Aviation blogger David Cenciotti routinely publishes instances of military and intelligence aircraft operating with Mode S and/or ADS-B turned on. The Government Accountability Office reports that ADS-B could adversely affect United States (US) Department of Defense security and missions in GAO report 18-177. While not all stakeholders agree on policy or budget considerations in the matter of securing Mode S-ES, those impacted by the lack of security agree that a solution is necessary.

HISTORY

The Royal Air Force (RAF) developed the military IFF system during World War II. A ground-based interrogator would broadcast a signal to nearby aircraft. If an aircraft did not respond properly, it was assumed to be enemy. Eventually, this challenge and response system would allow the directional replies to be correlated with radar, giving a more accurate picture with participating aircraft. The original IFF system is now extended into the military system of today.

The ATCRBS is a direct development from the military IFF system of the early 1960s. Developed largely in response to a string of midair collisions, it used 1030 MHz for interrogations and 1090 MHz for replies, which remains the current standard. ATCRBS uses mode A for identification (via an assignable 4-digit code) and mode C for pressure altitude encoding. These modes are compatible with military IFF.

Mode S developed due to frequency overloading and garbling which occurred as air traffic grew. The major change that allowed additional growth is the selective addressing scheme that Mode S uses. A major requirement for Mode S was backwards compatibility with ATCRBS. The Mode S development committee "concluded that incremental upgrade was feasible, and the benefits of reduced risk and cost outweighed the increased design difficulty of the new system."

The Massachusetts Institute of Technology (MIT) Lincoln Laboratory submitted Mode S-ES for use as an ADS-B standard. Developed as an extension of Mode S, it also favored backwards compatibility against new technology. The major difference and reason for lengthening the message is the inclusion of GNSS based positioning information. Mode S-ES is the global standard for ADS-B, supplemented by other protocols in limited use cases to reduce spectrum saturation.

Follow-on technology designs (IFF, ATCRBS, Mode S, and ADS-B) prioritize interoperability over new technology. This allows excellent safety features to propagate rapidly throughout the air transport industry. In modern times, security and safety are directly correlated, necessitating a focus on modern

security technology. The advantages of interoperability require a unique approach to security.

SECURITY PRINCIPLES

Traditional information security discussion uses the *CIA Triad* to frame security best practices:

- *Confidentiality*: information is only accessed by entities with a 'need to know'
- *Integrity*: information originates from an authenticated source and is not tampered with, changed, or destroyed en route to the using entity
- *Availability*: the service(s) which the information serves or is part of are available to authorized users when required/desired

Figure B1 further decompose these security principles as they pertain to ADS-B.

ADS-B *confidentiality*, means that data is only accessible to intended entities. The direct users of a given aircraft's ADS-B data are ATC and nearby aircraft. ATC requires knowledge of ADS-B data to accomplish their mission: safe separation of aircraft while enhancing system efficiency.

There may be cases in which the user of an airborne platform wishes or is required to participate and contribute to the safe conduct of air transport, yet desires some level of privacy or requires confidentiality for their movement or operation. This user requires that the ADS-B data associated with them be revealed only to those with need to know.

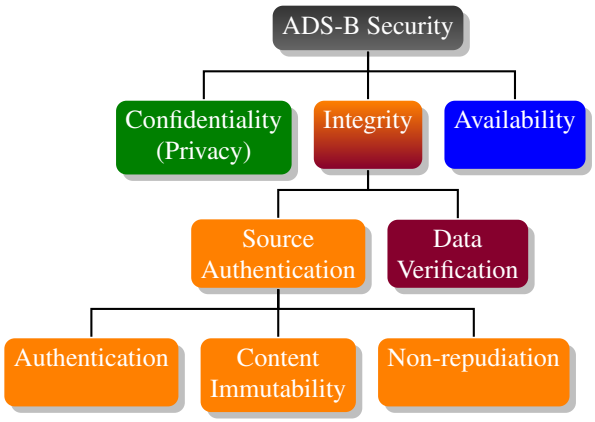


Figure B1 ADS-B Security Decomposition

It is important to note that the implementation of confidentiality does not imply any sort of authentication or verification. Depending on system design, one could have a confidential system in which an adversary could manipulate, remove, or insert false data.

The *integrity* of ADS-B data can be decomposed into *source authentication* and *data verification*, each with associated challenges.

Source authentication is the practice of ensuring that received data did originate from, and can be attributed to, a certain entity without modification by an outside entity. This reflects the authentication, content immutability, and non-repudiation principles. These three principles are grouped for the sake of organization. Source authentication does not give assurance that the reporting entity is where it says it is and is doing what it says it is doing. An authenticated aircraft could be inadvertently or maliciously sending false data as a trusted entity.

Data verification is a concept added under the umbrella of integrity when using untrusted broadcast communications. Data verification ensures that the information transmitted is accurate. For example, data verification is used to ensure that the location reported by an ADS-B target is the true location of that aircraft or vehicle. Data verification does not, in this case, determine whether a message has been tampered with; it only seeks to determine if the data is true.

Availability refers to assurance of service to users when and where it is required in accordance with design specifications. Generally, ADS-B should be available at all times to all users within its service volume unless a known or scheduled outage is communicated to users.

The advantage of decomposing security principles when addressing ADS-B security lies in the fact that maintaining interoperability with current standards likely requires a limited and simple approach. This is a far easier task when focusing efforts on one area of security. Additionally, the various stakeholders in ADS-B have different requirements and desires for a security scheme. State authorities and air defense organizations might care only about authentication or verification. ATC likely is concerned with verification and availability, since their focus is safety of flight. Meanwhile, corporate flight departments, military users, and intelligence related activities are probably concerned with confidentiality. Additionally, the rising emphasis on right to privacy makes the implementation of real-time data security a significant issue for all citizens, regardless of current privacy law.

The broadcast nature of ADS-B allows layered independent security protocols to accomplish tailored objectives where and when desired. Due to its emphasis on interoperability, this proposal for confidentiality is compatible with any number of physical layer techniques for authentication or verification, including widely used multilateration techniques.

INPUTS & REQUIREMENTS

When approaching the issue of ADS-B security, several inputs should be considered when deriving requirements. These include:

- Stakeholders
- Adversaries
- Standards
- Previous Work

Stakeholders

Various stakeholders are involved in the development, deployment, operation, and use of ADS-B. These entities have a singular common objective: *safe aircraft operations*, agnostic to aircraft type or operational objectives. From that point goals diverge and become operation or entity specific; they include efficiency, security, profitability, etc.

Users

Users include entities for which ADS-B is intended to increase operational safety and efficiency. They provide data to, while receiving services from, the system. These entities vary widely in size and mission but share the fundamental requirement for separation from other users while operating on the ground and in the air. Some users, such as corporate flight departments, military, intelligence, and state aircraft require or desire confidentiality in some or all of their operations. Other users, such as air carriers, have a public operation and therefore may not have a direct requirement for confidentiality.

Service Providers

Service providers are the entities which receive data from users and provide services to users. Generally, these services primarily provide separation of traffic while increasing airspace efficiency. They may also provide data up-links, currently in the form of traffic and weather. Providers include ATC, who provides actual traffic separation, as well as surveillance network operators and equipment manufacturers, who together provide the CNS capabilities required by ATC.

Regulatory Bodies

Regulatory bodies can be governmental or non-governmental and regional or global in influence. They primarily make laws, regulations, and technical standards to ensure safety, or charging third-parties with the same. Examples of regulatory bodies include CAAs, lawmakers, executives, RTCA, and EUROCAE. These institutions each play a role in the creation of regulations and standards for Communication, Navigation, and Surveillance (CNS) systems and ADS-B.

Adversaries

Two types of adversaries are addressed: active and passive. Active adversaries collect surveillance data directly related to a certain operation. This might be a foreign intelligence service tracking friendly military missions or movements. It may also be a corporate competitor keeping tabs on a rival's leadership. In any case, an active adversary has a pre-determined set of targets. Passive adversaries are not acting maliciously, but unknowingly make data publicly available to those who are. Popular flight tracking service providers will give operators the ability to block flights but smaller homegrown aggregation networks may not. These networks are generally used by researchers and hobbyists for benign or beneficial purposes. Even so, this disclosure of information can pose a threat to operations requiring confidentiality.

Active and passive adversaries have varying technical capability to aggregate surveillance data. A single receiver allows an adversary to read message content and gain knowledge that a certain aircraft is within radio range. If that aircraft is transmitting extended squitter (ES) location, the same single receiver can know precise location information. A network of receivers with precision timing information can use multilateration to gain location information using only signal externals.

Current Standards

As discussed above, RTCA and EUROCAE create, maintain, and update standards for Mode S and ADS-B. ICAO and various CAAs implement and/or augment these standards. It is important to recognize that the careful standards development and ratification process takes significant time. A primary goal of this proposal is to extend existing standards without deprecating any provision currently in place.

Requirements

Requirements which are specific and attainable offer the bridge between the objective of a secure and interoperable confidentiality scheme and the proposal detailed below.

Functional Requirements

Functional requirements detail what the protocol must do to prevent active and passive adversaries from exploiting ADS-B data transmitted as Mode S-ES packets. It must:

- Render a participating node's identification anonymous to third parties while remaining unambiguous to authorized receivers (ATC and air defense authorities).
- Selectively obfuscate data within the 'ME' field of a DF-17 ADS-B packet, rendering it unreadable to third parties yet readable to authorized receivers.
- Switch between clear and obscured modes manually or based on automated criteria (e.g. near another aircraft).
- When not in an encryption mode, it must behave in accordance with currently ratified standards for Mode S.

Performance Requirements

Performance requirements dictate quantitative standards by which the protocol can be evaluated. While defined parameters are beyond the scope of this effort, examples of performance standards follow. The protocol must:

- Have ≤ 0.1 probability of identification collisions between two separate airborne aircraft, and the event of a collision must be mitigated.
- Be capable of deployment in transponders fielded post 2010 and maintain a transmit rate specified in current standards while in a secure mode.
- If encryption is used to obfuscate transmitted information, it must resist a brute-force attack using current, commercially available technology for 25 years.
- Two obfuscation modes must be available: one which anonymizes the ICAO address and obfuscates the callsign, and a second which also obfuscates location and altitude.
- While set in a resolution advisory (RA) mode, the system must cease obfuscating location and altitude information when within 3 NM horizontally and 2000 feet vertically of traffic sensed from on-board sources. This behavior is not required for off-board sources (e.g. TIS-B). The system will continue to obfuscate identification.

Design Requirements

Design requirements force an implementation to adhere to external influences.

- The protocol must adhere to the design requirements and implementation specified in current RTCA standards in every respect other than the modules added to enable the above functions.
- Regardless of added modules, all RF characteristics of the protocol must adhere to RTCA standards.
- Any hardware or software cryptographic modules must be designed and implemented in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) for secure development and deployment.
- Key distribution to the general public is not feasible and will not be part of any encryption scheme used.

Constraints

Constraints put limits on how an implementation can be achieved and what technology may be used to do so.

- Interoperability and Backwards Compatibility:
  - The protocol allows unmodified transponders and traffic collision avoidance systems (TCASs) which are currently approved for use to continue operating without further updates.
  - The protocol will not require a modification to the processing and display of non-participating tracks to the ground segment.
  - The protocol allows for provisions to be *added* to technical standards, while disallowing current provisions to be deleted or modified.

- Return Data Channel and Broadcast Architecture:
  - Will not have access to a return data communications channel, since one does not and cannot exist within the 1090ES protocol without significant modification to current standards.
  - Because ADS-B is a broadcast protocol and many Mode S-ES transponders do not possess Mode S enhanced surveillance (EHS) or extended length message (ELM) capability, the security system will not use interrogate/reply Mode S capabilities as part of the security scheme.

PROTOCOL DESIGN

The following proposal meets the objectives and requirements discussed above.

Data Encryption

While authentication and verification can be completed with both cryptographic and non-cryptographic solutions, confidentiality of broadcast data requires obfuscation via encryption. FPE combines AES security with the capability to handle legacy data formats of variable length. NIST formally recommends the use of FF1 as a block cipher mode. This proposal makes use of FF1 as the symmetric encryption mode for encrypting Mode S-ES packets.

ICAO Address Anonymization

An aircraft's callsign can be encrypted by using FF1 on the 'ME' field of packets with a type code 1 through 4, though this leaves the aircraft's plaintext ICAO address available to uniquely identify it. Obfuscating the ICAO address requires substituting a *SUIA* on all packets transmitted, even those not encrypted. An SUIA is randomly generated from a set of ICAO addresses set aside for this purpose. A possible set is the block beginning with 1111 11, allowing 18 bits from which to generate one of $2^{18} = 262,144$ addresses. This block is currently allocated for special use. The SUIA is intended to last for a single session, which is at most a single flight from avionics initialization to engine shutdown.

SUIA & Session Key Handoff

The use of symmetric encryption and unique identifiers requires a method of sharing both an SUIA and session symmetric key (SSK) between a participating aircraft and the ground-based surveillance infrastructure.

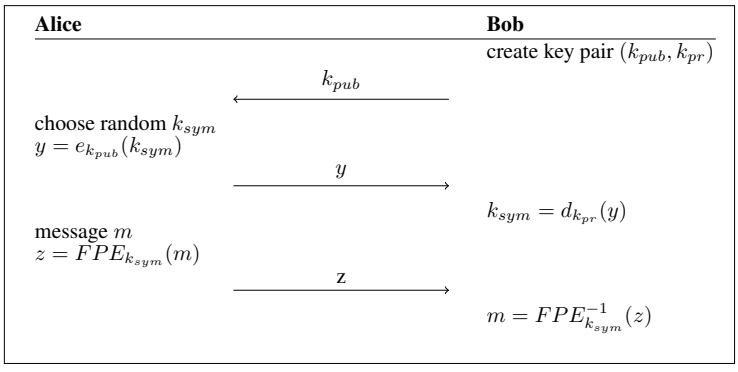


Figure B2 Broadcast Hybrid Encryption

While it is generally accepted that traditional public key infrastructure (PKI) is unsuitable for securing ADS-B in its current form, variations such as identity-based encryption (IBE) and retroactive key publication carry potential. In any case, a PKI solution to ADS-B security would more than likely require significant protocol modifications and infrastructure enhancements to be tenable.

The basic principles of asymmetric encryption are extended to propose *unidirectional public key encryption*, as shown in figure B2. The broadcast, stateless nature of ADS-B lends itself to this construct. ATC or the CAA generate a public/private key pair and publish the public key, potentially with the region's 28 day flight information

cycle. The aircraft wishing to participate securely generates an SUIA and session symmetric key (SSK) on board and encrypts them using the aforementioned public key. This data is then packetized and transmitted to ATC, who then possesses both the SUIA and SSK. With these, they are able to correlate follow on anonymous packets to a specific ICAO address and decrypt those 'ME' fields which were transmitted encrypted.

This proposal assumes that ground based infrastructure is capable of secure key handling among clients. For example, in the US, the Federal Aviation Administration (FAA) and North American Aerospace Defense Command (NORAD) can share SUIAs and SSKs within the ATC and air defense networks without revealing them to third parties. It also assumes that an entropy source sufficient to the level of security required exists or can exist in on-board avionics systems.

Given that ADS-B often has a high PER and is stateless (no return data channel for acknowledgement), the packetized nature of the key handoff segment presents a communications challenge. One solution is to resend the handoff packets a certain number of times that will result in a high probability of successful segment assembly. This can potentially be enhanced through the use of forward error correction (FEC) schemes, depending on the trade-off between increased packet count and reduced bit error rate (BER).

If a key handoff is unsuccessful after the certain number of attempts, this results in the aircraft not appearing on the controller's display and the controller is notified (using current or specialized notifications). The controller can then direct the aircrew to re-attempt the handoff using standard voice communications verbiage. This process will also occur if an aircraft attempts a handoff in which the generated SUIA collides with an existing SUIA.

Message Formats

Message: an abstract term used to denote the communication of certain data, without reference to a particular technical part of the Mode S protocol.

Packet: a $120\mu s$ Mode S data unit consisting of a $8\mu s$ preamble and 56 or 112 bits of data.

Segment: a data unit used for key handoff that is divided into multiple packets prior to transmission and reassembled upon receipt.

ME Field: the content-containing payload of a Mode S-ES packet.

Mode S uses downlink formats (DFs) to determine the size, type, and purpose of each data packet. This DF always consists of the first five bits of a packet. A DF-17 denotes a 112-bit extended squitter packet whose purpose is ADS-B. A DF-18 follows roughly the same format, but originates from a non-transponder source. In designing the protocol, unused DFs are brought into service arbitrarily. A future RTCA committee could allocate them as necessary.

All DF-17 packets have the same structure, depicted in figure B3. This structure consists of the DF, capability, address, payload (ME field), and checksum. The ME field is determined by a type and sub-type code, with 32 types currently defined.

DF-15	0 1111	CA: 3	SUIA: 24		Ciphertext ME: 56	PI: 24	Encrypted ES
DF-17	1 0001	CA: 3	ICAO or SUIA: 24		Plaintext ME: 56	PI: 24	Extended Squitter
DF-23	1 0110	ICAO: 24	Att: 7	Seq: 5	Data: 44	PI: 24	Key Handoff

Figure B3 Added Reply Formats

In this proposal, only the ME field is encrypted. This allows the system to selectively encrypt based on message type. For example, if a user is in a mode that masks identity, but does not deny location information, the transponder would only encrypt packets that contain an Aircraft Identification and Category Message.

Ground Infrastructure

Besides firmware or software updates for the transponders of those wishing to utilize confidential ADS-B, the ground segment receives the biggest addition. A *secure software module* acts as a filter for incoming Mode S packets, as shown in figure B4. This module is self contained, possessing a lookup table, capability to populate the table from key handoff segments, and a translation method. Any packet that has a normal ICAO address and DF passes through unmodified. A packet with an SUIA has its address field replaced with the actual ICAO address. A packet that is encrypted has its address replaced, DF set to 17 (or as required), and ME field decrypted. This is then forwarded as a normal DF-17 to current ATC software.

```
1:  procedure PACKETFILTER
2:      packet ← Incoming Mode S Packet, Post CRC
3:
4:      if packet.addr ≥ 0xFC0000  & ≤ 0xFFFFFF then
5:          suia ← true
6:
7:      if packet.df = 23 then
8:          addr, suia, sk, complete ← AssembleSegment(packet)
9:          if complete = true then
10:             AddEntryToTable(addr, suia, sk)
11:         return
12:     else if packet.df = 15 then
13:         key ← LookupKey(suia)
14:         packet.meField ← Decrypt(meField, key)
15:         packet.addr ← LookupIcaoAddr(suia)
16:         packet.df ← 17
17:     else if suia = true then
18:         packet.addr ← LookupIcaoAddr(suia)
19:     else
20:         No Changes to Packet
21:
22: return packet
```

Figure B4 Secure Software Module

Interoperability

Modern air surveillance technology accomplishes two core functions:

- Allow ground infrastructure to track aircraft movement and status
- Allow aircraft to automatically or manually avoid collisions among themselves

The ground infrastructure requires continuous knowledge of identification and precise location of each aircraft. The proposed protocol allows this by assuming that ground infrastructure (ATC/CAA/Air Defense) is trusted by the user and maintains internal trust among systems. Even if the user does not actually trust them, a prerequisite for using airspace is to contractually trust the authorities.

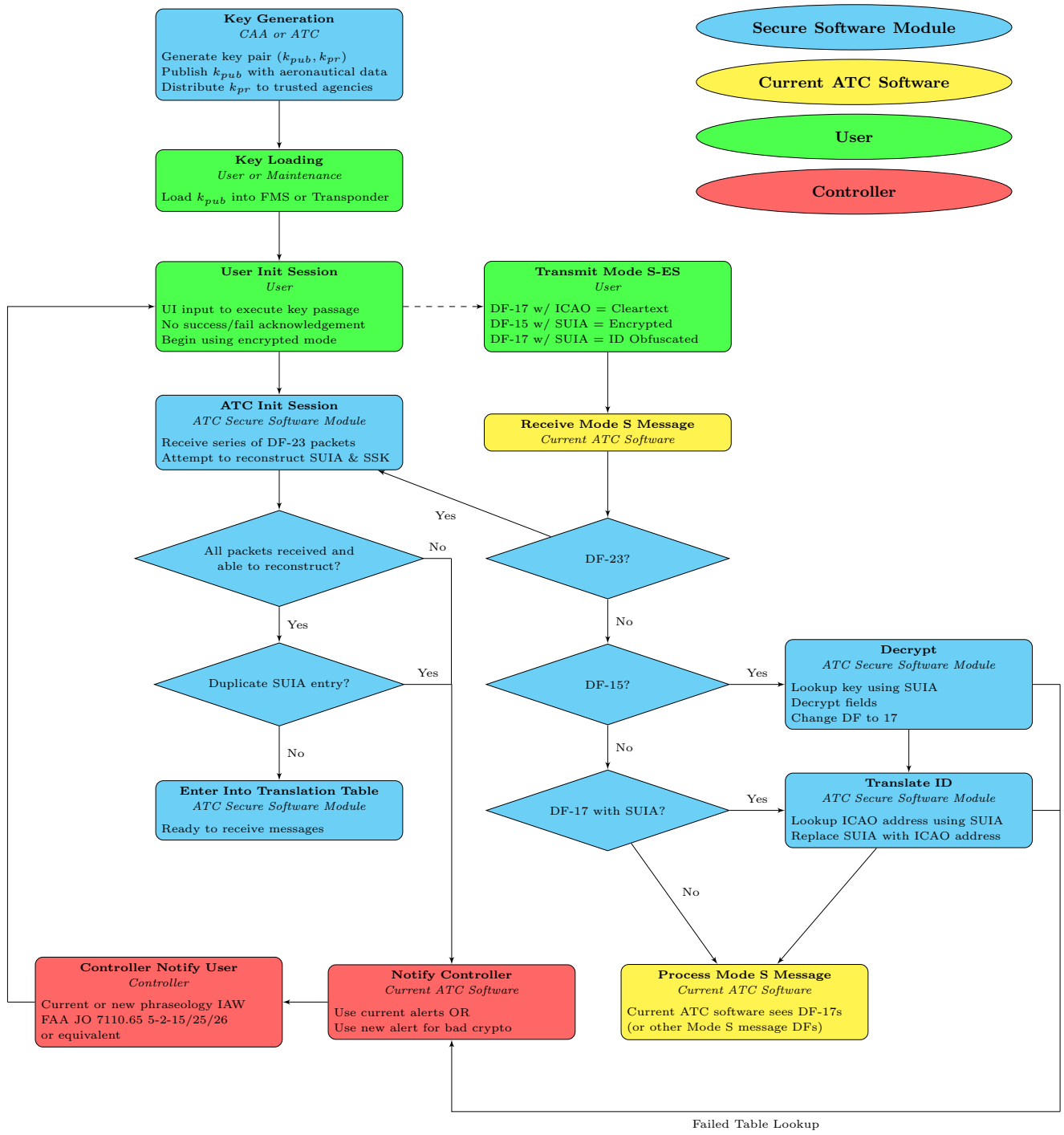


Figure B5 Functional Flow Diagram

On the other hand, any receiver of information besides the aforementioned authorities is untrusted by default. Other aircraft require some knowledge in order to avoid collisions. Required knowledge of identification is limited to size and required knowledge of precise position increases with proximity to other aircraft. This protocol allows interoperability in several ways:

- *TCAS:* Even with Mode S-ES packets encrypted, DF-16 TCAS packets are unaffected. Enabling hybrid surveillance mode may require using an SUIA with TCAS packets, a trivial modification to this scheme.
- *TIS-B:* ATC can re-transmit received DF-17 and non ADS-B information as DF-18, a service known as traffic information service broadcast (TIS-B). There is already a capability to anonymize or block these re-transmissions which could be extended to include confidential DF-17 participants.
- *Phase of Flight Discrimination*: Whether confidential participants are obfuscating identification only or also encrypting location information can be adjusted based on phase of flight. This will be a policy decision of CAAs and operators. For example, military aircraft who require confidentiality while executing tactics could broadcast plaintext location with obfuscated ID while transiting to and from special use airspace (SUAS). When established in the airspace, these aircraft would encrypt their location, allowing safety monitoring from controllers and security from adversaries. Another example is a corporate aircraft. Using an SUIA the entire flight, the aircraft could use plaintext location while in the congested airspace that contains potential visual flight rules (VFR) traffic, then obfuscate location while en route in instrument flight rules (IFR) only airspace. If the aircraft re-accomplishes a key handoff while en route, their SUIA will be different at their arrival location.
- *Auto Proximity Mode:* It is likely that a relatively low percentage of aircraft will have a requirement for confidentiality. Auto proximity mode would have an aircraft encrypting their location unless a traffic conflict is detected (with ADS-B or TCAS) within a certain horizontal and vertical proximity. The aircraft would then broadcast plaintext location (still using an SUIA) until the conflict has passed.

Each of these methods of achieving interoperability must be used with careful understanding of the trade-off between the safety gained and security lost. This protocol allows seamless integration of each user's unique confidentiality or security requirements while efficiently preserving the core functions of air surveillance.

SUMMARY

Interoperability is a key reason ADS-B was built on the Mode S-ES protocol and has significant benefits for safety. Unfortunately, it makes the implementation of security difficult to accomplish. This proposal makes use of industry standard cryptographic solutions to create a lightweight, interoperable scheme for Mode S confidentiality. A system which focuses solely on confidentiality is more cost effective to implement and compatible with existing Mode S users. It calls for the use of FPE to encrypt Mode S-ES packets without changing format and session identification tokens to anonymize users. It then propose the use of unidirectional, broadcast public key cryptography to transfer keys and tokens from users to ATC.

This work puts the initial protocol development steps in place to allow safe and secure operations in the global airspace system. With mandatory equipage rapidly approaching, a significant portion of the ADS-B user base requires a solution to confidentiality other than "turn it off." A lightweight, interoperable system allows those users to gain the safety benefits of ADS-B without compromising their operations.

APPENDIX C – MODEL

MODEL DEFINITION

The logistic regression model for PER was defined as

$$P_{error} = 1 - \left[\left(1 - \frac{e^{\beta_{intx}+\beta_r r+\beta_f f+\beta_a a+\beta_d d}}{e^{\beta_{intx}+\beta_r r+\beta_f f+\beta_a a+\beta_d d}+1}\right)1.7\right]$$

where P_{error} was the probability of a packet error, or PER, β_{intx} was the intercept coefficient, and β_i were the coefficients for each factor. Range is measured in nautical miles. The binary factors are represented by the value 1 for Low FRUIT, Omni Antenna, and Inbound Direction and the value 2 for High FRUIT, Directional Antenna, and Outbound Direction. Models were generated for all combinations of factors to allow the use of only the variables of interest. To use a subset of variables, simply omit the undesired terms. Note the adjustment coefficient of 1.7 included in the model due to the receiver limitation discussed in *Constraints and Limitations*. Table C1 contains the coefficients for the model.

Table C1 Model Coefficients

	Range	**Range FRUIT**	**Range Antenna**	**Range Direction**	**Range FRUIT Antenna**	**Range FRUIT Direction**	**Range Antenna Direction**	**Range FRUIT Antenna Direction**
$\boldsymbol{\beta_{intx}}$	1.088422157	0.32170932	1.36286078	3.88921704	0.59784947	3.08345370	4.19256129	3.38967477
$\boldsymbol{\beta_r}$	0.01756133	0.01697433	0.01757497	0.02088855	0.01698839	0.02037372	0.02091456	0.02040034
$\boldsymbol{\beta_f}$	-	0.55304155	-	-	0.55358029	0.59664200	-	0.59751668
$\boldsymbol{\beta_a}$	-	-	-0.18140779	-	-0.18305126	-	-0.19863500	-0.20121717
$\boldsymbol{\beta_d}$	-	-	-	-1.86187977	-	-1.87875095	-1.86398346	-1.88099134

This example calculates the PER for 10 NM, Low FRUIT, Directional Antenna, and Outbound Direction of Flight:

$$P_{error} = 1 - \left[\left(1 - \frac{e^{3.38967477+(0.02040034)(10)+(0.59751668)(1)+(-0.20121717)(2)+(-1.88099134)(2)}}{e^{3.38967477+(0.02040034)(10)+(0.59751668)(1)+(-0.20121717)(2)+(-1.88099134)(2)}+1}\right)1.7\right] = 0.16$$

MODEL ANALYSIS

Statistical analysis showed a high level of confidence in the models based on test day conditions. The worst-case statistical level of confidence, based on samples per one nautical mile bin (figure D6), is 0.9954. This level is for the eight NM bin. Figure C1 shows the corresponding confidence interval plotted with dashed lines.

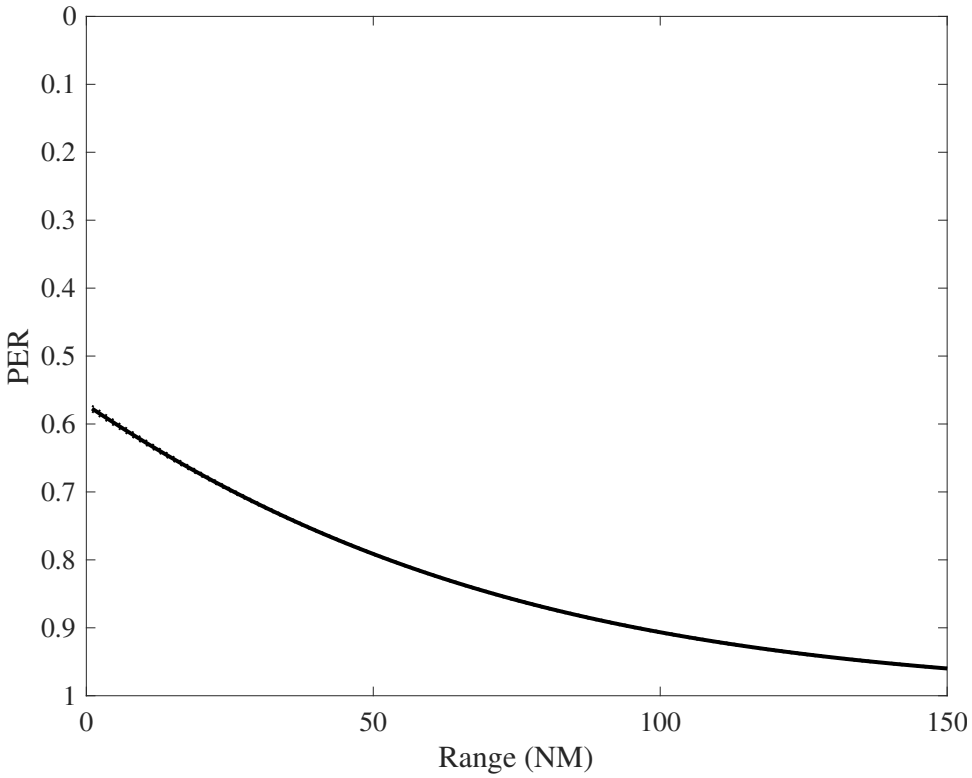


Figure C1 Confidence Interval

Analysis also showed that all investigated factors were significant in all models. Table C2 shows the P-Values for the factors investigated. Values showing $\lim_{p\to 0}$ are limited by the minimum of MATLAB 64-bit double precision floating point numbers. These can be approximated to zero.

Table C2 Model P-Values

	Range	**Range FRUIT**	**Range Antenna**	**Range Direction**	**Range FRUIT Antenna**	**Range FRUIT Direction**	**Range Antenna Direction**	**Range FRUIT Antenna Direction**
Intercept	$\lim_{p\to 0}$	$7.22 \cdot 10^{-52}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$3.98 \cdot 10^{-96}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$
Range	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$
FRUIT	-	$\lim_{p\to 0}$	-	-	$\lim_{p\to 0}$	$\lim_{p\to 0}$	-	$\lim_{p\to 0}$
Antenna	-	-	$2.72 \cdot 10^{-46}$	-	$1.08 \cdot 10^{-46}$	-	$1.62 \cdot 10^{-50}$	$3.78 \cdot 10^{-51}$
Direction	-	-	-	$\lim_{p\to 0}$	-	$\lim_{p\to 0}$	$\lim_{p\to 0}$	$\lim_{p\to 0}$

TABULAR MODEL

Pre-calculated tabular data is included here for ease of access. Tables C3 through C7 contain PER data rounded to the hundredths place.

Table C3 Tabular Model: 8-30 NM

Range (NM)	Overall	Low FRUIT	High FRUIT	Omni Ant	Directional Ant	Inbound	Outbound	Low / Omni	Low / Dir	High / Omni	High / Dir	Omni / In	Omni / Out	Dir / In	Dir / Out	Low / In	Low / Out	High / In	High / Out	Low / Omni / In	Low / Omni / Out	Low / Dir / In	Low / Dir / Out	High / Omni / In	High / Omni / Out	High / Dir / In	High / Dir / Out
8	.62	.55	.71	.64	.59	.83	.29	.58	.52	.73	.68	.84	.33	.81	.25	.79	.19	.88	.43	.81	.23	.77	.14	.89	.47	.87	.39
9	.62	.55	.71	.65	.59	.83	.30	.58	.52	.73	.69	.85	.34	.82	.26	.79	.19	.88	.44	.81	.24	.78	.15	.89	.47	.87	.40
10	.63	.56	.71	.65	.60	.84	.31	.59	.53	.74	.69	.85	.35	.82	.27	.80	.20	.88	.44	.82	.25	.78	.16	.89	.48	.87	.41
11	.63	.56	.72	.66	.60	.84	.32	.59	.53	.74	.70	.85	.36	.82	.28	.80	.21	.88	.45	.82	.26	.78	.17	.90	.49	.87	.41
12	.64	.57	.72	.66	.61	.84	.32	.60	.54	.74	.70	.86	.36	.83	.28	.81	.22	.89	.46	.82	.26	.79	.18	.90	.50	.88	.42
13	.64	.57	.73	.67	.62	.84	.33	.60	.54	.75	.70	.86	.37	.83	.29	.81	.23	.89	.47	.83	.27	.79	.19	.90	.50	.88	.43
14	.65	.58	.73	.67	.62	.85	.34	.61	.55	.75	.71	.86	.38	.83	.30	.81	.24	.89	.47	.83	.28	.80	.20	.90	.51	.88	.44
15	.65	.58	.73	.68	.63	.85	.35	.61	.56	.75	.71	.86	.39	.84	.31	.82	.25	.89	.48	.83	.29	.80	.20	.90	.52	.88	.45
16	.66	.59	.74	.68	.63	.85	.36	.62	.56	.76	.72	.87	.40	.84	.32	.82	.26	.90	.49	.84	.30	.80	.21	.91	.53	.89	.45
17	.66	.60	.74	.68	.64	.86	.37	.62	.57	.76	.72	.87	.41	.84	.33	.82	.26	.90	.50	.84	.31	.81	.22	.91	.53	.89	.46
18	.66	.60	.74	.69	.64	.86	.37	.63	.57	.76	.72	.87	.41	.85	.34	.83	.27	.90	.50	.84	.31	.81	.23	.91	.54	.89	.47
19	.67	.61	.75	.69	.65	.86	.38	.63	.58	.77	.73	.87	.42	.85	.34	.83	.28	.90	.51	.84	.32	.81	.24	.91	.55	.89	.48
20	.67	.61	.75	.70	.65	.86	.39	.64	.58	.77	.73	.88	.43	.85	.35	.83	.29	.90	.52	.85	.33	.82	.25	.91	.55	.89	.48
21	.68	.62	.76	.70	.66	.87	.40	.64	.59	.77	.74	.88	.44	.85	.36	.83	.30	.90	.52	.85	.34	.82	.26	.91	.56	.90	.49
22	.68	.62	.76	.71	.66	.87	.41	.65	.59	.78	.74	.88	.45	.86	.37	.84	.31	.91	.53	.85	.35	.82	.26	.92	.57	.90	.50
23	.69	.63	.76	.71	.66	.87	.42	.65	.60	.78	.74	.88	.45	.86	.38	.84	.31	.91	.54	.86	.36	.83	.27	.92	.57	.90	.50
24	.69	.63	.77	.72	.67	.87	.42	.66	.60	.78	.75	.89	.46	.86	.39	.84	.32	.91	.55	.86	.36	.83	.28	.92	.58	.90	.51
25	.70	.64	.77	.72	.67	.88	.43	.66	.61	.79	.75	.89	.47	.87	.39	.85	.33	.91	.55	.86	.37	.83	.29	.92	.59	.90	.52
26	.70	.64	.77	.72	.68	.88	.44	.67	.61	.79	.75	.89	.48	.87	.40	.85	.34	.91	.56	.86	.38	.84	.30	.92	.59	.91	.53
27	.71	.65	.78	.73	.68	.88	.45	.67	.62	.79	.76	.89	.48	.87	.41	.85	.35	.92	.57	.87	.39	.84	.31	.92	.60	.91	.53
28	.71	.65	.78	.73	.69	.88	.45	.68	.62	.80	.76	.89	.49	.87	.42	.85	.36	.92	.57	.87	.40	.84	.32	.92	.60	.91	.54
29	.71	.65	.78	.74	.69	.89	.46	.68	.63	.80	.77	.90	.50	.88	.43	.86	.36	.92	.58	.87	.40	.84	.32	.93	.61	.91	.55
30	.72	.66	.79	.74	.70	.89	.47	.68	.63	.80	.77	.90	.51	.88	.43	.86	.37	.92	.59	.87	.41	.85	.33	.93	.62	.91	.55

Table C4 Tabular Model: 31-60 NM

Range (NM)	Overall	Low FRUIT	High FRUIT	Omni Ant	Directional Ant	Inbound	Outbound	Low / Omni	Low / Dir	High / Omni	High / Dir	Omni / In	Omni / Out	Dir / In	Dir / Out	Low / In	Low / Out	High / In	High / Out	Low / Omni / In	Low / Omni / Out	Low / Dir / In	Low / Dir / Out	High / Omni / In	High / Omni / Out	High / Dir / In	High / Dir / Out
31	.72	.66	.79	.74	.70	.89	.48	.69	.64	.81	.77	.90	.51	.88	.44	.86	.38	.92	.59	.88	.42	.85	.34	.93	.62	.91	.56
32	.73	.67	.79	.75	.71	.89	.49	.69	.64	.81	.78	.90	.52	.88	.45	.87	.39	.92	.60	.88	.43	.85	.35	.93	.63	.92	.57
33	.73	.67	.80	.75	.71	.89	.49	.70	.65	.81	.78	.90	.53	.88	.46	.87	.40	.92	.60	.88	.43	.86	.36	.93	.63	.92	.57
34	.73	.68	.80	.75	.71	.90	.50	.70	.65	.81	.78	.91	.54	.89	.47	.87	.40	.93	.61	.88	.44	.86	.36	.93	.64	.92	.58
35	.74	.68	.80	.76	.72	.90	.51	.71	.66	.82	.79	.91	.54	.89	.47	.87	.41	.93	.62	.88	.45	.86	.37	.93	.65	.92	.59
36	.74	.69	.80	.76	.72	.90	.51	.71	.66	.82	.79	.91	.55	.89	.48	.88	.42	.93	.62	.89	.46	.86	.38	.94	.65	.92	.59
37	.75	.69	.81	.77	.73	.90	.52	.71	.67	.82	.79	.91	.56	.89	.49	.88	.43	.93	.63	.89	.47	.87	.39	.94	.66	.92	.60
38	.75	.69	.81	.77	.73	.90	.53	.72	.67	.83	.79	.91	.56	.90	.50	.88	.43	.93	.63	.89	.47	.87	.40	.94	.66	.93	.61
39	.75	.70	.81	.77	.73	.91	.54	.72	.68	.83	.80	.92	.57	.90	.50	.88	.44	.93	.64	.89	.48	.87	.40	.94	.67	.93	.61
40	.76	.70	.82	.78	.74	.91	.54	.73	.68	.83	.80	.92	.58	.90	.51	.88	.45	.93	.65	.90	.49	.87	.41	.94	.67	.93	.62
41	.76	.71	.82	.78	.74	.91	.55	.73	.69	.83	.80	.92	.58	.90	.52	.89	.46	.94	.65	.90	.49	.88	.42	.94	.68	.93	.62
42	.76	.71	.82	.78	.75	.91	.56	.73	.69	.84	.81	.92	.59	.90	.52	.89	.47	.94	.66	.90	.50	.88	.43	.94	.68	.93	.63
43	.77	.72	.82	.79	.75	.91	.56	.74	.69	.84	.81	.92	.60	.91	.53	.89	.47	.94	.66	.90	.51	.88	.44	.94	.69	.93	.64
44	.77	.72	.83	.79	.75	.92	.57	.74	.70	.84	.81	.92	.60	.91	.54	.89	.48	.94	.67	.90	.52	.88	.44	.95	.69	.93	.64
45	.77	.72	.83	.79	.76	.92	.58	.74	.70	.84	.82	.92	.61	.91	.55	.89	.49	.94	.67	.90	.52	.88	.45	.95	.70	.93	.65
46	.78	.73	.83	.80	.76	.92	.58	.75	.71	.85	.82	.93	.61	.91	.55	.90	.49	.94	.68	.91	.53	.89	.46	.95	.70	.94	.65
47	.78	.73	.83	.80	.76	.92	.59	.75	.71	.85	.82	.93	.62	.91	.56	.90	.50	.94	.68	.91	.54	.89	.47	.95	.71	.94	.66
48	.78	.74	.84	.80	.77	.92	.60	.76	.71	.85	.82	.93	.63	.91	.57	.90	.51	.94	.69	.91	.54	.89	.47	.95	.71	.94	.66
49	.79	.74	.84	.80	.77	.92	.60	.76	.72	.85	.83	.93	.63	.92	.57	.90	.52	.94	.69	.91	.55	.89	.48	.95	.72	.94	.67
50	.79	.74	.84	.81	.77	.92	.61	.76	.72	.85	.83	.93	.64	.92	.58	.90	.52	.95	.70	.91	.56	.90	.49	.95	.72	.94	.67
51	.79	.75	.84	.81	.78	.93	.62	.77	.73	.86	.83	.93	.65	.92	.59	.91	.53	.95	.70	.92	.56	.90	.50	.95	.73	.94	.68
52	.80	.75	.85	.81	.78	.93	.62	.77	.73	.86	.83	.93	.65	.92	.59	.91	.54	.95	.71	.92	.57	.90	.50	.95	.73	.94	.69
53	.80	.75	.85	.82	.78	.93	.63	.77	.73	.86	.84	.94	.66	.92	.60	.91	.54	.95	.71	.92	.58	.90	.51	.95	.74	.94	.69
54	.80	.76	.85	.82	.79	.93	.63	.78	.74	.86	.84	.94	.66	.92	.61	.91	.55	.95	.72	.92	.58	.90	.52	.95	.74	.95	.70
55	.81	.76	.85	.82	.79	.93	.64	.78	.74	.87	.84	.94	.67	.93	.61	.91	.56	.95	.72	.92	.59	.90	.52	.96	.75	.95	.70
56	.81	.76	.86	.83	.79	.93	.65	.78	.75	.87	.84	.94	.67	.93	.62	.91	.56	.95	.73	.92	.60	.91	.53	.96	.75	.95	.71
57	.81	.77	.86	.83	.80	.93	.65	.79	.75	.87	.85	.94	.68	.93	.62	.92	.57	.95	.73	.92	.60	.91	.54	.96	.76	.95	.71
58	.82	.77	.86	.83	.80	.94	.66	.79	.75	.87	.85	.94	.68	.93	.63	.92	.58	.95	.74	.93	.61	.91	.54	.96	.76	.95	.72
59	.82	.77	.86	.83	.80	.94	.66	.79	.76	.87	.85	.94	.69	.93	.64	.92	.58	.95	.74	.93	.61	.91	.55	.96	.76	.95	.72
60	.82	.78	.86	.84	.81	.94	.67	.80	.76	.88	.85	.94	.70	.93	.64	.92	.59	.96	.75	.93	.62	.91	.56	.96	.77	.95	.72

Table C5 Tabular Model: 61-90 NM

Range (NM)	Overall	Low FRUIT	High FRUIT	Omni Ant	Directional Ant	Inbound	Outbound	Low / Omni	Low / Dir	High / Omni	High / Dir	Omni / In	Omni / Out	Dir / In	Dir / Out	Low / In	Low / Out	High / In	High / Out	Low / Omni / In	Low / Omni / Out	Low / Dir / In	Low / Dir / Out	High / Omni / In	High / Omni / Out	High / Dir / In	High / Dir / Out
61	.82	.78	.87	.84	.81	.94	.67	.80	.76	.88	.86	.95	.70	.93	.65	.92	.60	.96	.75	.93	.63	.92	.56	.96	.77	.95	.73
62	.83	.78	.87	.84	.81	.94	.68	.80	.77	.88	.86	.95	.71	.94	.65	.92	.60	.96	.76	.93	.63	.92	.57	.96	.78	.95	.73
63	.83	.79	.87	.84	.82	.94	.69	.80	.77	.88	.86	.95	.71	.94	.66	.93	.61	.96	.76	.93	.64	.92	.58	.96	.78	.95	.74
64	.83	.79	.87	.85	.82	.94	.69	.81	.77	.88	.86	.95	.72	.94	.67	.93	.61	.96	.76	.93	.64	.92	.58	.96	.78	.96	.74
65	.83	.79	.87	.85	.82	.94	.70	.81	.78	.89	.86	.95	.72	.94	.67	.93	.62	.96	.77	.94	.65	.92	.59	.96	.79	.96	.75
66	.84	.80	.88	.85	.82	.95	.70	.81	.78	.89	.87	.95	.73	.94	.68	.93	.63	.96	.77	.94	.66	.92	.60	.96	.79	.96	.75
67	.84	.80	.88	.85	.83	.95	.71	.82	.78	.89	.87	.95	.73	.94	.68	.93	.63	.96	.78	.94	.66	.92	.60	.97	.80	.96	.76
68	.84	.80	.88	.86	.83	.95	.71	.82	.79	.89	.87	.95	.73	.94	.69	.93	.64	.96	.78	.94	.67	.93	.61	.97	.80	.96	.76
69	.85	.81	.88	.86	.83	.95	.72	.82	.79	.89	.87	.95	.74	.94	.69	.93	.64	.96	.78	.94	.67	.93	.62	.97	.80	.96	.76
70	.85	.81	.88	.86	.83	.95	.72	.82	.79	.89	.87	.95	.74	.94	.70	.94	.65	.96	.79	.94	.68	.93	.62	.97	.81	.96	.77
71	.85	.81	.89	.86	.84	.95	.73	.83	.80	.90	.88	.96	.75	.95	.70	.94	.66	.96	.79	.94	.68	.93	.63	.97	.81	.96	.77
72	.85	.81	.89	.86	.84	.95	.73	.83	.80	.90	.88	.96	.75	.95	.71	.94	.66	.97	.79	.94	.69	.93	.63	.97	.81	.96	.78
73	.85	.82	.89	.87	.84	.95	.74	.83	.80	.90	.88	.96	.76	.95	.71	.94	.67	.97	.80	.94	.69	.93	.64	.97	.82	.96	.78
74	.86	.82	.89	.87	.85	.95	.74	.83	.80	.90	.88	.96	.76	.95	.72	.94	.67	.97	.80	.95	.70	.93	.65	.97	.82	.96	.78
75	.86	.82	.89	.87	.85	.95	.74	.84	.81	.90	.88	.96	.77	.95	.72	.94	.68	.97	.81	.95	.70	.94	.65	.97	.82	.96	.79
76	.86	.82	.89	.87	.85	.96	.75	.84	.81	.90	.89	.96	.77	.95	.73	.94	.68	.97	.81	.95	.71	.94	.66	.97	.83	.96	.79
77	.86	.83	.90	.88	.85	.96	.75	.84	.81	.91	.89	.96	.77	.95	.73	.94	.69	.97	.81	.95	.71	.94	.66	.97	.83	.97	.80
78	.87	.83	.90	.88	.85	.96	.76	.84	.82	.91	.89	.96	.78	.95	.74	.94	.69	.97	.82	.95	.72	.94	.67	.97	.83	.97	.80
79	.87	.83	.90	.88	.86	.96	.76	.85	.82	.91	.89	.96	.78	.95	.74	.95	.70	.97	.82	.95	.72	.94	.67	.97	.84	.97	.80
80	.87	.84	.90	.88	.86	.96	.77	.85	.82	.91	.89	.96	.79	.95	.75	.95	.70	.97	.82	.95	.73	.94	.68	.97	.84	.97	.81
81	.87	.84	.90	.88	.86	.96	.77	.85	.82	.91	.89	.96	.79	.96	.75	.95	.71	.97	.83	.95	.73	.94	.68	.97	.84	.97	.81
82	.87	.84	.90	.88	.86	.96	.77	.85	.83	.91	.90	.96	.79	.96	.76	.95	.71	.97	.83	.95	.74	.94	.69	.97	.84	.97	.81
83	.88	.84	.91	.89	.87	.96	.78	.86	.83	.91	.90	.97	.80	.96	.76	.95	.72	.97	.83	.95	.74	.94	.69	.97	.85	.97	.82
84	.88	.85	.91	.89	.87	.96	.78	.86	.83	.92	.90	.97	.80	.96	.76	.95	.72	.97	.84	.96	.75	.95	.70	.98	.85	.97	.82
85	.88	.85	.91	.89	.87	.96	.79	.86	.83	.92	.90	.97	.81	.96	.77	.95	.73	.97	.84	.96	.75	.95	.70	.98	.85	.97	.82
86	.88	.85	.91	.89	.87	.96	.79	.86	.84	.92	.90	.97	.81	.96	.77	.95	.73	.97	.84	.96	.75	.95	.71	.98	.86	.97	.83
87	.88	.85	.91	.89	.87	.96	.79	.86	.84	.92	.90	.97	.81	.96	.78	.95	.74	.97	.84	.96	.76	.95	.71	.98	.86	.97	.83
88	.89	.85	.91	.90	.88	.97	.80	.87	.84	.92	.91	.97	.82	.96	.78	.95	.74	.97	.85	.96	.76	.95	.72	.98	.86	.97	.83
89	.89	.86	.91	.90	.88	.97	.80	.87	.84	.92	.91	.97	.82	.96	.78	.96	.75	.98	.85	.96	.77	.95	.72	.98	.86	.97	.84
90	.89	.86	.92	.90	.88	.97	.81	.87	.85	.92	.91	.97	.82	.96	.79	.96	.75	.98	.85	.96	.77	.95	.73	.98	.87	.97	.84

Table C6 Tabular Model: 91-120 NM

Range (NM)	Overall	Low FRUIT	High FRUIT	Omni Ant	Directional Ant	Inbound	Outbound	Low / Omni	Low / Dir	High / Omni	High / Dir	Omni / In	Omni / Out	Dir / In	Dir / Out	Low / In	Low / Out	High / In	High / Out	Low / Omni / In	Low / Omni / Out	Low / Dir / In	Low / Dir / Out	High / Omni / In	High / Omni / Out	High / Dir / In	High / Dir / Out
91	.89	.86	.92	.90	.88	.97	.81	.87	.85	.92	.91	.97	.83	.96	.79	.96	.75	.98	.86	.96	.78	.95	.73	.98	.87	.97	.84
92	.89	.86	.92	.90	.88	.97	.81	.87	.85	.93	.91	.97	.83	.96	.80	.96	.76	.98	.86	.96	.78	.95	.74	.98	.87	.97	.84
93	.90	.87	.92	.90	.89	.97	.82	.88	.85	.93	.91	.97	.83	.97	.80	.96	.76	.98	.86	.96	.78	.95	.74	.98	.87	.97	.85
94	.90	.87	.92	.91	.89	.97	.82	.88	.86	.93	.91	.97	.84	.97	.80	.96	.77	.98	.86	.96	.79	.96	.75	.98	.88	.98	.85
95	.90	.87	.92	.91	.89	.97	.82	.88	.86	.93	.92	.97	.84	.97	.81	.96	.77	.98	.87	.96	.79	.96	.75	.98	.88	.98	.85
96	.90	.87	.92	.91	.89	.97	.83	.88	.86	.93	.92	.97	.84	.97	.81	.96	.77	.98	.87	.97	.79	.96	.75	.98	.88	.98	.86
97	.90	.87	.92	.91	.89	.97	.83	.88	.86	.93	.92	.97	.84	.97	.81	.96	.78	.98	.87	.97	.80	.96	.76	.98	.88	.98	.86
98	.90	.88	.93	.91	.90	.97	.83	.89	.86	.93	.92	.97	.85	.97	.82	.96	.78	.98	.87	.97	.80	.96	.76	.98	.88	.98	.86
99	.90	.88	.93	.91	.90	.97	.84	.89	.87	.93	.92	.97	.85	.97	.82	.96	.79	.98	.88	.97	.81	.96	.77	.98	.89	.98	.86
100	.91	.88	.93	.91	.90	.97	.84	.89	.87	.93	.92	.98	.85	.97	.82	.96	.79	.98	.88	.97	.81	.96	.77	.98	.89	.98	.87
101	.91	.88	.93	.92	.90	.97	.84	.89	.87	.94	.92	.98	.86	.97	.83	.96	.79	.98	.88	.97	.81	.96	.78	.98	.89	.98	.87
102	.91	.88	.93	.92	.90	.97	.84	.89	.87	.94	.92	.98	.86	.97	.83	.97	.80	.98	.88	.97	.82	.96	.78	.98	.89	.98	.87
103	.91	.88	.93	.92	.90	.97	.85	.89	.88	.94	.93	.98	.86	.97	.83	.97	.80	.98	.88	.97	.82	.96	.78	.98	.90	.98	.87
104	.91	.89	.93	.92	.91	.97	.85	.90	.88	.94	.93	.98	.86	.97	.84	.97	.80	.98	.89	.97	.82	.96	.79	.98	.90	.98	.88
105	.91	.89	.93	.92	.91	.98	.85	.90	.88	.94	.93	.98	.87	.97	.84	.97	.81	.98	.89	.97	.83	.96	.79	.98	.90	.98	.88
106	.92	.89	.94	.92	.91	.98	.86	.90	.88	.94	.93	.98	.87	.97	.84	.97	.81	.98	.89	.97	.83	.97	.79	.98	.90	.98	.88
107	.92	.89	.94	.92	.91	.98	.86	.90	.88	.94	.93	.98	.87	.97	.85	.97	.81	.98	.89	.97	.83	.97	.80	.98	.90	.98	.88
108	.92	.89	.94	.93	.91	.98	.86	.90	.88	.94	.93	.98	.87	.97	.85	.97	.82	.98	.89	.97	.83	.97	.80	.98	.90	.98	.89
109	.92	.90	.94	.93	.91	.98	.86	.90	.89	.94	.93	.98	.88	.98	.85	.97	.82	.98	.90	.97	.84	.97	.81	.99	.91	.98	.89
110	.92	.90	.94	.93	.91	.98	.87	.91	.89	.94	.93	.98	.88	.98	.85	.97	.82	.98	.90	.97	.84	.97	.81	.99	.91	.98	.89
111	.92	.90	.94	.93	.92	.98	.87	.91	.89	.95	.93	.98	.88	.98	.86	.97	.83	.98	.90	.97	.84	.97	.81	.99	.91	.98	.89
112	.92	.90	.94	.93	.92	.98	.87	.91	.89	.95	.94	.98	.88	.98	.86	.97	.83	.98	.90	.97	.85	.97	.82	.99	.91	.98	.89
113	.92	.90	.94	.93	.92	.98	.87	.91	.89	.95	.94	.98	.89	.98	.86	.97	.83	.98	.90	.98	.85	.97	.82	.99	.91	.98	.90
114	.93	.90	.94	.93	.92	.98	.88	.91	.90	.95	.94	.98	.89	.98	.87	.97	.84	.98	.91	.98	.85	.97	.82	.99	.92	.98	.90
115	.93	.90	.94	.93	.92	.98	.88	.91	.90	.95	.94	.98	.89	.98	.87	.97	.84	.99	.91	.98	.85	.97	.83	.99	.92	.98	.90
116	.93	.91	.94	.93	.92	.98	.88	.91	.90	.95	.94	.98	.89	.98	.87	.97	.84	.99	.91	.98	.86	.97	.83	.99	.92	.98	.90
117	.93	.91	.95	.94	.92	.98	.88	.92	.90	.95	.94	.98	.89	.98	.87	.97	.85	.99	.91	.98	.86	.97	.83	.99	.92	.98	.90
118	.93	.91	.95	.94	.92	.98	.89	.92	.90	.95	.94	.98	.90	.98	.88	.98	.85	.99	.91	.98	.86	.97	.83	.99	.92	.98	.91
119	.93	.91	.95	.94	.93	.98	.89	.92	.90	.95	.94	.98	.90	.98	.88	.98	.85	.99	.91	.98	.87	.97	.84	.99	.92	.99	.91
120	.93	.91	.95	.94	.93	.98	.89	.92	.90	.95	.94	.98	.90	.98	.88	.98	.85	.99	.92	.98	.87	.97	.84	.99	.92	.99	.91

Table C7 Tabular Model: 121-150 NM

Range (NM)	Overall	Low FRUIT	High FRUIT	Omni Ant	Directional Ant	Inbound	Outbound	Low / Omni	Low / Dir	High / Omni	High / Dir	Omni / In	Omni / Out	Dir / In	Dir / Out	Low / In	Low / Out	High / In	High / Out	Low / Omni / In	Low / Omni / Out	Low / Dir / In	Low / Dir / Out	High / Omni / In	High / Omni / Out	High / Dir / In	High / Dir / Out
121	.93	.91	.95	.94	.93	.98	.89	.92	.91	.95	.94	.98	.90	.98	.88	.98	.86	.99	.92	.98	.87	.97	.84	.99	.93	.99	.91
122	.94	.92	.95	.94	.93	.98	.89	.92	.91	.95	.95	.98	.90	.98	.88	.98	.86	.99	.92	.98	.87	.97	.85	.99	.93	.99	.91
123	.94	.92	.95	.94	.93	.98	.90	.92	.91	.96	.95	.98	.91	.98	.89	.98	.86	.99	.92	.98	.87	.98	.85	.99	.93	.99	.91
124	.94	.92	.95	.94	.93	.98	.90	.92	.91	.96	.95	.99	.91	.98	.89	.98	.86	.99	.92	.98	.88	.98	.85	.99	.93	.99	.92
125	.94	.92	.95	.94	.93	.98	.90	.93	.91	.96	.95	.99	.91	.98	.89	.98	.87	.99	.92	.98	.88	.98	.86	.99	.93	.99	.92
126	.94	.92	.95	.94	.93	.98	.90	.93	.91	.96	.95	.99	.91	.98	.89	.98	.87	.99	.93	.98	.88	.98	.86	.99	.93	.99	.92
127	.94	.92	.95	.95	.94	.98	.90	.93	.91	.96	.95	.99	.91	.98	.90	.98	.87	.99	.93	.98	.88	.98	.86	.99	.93	.99	.92
128	.94	.92	.95	.95	.94	.98	.91	.93	.92	.96	.95	.99	.91	.98	.90	.98	.87	.99	.93	.98	.89	.98	.86	.99	.94	.99	.92
129	.94	.92	.96	.95	.94	.99	.91	.93	.92	.96	.95	.99	.92	.98	.90	.98	.88	.99	.93	.98	.89	.98	.87	.99	.94	.99	.92
130	.94	.93	.96	.95	.94	.99	.91	.93	.92	.96	.95	.99	.92	.98	.90	.98	.88	.99	.93	.98	.89	.98	.87	.99	.94	.99	.92
131	.94	.93	.96	.95	.94	.99	.91	.93	.92	.96	.95	.99	.92	.98	.90	.98	.88	.99	.93	.98	.89	.98	.87	.99	.94	.99	.93
132	.95	.93	.96	.95	.94	.99	.91	.93	.92	.96	.95	.99	.92	.98	.91	.98	.88	.99	.93	.98	.89	.98	.87	.99	.94	.99	.93
133	.95	.93	.96	.95	.94	.99	.91	.94	.92	.96	.95	.99	.92	.98	.91	.98	.89	.99	.94	.98	.90	.98	.88	.99	.94	.99	.93
134	.95	.93	.96	.95	.94	.99	.92	.94	.92	.96	.96	.99	.92	.99	.91	.98	.89	.99	.94	.98	.90	.98	.88	.99	.94	.99	.93
135	.95	.93	.96	.95	.94	.99	.92	.94	.93	.96	.96	.99	.93	.99	.91	.98	.89	.99	.94	.98	.90	.98	.88	.99	.94	.99	.93
136	.95	.93	.96	.95	.94	.99	.92	.94	.93	.96	.96	.99	.93	.99	.91	.98	.89	.99	.94	.98	.90	.98	.88	.99	.94	.99	.93
137	.95	.93	.96	.95	.95	.99	.92	.94	.93	.96	.96	.99	.93	.99	.91	.98	.89	.99	.94	.98	.90	.98	.88	.99	.95	.99	.93
138	.95	.93	.96	.96	.95	.99	.92	.94	.93	.97	.96	.99	.93	.99	.92	.98	.90	.99	.94	.98	.91	.98	.89	.99	.95	.99	.94
139	.95	.94	.96	.96	.95	.99	.92	.94	.93	.97	.96	.99	.93	.99	.92	.98	.90	.99	.94	.99	.91	.98	.89	.99	.95	.99	.94
140	.95	.94	.96	.96	.95	.99	.93	.94	.93	.97	.96	.99	.93	.99	.92	.98	.90	.99	.94	.99	.91	.98	.89	.99	.95	.99	.94
141	.95	.94	.96	.96	.95	.99	.93	.94	.93	.97	.96	.99	.93	.99	.92	.98	.90	.99	.94	.99	.91	.98	.89	.99	.95	.99	.94
142	.95	.94	.96	.96	.95	.99	.93	.94	.93	.97	.96	.99	.94	.99	.92	.98	.90	.99	.95	.99	.91	.98	.89	.99	.95	.99	.94
143	.95	.94	.96	.96	.95	.99	.93	.94	.93	.97	.96	.99	.94	.99	.92	.98	.91	.99	.95	.99	.91	.98	.90	.99	.95	.99	.94
144	.96	.94	.97	.96	.95	.99	.93	.95	.94	.97	.96	.99	.94	.99	.93	.99	.91	.99	.95	.99	.92	.98	.90	.99	.95	.99	.94
145	.96	.94	.97	.96	.95	.99	.93	.95	.94	.97	.96	.99	.94	.99	.93	.99	.91	.99	.95	.99	.92	.98	.90	.99	.95	.99	.94
146	.96	.94	.97	.96	.95	.99	.93	.95	.94	.97	.96	.99	.94	.99	.93	.99	.91	.99	.95	.99	.92	.98	.90	.99	.95	.99	.95
147	.96	.94	.97	.96	.95	.99	.94	.95	.94	.97	.96	.99	.94	.99	.93	.99	.91	.99	.95	.99	.92	.98	.90	.99	.96	.99	.95
148	.96	.94	.97	.96	.95	.99	.94	.95	.94	.97	.96	.99	.94	.99	.93	.99	.91	.99	.95	.99	.92	.99	.91	.99	.96	.99	.95
149	.96	.95	.97	.96	.96	.99	.94	.95	.94	.97	.97	.99	.94	.99	.93	.99	.92	.99	.95	.99	.92	.99	.91	.99	.96	.99	.95
150	.96	.95	.97	.96	.96	.99	.94	.95	.94	.97	.97	.99	.95	.99	.93	.99	.92	.99	.95	.99	.93	.99	.91	.99	.96	.99	.95

This page was intentionally left blank.

APPENDIX D – ADDITIONAL PLOTS

The plots in this section represent most combinations of model outputs. Figure D1 represents all data from all flights with a focus on the impact of each of the single factors. Figure D2 displays only data collected while the aircraft was travelling outbound, and shows the single factor impact of FRUIT and antenna type. Figure D3 displays only outbound data and shows multi-factor effects of FRUIT and antenna type. Figures D4 and D5 display inbound data with single factor effects and multi-factor effects, respectively. Figure D6 shows the total number of transmitted samples in one NM range bins from 8 to 150 NM.

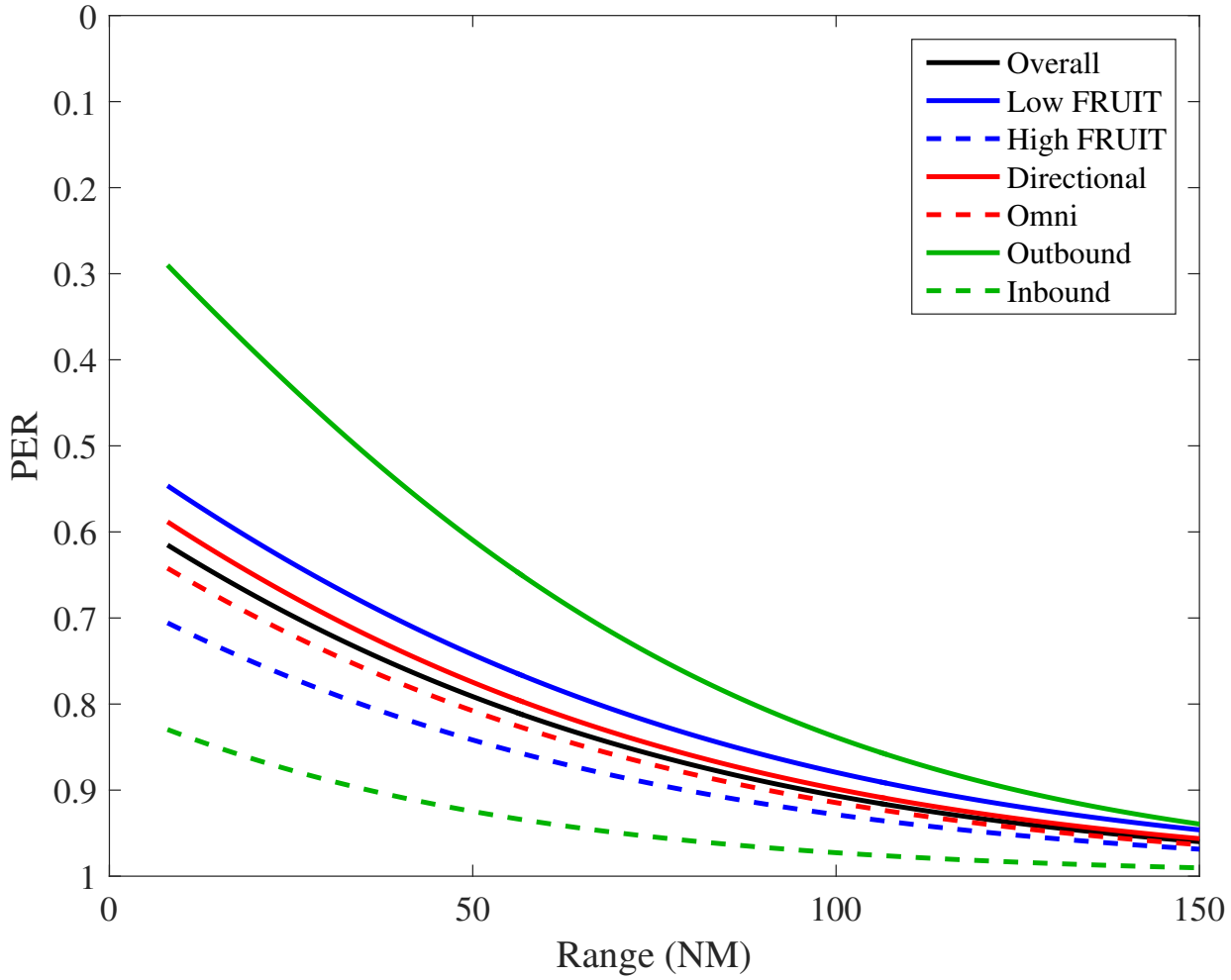


Figure D1 PER Results: All Single Factors

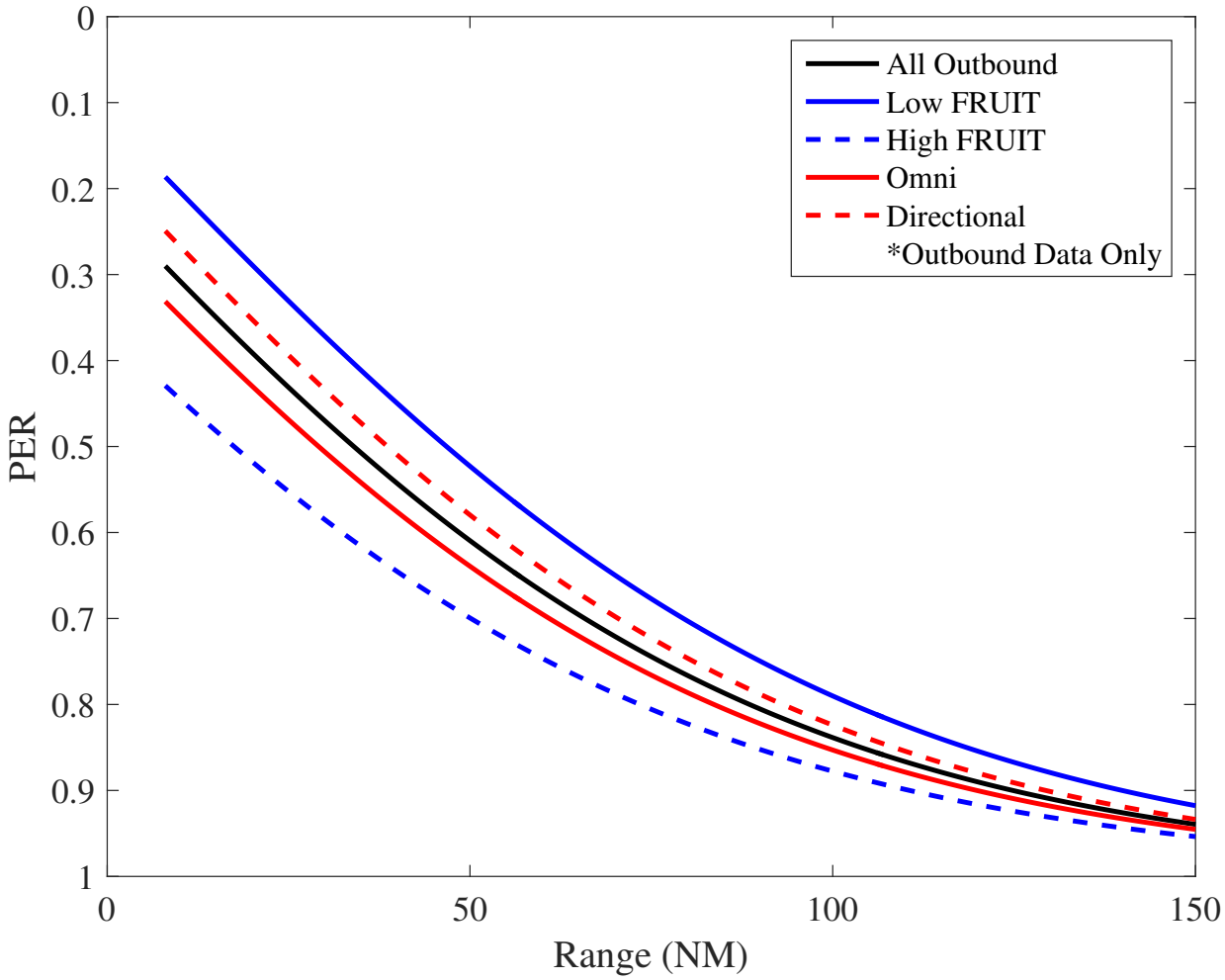


Figure D2 PER Results: Single Factor

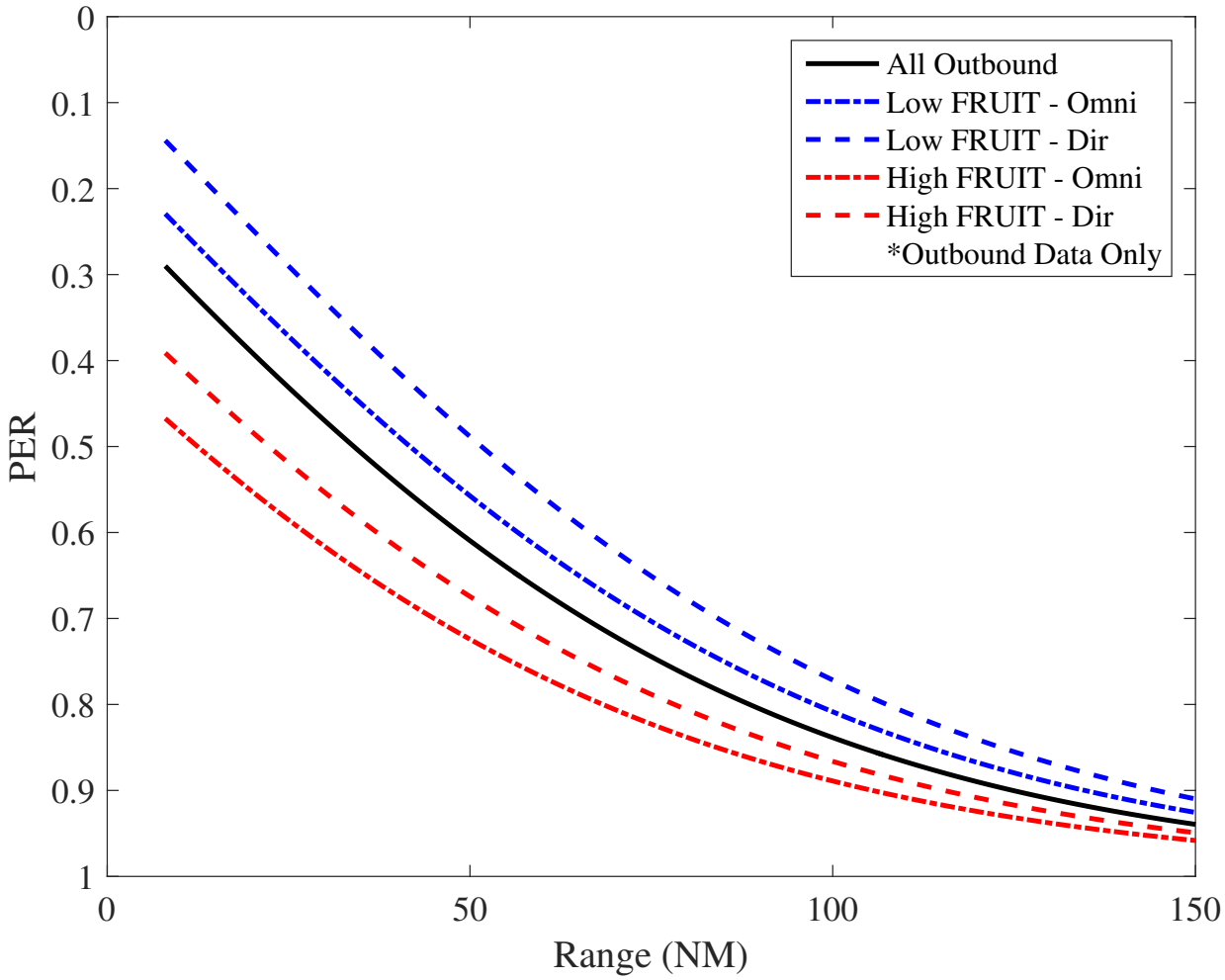


Figure D3 PER Results: Multi-Factor

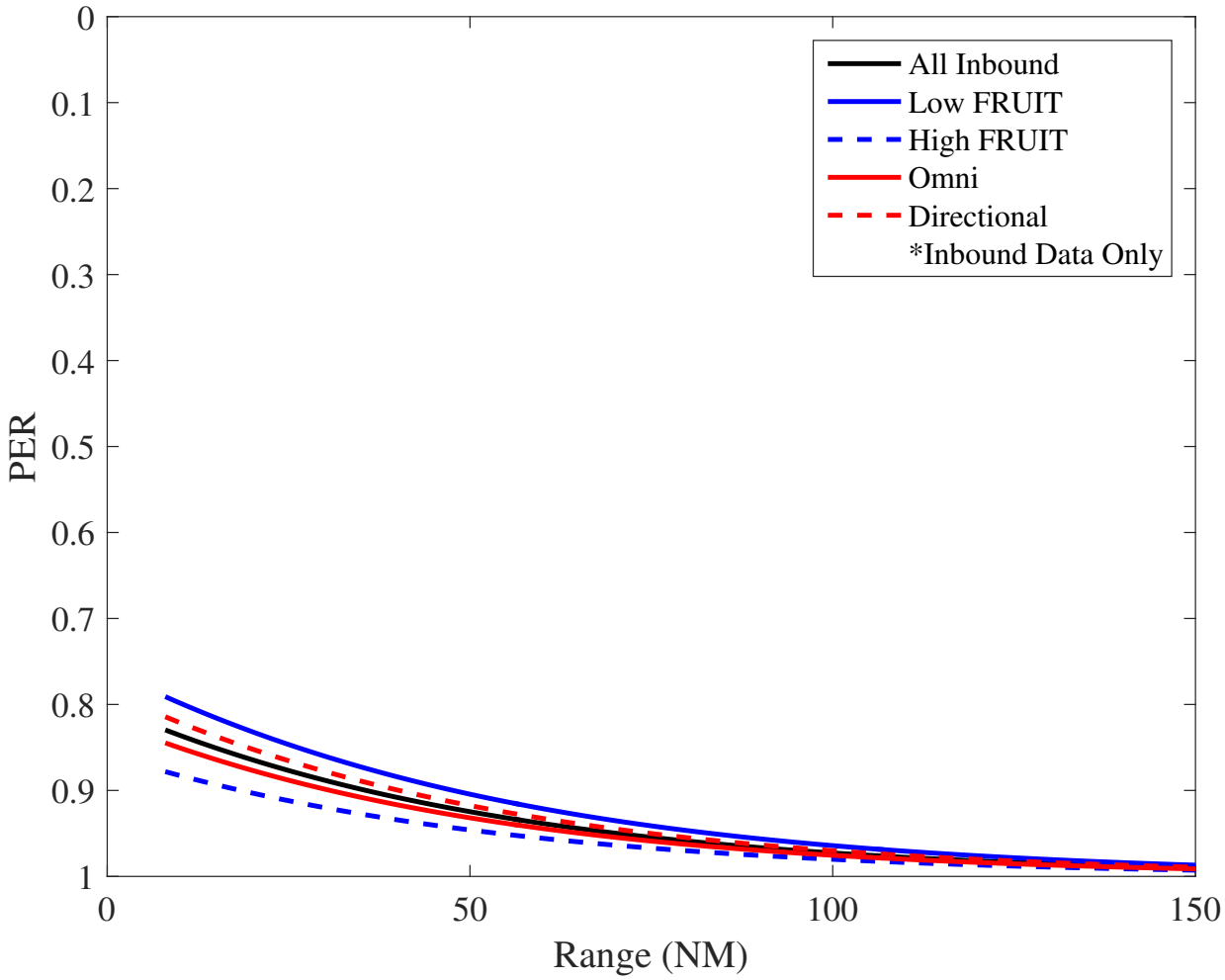


Figure D4 PER Results: Single Factor

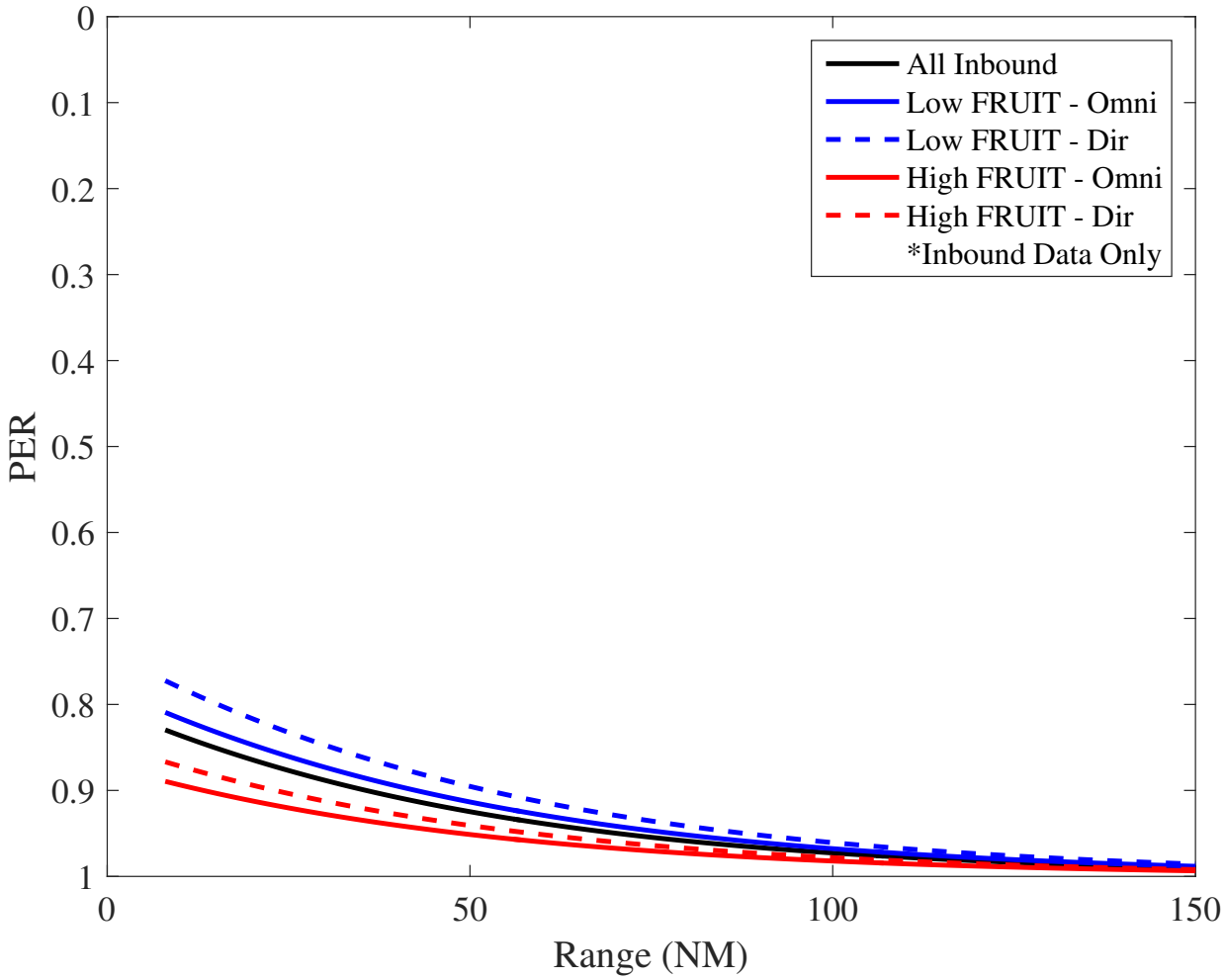


Figure D5 PER Results: Multi-Factor

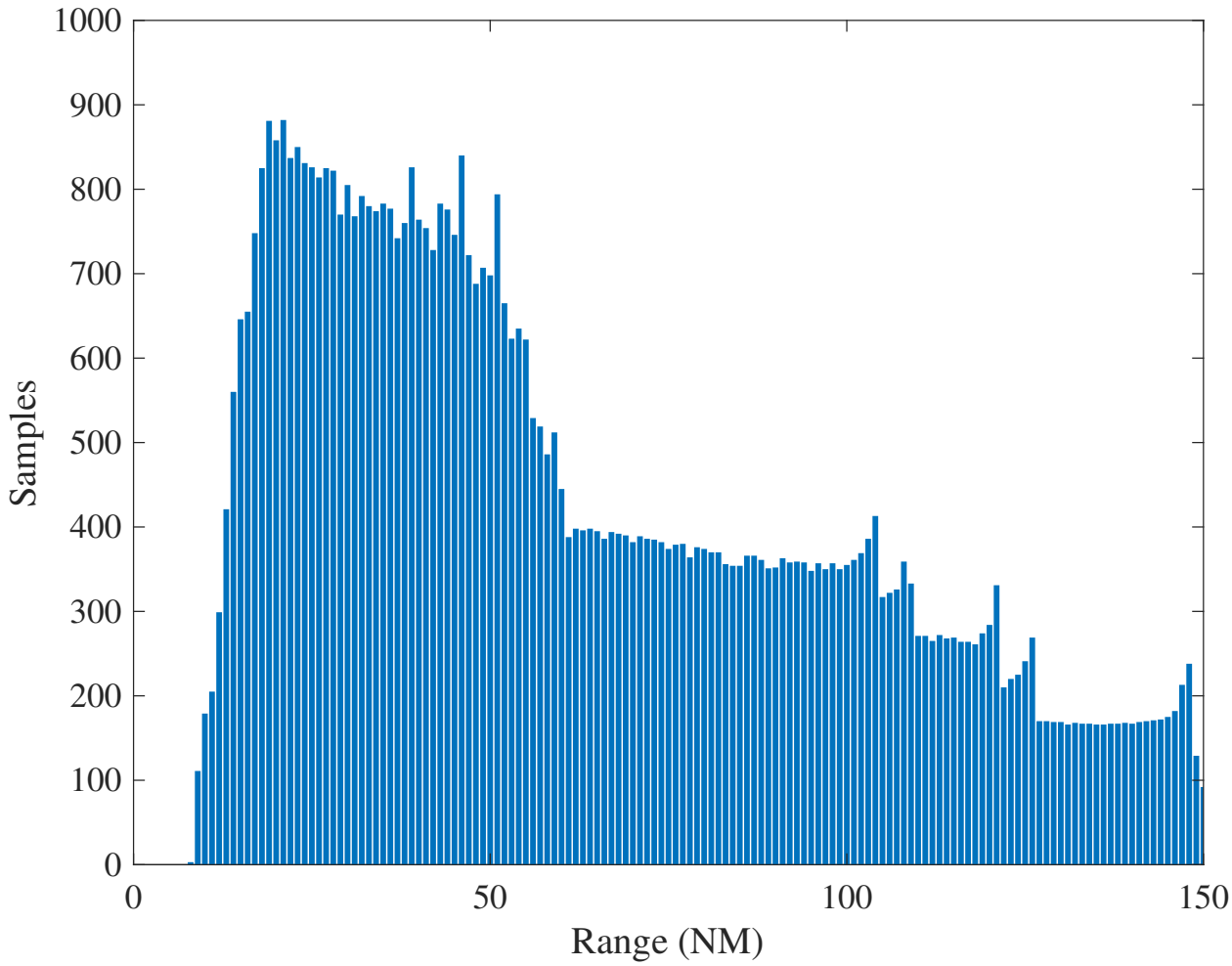


Figure D6 Number of Packets Transmitted (Samples) in Each 1 NM Range Bin

APPENDIX E – ANALYSIS TECHNIQUES

INTRODUCTION

This section applies to the first general test objective regarding the quantitative analysis of collected data and the creation of final data products. The model determined from the test data is a logistic regression model of PER or HER.

After each flight, a log of transmitted files was transferred from the test aircraft and from the four receivers. A MATLAB script loaded both datasets and compared the transmitted messages to the received messages. The MATLAB code processed the data using the logistic regression model outlined in the model determination section, below. The code presented plots of PER and HER for all combinations of predictors, and can be found in appendix H. Statistical level of confidence was determined per the assessment of success section below.

DATA ACQUISITION AND TRANSFORMATION

Each flight produced transmit (Tx) and receive (Rx) logs containing all messages transmitted from the aircraft and received at both ground station sites. In total, each flight generated five separate logs:

- Tx Log
- Rx Log - Low FRUIT / Omni Antenna
- Rx Log - Low FRUIT / Directional Antenna
- Rx Log - High FRUIT / Omni Antenna
- Rx Log - High FRUIT / Directional Antenna

Entries in each Tx log consisted of position, Tx rate, and packet contents, while entries in each Rx log contained position, FRUIT environment, antenna type, and packet contents. Reference figure E1 for the contents of Tx and Rx logs. The Tx rate was unchanged throughout the test, so in post-processing the Tx rate field was replaced with a direction of flight field, determined by whether aircraft range from the receiver sites was increasing or decreasing. Aircraft position was determined using the Dual XGPS160 SkyPro GPS Receiver and integrated into the Tx logging function. Position of the ground station sites was hard coded prior to each flight.

Tx Log		
Position	Tx Rate	Packet

Rx Log			
Position	FRUIT Enviro	Antenna Type	Packet

Figure E1 Transmit and Receive Log Contents

Additionally, the data field (ME field) within each packet contained Tx rate, Julian date (day, hour, minute, second, millisecond), key handoff attempt number, and packet sequence number (1-12). Reference figure E2. The Julian date provided two things, a time stamp of the current message, and an identifier unique to each message eliminating any potential comparison collisions that might have delayed post-processing and data analysis.

Post-processing occurred at the end of each flight. All log files were consolidated into a single Tx and single Rx data file containing meta data on all packets sent across all completed flights. For each entry in the consolidated Tx file, or each transmitted packet, a search was conducted on the Rx file looking for entries

TxR	Day	Hour	Minute	Second	Millis	Attempt	Sequence

Figure E2 Data Field Contents

that matched its unique data contents. A match indicated successful packet transmission, a failed search indicated an error in transmission.

Following this analysis, the correlated data was stored in a single Model Input file containing range, FRUIT environment, direction of flight, antenna type, and success/error for each packet sent. This data file included the entire sample population to be used in the calculation of PER and HER, and the generation of a regression model. Reference figure E3 for the overall data transformation process.

Tx Log		
Position	Tx Rate	Packet

+

Rx Log			
Position	FRUIT Enviro	Antenna Type	Packet

⇓

Model Input				
Range	FRUIT Enviro	Antenna Type	Tx Rate	Success

Figure E3 Data Transformation

The final data products are a model of PER and HER as a function of range, FRUIT environment, antenna pattern, and direction of flight. The model was used to generate plots of PER and HER versus range, in nautical miles, for the different factors.

MODEL DETERMINATION

In the case of a model for PER and HER, the response variable had two categories, *success* or *error*. As discussed above, the model had the following predictors:

- Range (Continuous: 8-150 NM)
- FRUIT Environment (Categorical: High, Low)
- Antenna Pattern (Categorical: Omni, Directional)
- Direction of Flight (Categorical: Inbound, Outbound)

Given these properties and the binary success/error outcomes, the appropriate analysis tool was a logistic regression model. Sample success/failure data and the resulting logistic regression output from that data can be seen in figure E4.

The *mnrfit* function performed a multinomial logistic regression and output a β coefficient matrix. The *mnrval* function took the coefficients as inputs and computed the predicted probabilities for the desired predictors and regression.

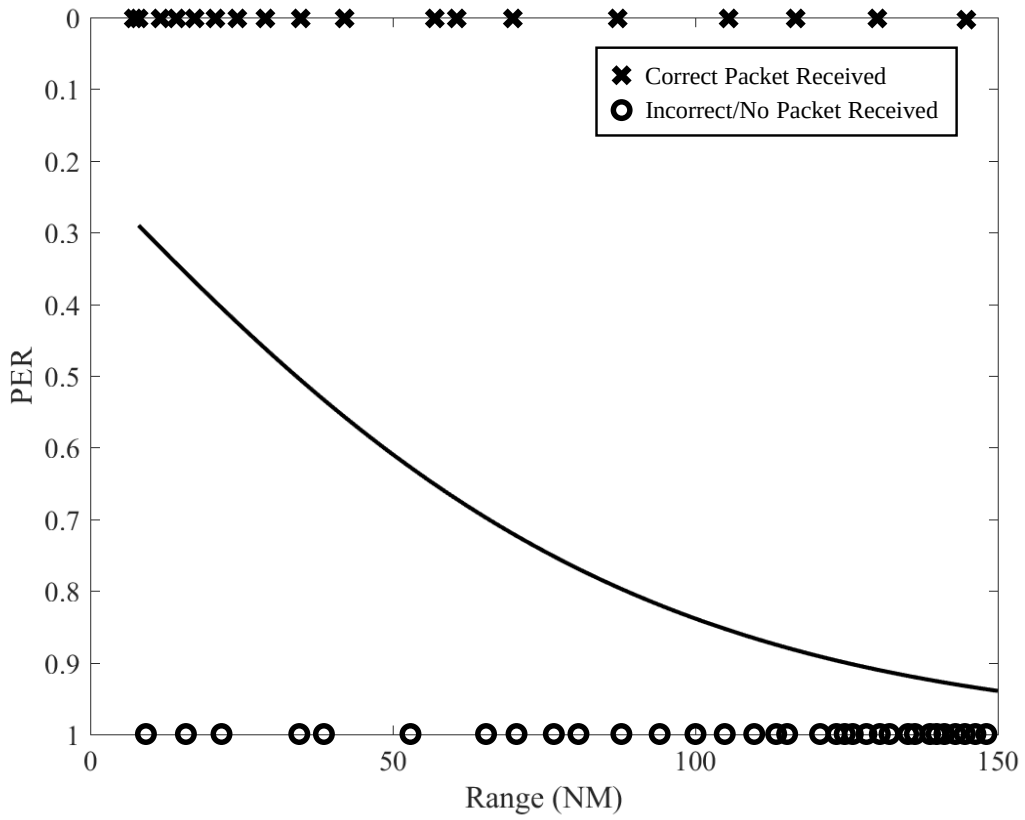


Figure E4 Sample Logistic Regression Model

HER was also determined analytically as a function of PER. Statistically, once the success rate (1 - PER) for a single packet was determined, the success rate for a 12-packet handoff was determined using the equation:

$$HER = 1 - (1 - PER)^{12}$$

ASSESSMENT OF SUCCESS

Statistical Level of Confidence

In the Mode S digital communications system, PER and HER are estimated probabilities of error. A packet or handoff transmitted through the system could be falsely represented when reconstructed at the receiver. The quality of estimation increases as the number of samples, n increases. As $n \rightarrow \infty$, the estimation perfectly models the actual probability of error. Statistical level of confidence (SLC) is the probability, based on a set of measurements, that the actual probability of error is greater than or less than a target or desired value.

Calculation of SLC was based on the distribution function, expressed as:

$$P_n(k) = \frac{n!}{k!(n-k)!} p^k q^n - k$$

where k is the number of errors in n attempts, p is the probability of an error, and $q = 1 - p$ is the probability of a non-error.

The cumulative binomial distribution gave the error rate, $P(e)$ when more or less than N events occurred in n attempts:

$$P(e \leq N) = \sum_{k=0}^{N} \frac{n!}{k!(n-k)!} p^k q^{n-k}$$

$$P(e > N) = \sum_{k=N+1}^{n} \frac{n!}{k!(n-k)!} p^k q^{n-k}$$

Using the cumulative distribution function, the level of confidence was:

$$SLC = P\Big(e > \frac{N}{p_h}\Big) = 1 - \sum_{k=0}^{N} \frac{n!}{k!(n-k)!} p_h^k (1-p_h)^{n-k}$$

Rearranging and using a natural logarithmic approximation for the cumulative distribution gave the total number of samples required for a given level of confidence:

$$n = \frac{1}{P(e)} \Bigg[-\ln(1 - SLC) + ln\Bigg(\sum_{k=0}^{N} \frac{(n \cdot P(e))^k}{k!} \Bigg) \Bigg]$$

where n is the number of samples required, $P(e)$ is the probability of error (PER or HER), and N is the total number of detected errors.

APPENDIX F – LESSONS LEARNED

MODIFICATION PROCESS

It is best to separate a discussion on the inefficiencies and failures of the modification process into two parts: that of TPS/XP, TPS/TS, and 812 AITS/ENI and that of 412 MXI. Significant inefficiency and poor prioritization were existent in 412 MXG throughout the modification process. A discussion of particulars and potential fixes is beyond the scope of this section.

The issues involving TPS and ENI boil down to an over tasking of available personnel with TPS modification projects. During the six to nine months prior to Have Crypto execution, TPS/TS and ENI were involved with: four TMPs, two C-12 depot exchanges, and the implementation of instrumentation to support the structures curriculum sortie. The resources do not exist to support these simultaneous efforts. Furthermore, Have Crypto was acknowledged to be an effort with well above average workload; it required six modification packages. Several of these were new efforts, the most significant being the mounting of RASCAL and ALQ-188 pods on the T-38C. In the future, TPS/XP should work with ENI to gain a realistic expectation of available personnel resources. They should also evaluate the impact of sequential TMP execution cycles upon each other. Furthermore, unusual or first-of-a-kind projects should not be scheduled simultaneously with other projects.

One efficiency gained in the modification process was the use of previous approvals to equip the T-38C rear cockpit with a Getac tablet computer. Unfortunately, the approved tablet lacked the performance necessary to achieve all test objectives. While the test team failed to identify this early in the modification process, there was pressure against seeking approval for alternative devices. In future projects, it is imperative to determine equipment performance requirements and seek approvals as necessary to meet them.

MATLAB

MATLAB is not capable of implementing a pipelined architecture, a feature critical for the implementation of real-time radio reception. It was desired to use MATLAB to enable participation of all team members and ability to use multiple computers to process data. This resulted in a limitation discussed in the body of the report. TPS should support the use of alternative programming languages to accomplish projects. This will become more important as the Air Force Test Center (AFTC) continues to grow into a cyber test organization.

ANTENNA CHARACTERIZATION

As detailed in the test results, the outbound PER compared to the inbound PER showed a significant difference. This was attributed to an asymmetric antenna pattern despite the antenna being marketed as a dipole antenna with equal power output at all azimuths. However, this could not be definitively proven due to a lack of testing and characterization of the actual antenna pattern. Future test teams should utilize anechoic chambers and other measurement facilities to characterize antennas before comencement of testing.

UNITED STATES FOREST SERVICE COORDINATION

The ground receiver sites used for GTO 1 were both located on United States Forest Service (USFS) land and therefore required permission and coordination for land and facility use. This was a lengthy, multi-month process, largely driven by miscommunication and confusion on who the proper authority at the USFS was for the specific Have Crypto test. Once the proper authority was determined, the approval process took approximately 2 weeks. Had this test not been as limited as it was, the process could potentially have taken several months, requiring complicated special permits and having to go through more official channels. After coordination with the specific National Forest (San Bernardino) Special Uses Permit Administrator,

the USFS decided the test fell under a ”nominal effect” category allowing the District Ranger to simply sign a letter giving the test team permission to use USFS land.

Additionally, there were other layers of coordination required for execution beyond approval to conduct testing on USFS land. This included fire tower and airspace coordination through the Lookout Volunteer Coordinator and Aviation Management Officer respectively. The fire towers are staffed on a daily basis with volunteers who are friendly and more than willing to help; however, official coordination is still highly desired. The Aviation Management Officer did not directly control or regulate the airspace over the National Forest, however, if there had been a forest fire during the test window, they would have taken control through the use of a fire traffic area (FTA) or more restrictive temporary flight restriction (TFR). With prior coordination and real time radio contact, air assets could theoretically still operate as planned given there was no conflict with higher priority firefighting assets.

APPENDIX G – AREAS OF FUTURE RESEARCH

- Determine PER for ranges between zero and eight NM
- Determine PER and HER using production transmitters and receivers
- Demonstrate random number generation in various avionics systems
- Determine spectrum saturation impacts when increasing Mode S transmission rate
- Observe spoofing operations in multi-aircraft, dynamically generated scenarios
- Verify the entropy of various FPE algorithms

This page was intentionally left blank.

APPENDIX H – DIGITAL DATA

The digital appendix H is available and contains the following file structure. File names are in descriptive plain english.

- **Raw Data**
  - **Logs**: the files detailed in figures E1 and E3
  - **Model Input**: the file detailed in the last step of figure E3
- **Videos**
  - **Compilations**: recordings pieced together and played at various speeds
  - **Screen Captures**: time synchronized raw recordings of the various devices used during GTO 2

This page was intentionally left blank.

APPENDIX I – DEFINITIONS

Advanced Encryption Standard	Specification for data encryption established by the U.S. National Institute of Standards and Technology
Asymmetric Encryption	Public and private key pairs are used to allow different keys for encryption and decryption of a message
Connectionless	One way data transmission with no acknowledgement of successful receipt
CRC	Cyclical redundancy check, a mathematical scheme which uses a checksum to detect bit errors in a received message
Format Preserving Encryption	Ciphertext has the same format as the input (plaintext), e.g., a social security number would have 9 digits when encrypted
FRUIT	False replies unsynchronized in time, a type of destructive radio interference
Handoff	Successful transmission of 12 sequential Mode S-ES packets
Handoff Error Ratio	The number of incorrectly received handoffs (12 packets) divided by the total number of handoff attempts
Key Handoff	Unidirectional transmission of cryptographic key
Mode S	Secondary radar process that allows selective interrogation of aircraft via the unique address assigned to each aircraft
Mode S-ES	112 bit Mode S message used to implement ADS-B
Packet	Formatted unit of data that contains control information and data payload
Packet Error Ratio	The number of incorrectly received data packets divided by the total number of attempted packet transmissions
Packet Switching	Spreading contiguous data across multiple packets
Session Symmetric Key	Single use symmetric key used for encryption during one communication session
Stateless	No return data channel for acknowledgement
Symmetric Encryption	Same cryptographic key used for message encryption and decryption

This page was intentionally left blank.

APPENDIX J – ABBREVIATIONS, ACRONYMS, AND SYMBOLS

Abbreviation	Definition	Units
ADS-B	automatic dependent surveillance-broadcast	—
AES	Advanced Encryption Standard	—
AFB	Air Force Base	—
AFTC	Air Force Test Center	—
AIMS	ATCRBS, IFF, Mark XII/XIIA SPO	—
ATC	air traffic control	—
ATCRBS	air traffic control radar beacon system	—
BER	bit error rate	—
CAA	civil aviation authority	—
CNS	Communication, Navigation, and Surveillance	—
CRC	cyclic redundancy check	—
DF	downlink format	—
DoD	Department of Defense	—
EATS	Experimental ADS-B Testbed System	—
ECM	electronic counter measures	—
EHS	enhanced surveillance	—
ELM	extended length message	—
EO	electro-optical	—
ES	extended squitter	—
EUROCAE	European Organisation for Civil Aviation Equipment	—
FAA	Federal Aviation Administration	—
FEC	forward error correction	—
FIPS	Federal Information Processing Standards	—
FPE	format preserving encryption	—
FRUIT	false replies unsynchronized in time	—
FTA	fire traffic area	—
GNSS	global navigation satellite system	—
GTO	general test objective	—
GUI	graphical user interface	—
HER	handoff error ratio	—
IBE	identity-based encryption	—
ICAO	International Civil Aviation Organization	—
IFF	identification friend or foe	—
IFR	instrument flight rules	—
KGS	knots ground speed	—
LA	Los Angeles	—
LOS	line-of-sight	—
MATLAB	Matrix Laboratory	—
MIT	Massachusetts Institute of Technology	—
Mode S-ES	Mode S - Extended Squitter	—
MSL	mean sea level	—
NIST	National Institute of Standards and Technology	—
NM	nautical mile	—
NORAD	North American Aerospace Defense Command	—
PER	packet error ratio	—
PKI	public key infrastructure	—
PPM	pulse position modulated	—
RA	resolution advisory	—

Abbreviation	Definition	Units
RAF	Royal Air Force	—
RASCAL	Reconfigurable Airborne Sensor, Communication, and Laser	—
RF	radio frequency	—
RTCA	Radio Technical Commission for Aeronautics	—
Rx	receive	—
SBAS	space-based augmentation system	—
SDR	software defined radio	—
SLC	statistical level of confidence	—
SPO	system program office	—
SSK	session symmetric key	—
SSR	secondary surveillance radar	—
STO	specific test objective	—
SUAS	special use airspace	—
SUIA	session unique ICAO address	—
SUT	system under test	—
TCAS	traffic collision avoidance system	—
TFR	temporary flight restriction	—
TIS-B	traffic information service broadcast	—
TMP	test management project	—
TPS	Test Pilot School	—
Tx	transmit	—
UAT	universal access transceiver	—
US	United States	—
USAF	United States Air Force	—
USFS	United States Forest Service	—
VFR	visual flight rules	—

APPENDIX K – DISTRIBUTION LIST

Onsite	Number of Copies		
	E-mail	Digital	Paper
Test Pilot School Attn: David Vanhoy 220 Wolfe Ave Edwards AFB, CA 93524		1	
AFTC/CA Attn: Eileen Bjorkman 1 S Rosamond Blvd Edwards AFB, CA 93524		1	
Edwards AFB Technical Research Library Attn: Darrell Shiplett 307 E Popson Ave Edwards AFB, CA 93524		1	
411 FLTS/ADO Attn: Brandon Burfeind 411 FLTS Edwards AFB, CA 93524		1	
Offsite			
Defense Technical Information Center Attn: DTIC-O 8725 John J. Kingman Rd, Ste 0944 Ft Belvoir, VA 22060 Email: aq@dtic.mil		1	
AFIT/ENG Attn: Bob Mills 2950 Hobson Way WPAFB, OH 45433		1	
AFRL/RY Attn: RYWA 2241 Avionics Circle Bldg 620 WPAFB, OH 45433		1	
Total	0	7	0