INTEROPERABLE ADS-B CONFIDENTIALITY

THESIS

Brandon C. Burfeind, Major, USAF

AFIT-ENG-MS-20-M-009

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

INTEROPERABLE ADS-B CONFIDENTIALITY

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Brandon C. Burfeind, BS, MS

Major, USAF

March 2020

AFIT-ENG-MS-20-M-009

INTEROPERABLE ADS-B CONFIDENTIALITY

Brandon C. Burfeind, BS, MS
Major, USAF

Committee Membership:

Robert F. Mills, PhD
Chair

Col Eric D. Trias, PhD
Member

Scott L. Nykl, PhD
Member

Maj J. Addison Betances, PhD
Member

AFIT-ENG-MS-20-M-009

Abstract

The worldwide air traffic infrastructure is in the late stages of transition from legacy transponder systems to Automatic Dependent Surveillance - Broadcast (ADS-B) based systems. ADS-B relies on position information from GNSS and requires aircraft to transmit their identification, state, and position. ADS-B promises the availability of high-fidelity air traffic information; however, position and identification data are not secured via authentication or encryption. This lack of security for ADS-B allows non-participants to observe and collect data on both government and private flight activity. This is a proposal for a lightweight, interoperable ADS-B confidentiality protocol which uses existing format preserving encryption and an innovative unidirectional key handoff to ensure backward compatibility. Anonymity and data confidentiality are achieved selectively on a per-session basis. This research also investigates the effect of false replies unsynchronized in time (FRUIT) on the packet error ratio (PER) for Mode S transmissions. High PERs result in range and time limits being imposed on the key handoff mechanism of this proposal. Overall, this confidentiality protocol is ready for implementation, however further research is required to validate a revised key handoff mechanism.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

8PSK eight phase shift keying

ADS-B automatic dependent surveillance-broadcast

AFB Air Force Base

AIMS air traffic control radar beacon system (ATCRBS), identification friend or foe

   (IFF), Mark XII/XIIA system program office (SPO)

ATC air traffic control

ATCRBS air traffic control radar beacon system

AWGN additive white Gaussian noise

BER bit error rate

CAA civil aviation authority

CRC cyclic redundancy check

CSPRN cryptographically secure pseudo-random number

DF downlink format

DoD Department of Defense

DoDAF Department of Defense (DoD) Architecture Framework

DoS denial of service

DPSK differential phase-shift keying

EATS Experimental ADS-B Testbed System

EHS enhanced surveillance

ELM extended length message

ES extended squitter

EUROCAE European Organisation for Civil Aviation Equipment

FAA	Federal Aviation Administration
FEC	forward error correction
FIPS	Federal Information Processing Standards
FMS	flight management system
FPE	format preserving encryption
FRUIT	false replies unsynchronized in time
GA	general aviation
GNSS	global navigation satellite system
GPS	Global Positioning System
GUI	graphical user interface
HAE	height above ellipsoid
HER	handoff error ratio
I/Q	in-phase and quadrature
ICAO	International Civil Aviation Organization
IFF	identification friend or foe
IFR	instrument flight rules
IP	Internet Protocol
KTAS	true airspeed
LA	Los Angeles
LOS	line-of-sight
MATLAB	Matrix Laboratory
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
RAF	Royal Air Force
RASCAL	Reconfigurable Airborne Sensor, Communication, and Laser
RF	radio frequency
RTCA	Radio Technical Commission for Aeronautics
Rx	receive
SARPs	Standards and Recommended Practices
SDR	software defined radio
SIBE	staged identity based encryption
SLC	statistical level of confidence
SNR	sigal-to-noise ratio
SPO	system program office
SSK	session symmetric key
SSR	secondary surveillance radar
SUIA	session unique ICAO address
TCAS	traffic collision avoidance system
TESLA	timed efficient stream loss-tolerant authentication
TIS-B	traffic information service broadcast
TMP	test management project
TPS	Test Pilot School

Tx   transmit

UAT   universal access transceiver

UDP   user datagram protocol

US   United States

USAF   United States Air Force

USB   universal serial bus

VFR   visual flight rules

WGS-84   World Geodetic System

I. Introduction

1.1 Motivation

A rash of mid-air collisions occurred in American skies during the late 1950s and early 1960s. These prompted the development and deployment of widespread air surveillance infrastructure. This system was called the air traffic control radar beacon system (ATCRBS) and was the first major development in civil air surveillance. As the volume of air traffic has increased over time there has been a continued need for modernization of the surveillance infrastructure [2].

Automatic dependent surveillance-broadcast (ADS-B) is the future of air surveillance and collision avoidance and is implemented by the Mode S - Extended Squitter (Mode S-ES) protocol. ADS-B is a means by which aircraft self report position and other data, allowing precise surveillance for air traffic control (ATC). The Federal Aviation Administration (FAA) includes the technology in its "Next Generation Air Transportation System

Figure 1. Deadly Collision, 31 Jan 1957 [1]

(NextGen)" technology suite, designed to make air transportation safer and more efficient. The International Civil Aviation Organization (ICAO) and at least 19 nations require its use. The paradox of ADS-B is that it implements modern and future applications with legacy digital communications technology in an already congested spectrum. Chapter II will discuss this history and show that a focus on backward compatibility for any additions to Mode S-ES is important to gain acceptance among regulators and users.

This paradigm leaves the global air transport system with dated technology that is asked to carry growing amounts of data. Innovative methods are used to include information such as identification, precise location, and status in broadcast data packets. This data is transmitted without security considerations. Any entity, malicious or not, with a software defined radio (SDR) (available for under $20) can trivially receive and decode messages from any aircraft within line-of-sight [3]. This enables real-time precision tracking of any aircraft transmitting ADS-B. This data is aggregated and made publicly available by numerous crowdsourcing applications such as FlightRadar24 and FlightAware, increasing coverage beyond line-of-sight. Figure 2 shows the coverage of FlightAware's ADS-B reception network. State-sponsored intelligence services with advanced capabilities can easily and quickly gather precise and accurate data on sensitive platforms and operations.
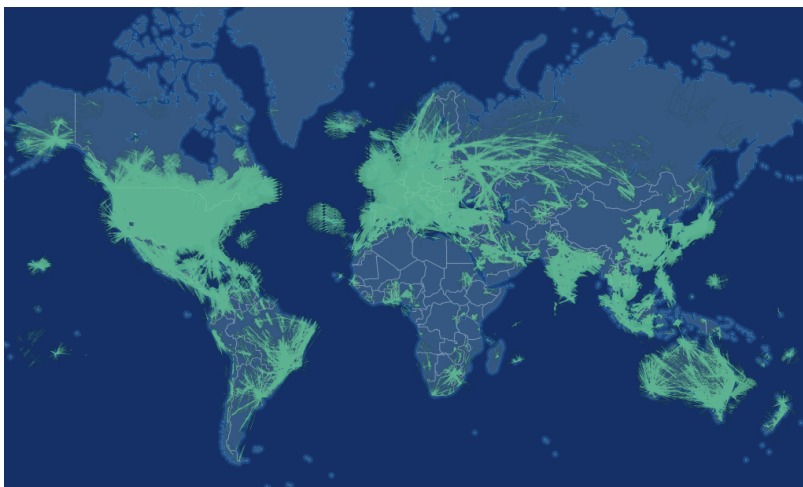
Figure 2. FlightAware Coverage

Further, the lack of ADS-B integrity provisions allow malicious entities opportunity to inject false data into the network. This data can cause denial of service, inclusion of nonexistent tracks, or modification of legitimate tracks. Figure 3 shows a real-world example of one real aircraft injecting seven false tracks [4]. With very limited resources, an entity can do this or launch other cyber attacks detailed in Chapter II.
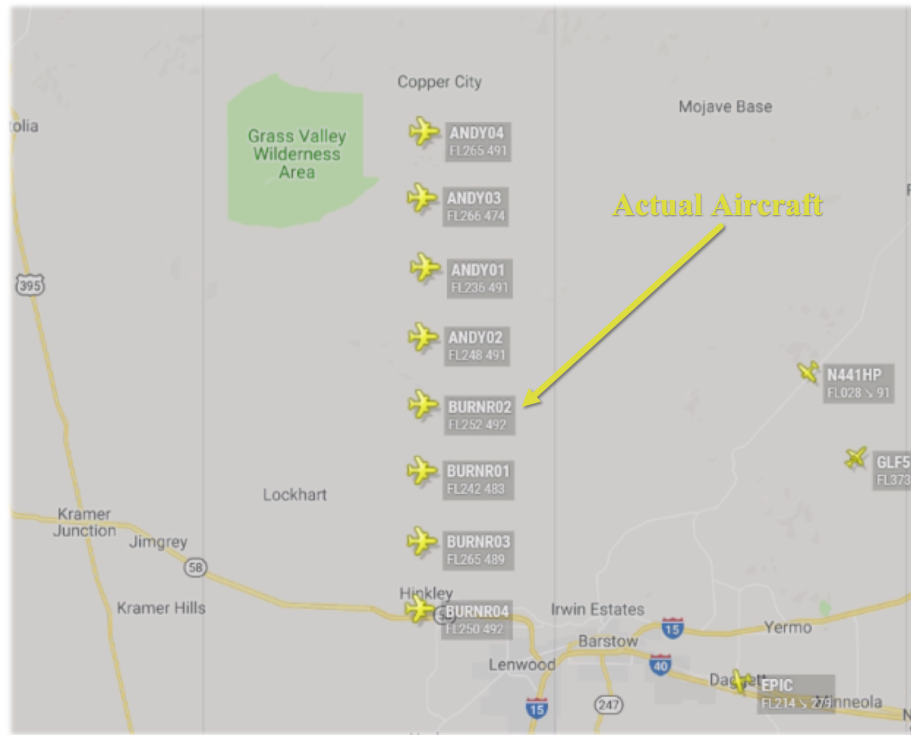
Figure 3. Spoofed ADS-B Tracks

Most industry stakeholders are concerned, in some respect, with security. Those involved in aviation generally maintain safety as their primary objective. For these entities, including civil aviation authorities (CAAs) and airlines, they may only be concerned with security as far as it impacts safety. Their efforts to improve ADS-B security are likely focused on integrity issues. Others, such as military, government, intelligence, corporate, or privacy conscious general aviation (GA) operators, will often have a desire for confidentiality or privacy while retaining safety as the primary goal. Figures 4, 5, and 6 show instances of potentially sensitive missions being monitored in real-time via crowdsourcing networks.

3

United States (US) national leadership, as well as defense and intelligence organizations, have a serious concern with the future of insecure and easily aggregated surveillance data [5]. In the past, adversaries desiring this level of data would spend enormous sums to gain access to data they can now access for free.

The research herein focuses primarily on the mitigation of vulnerabilities imposed on ADS-B by its lack of confidentiality provisions.
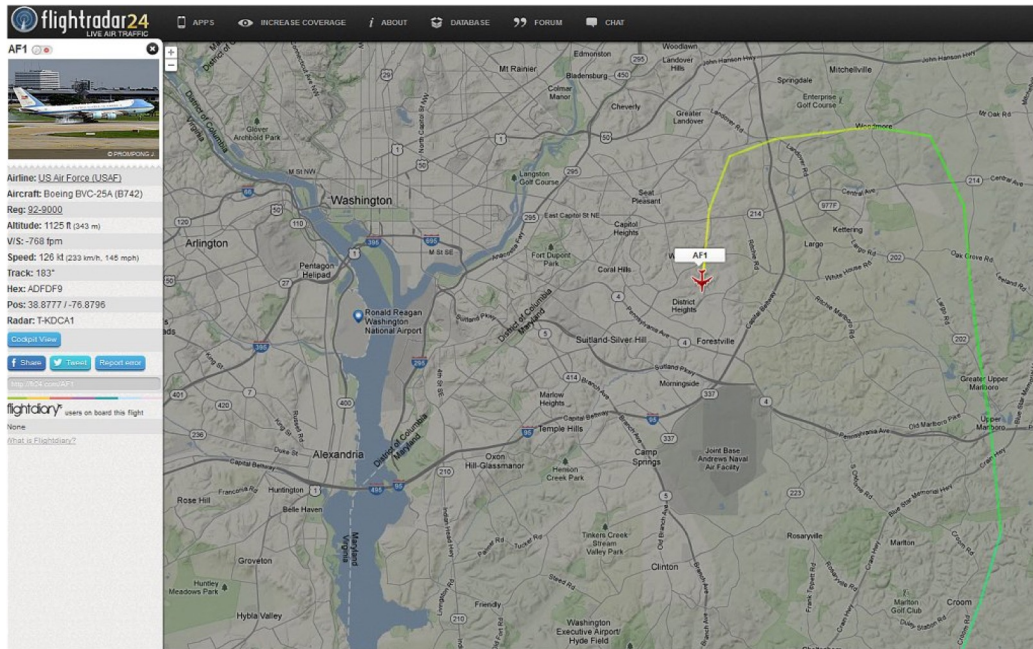
Figure 4. Air Force One
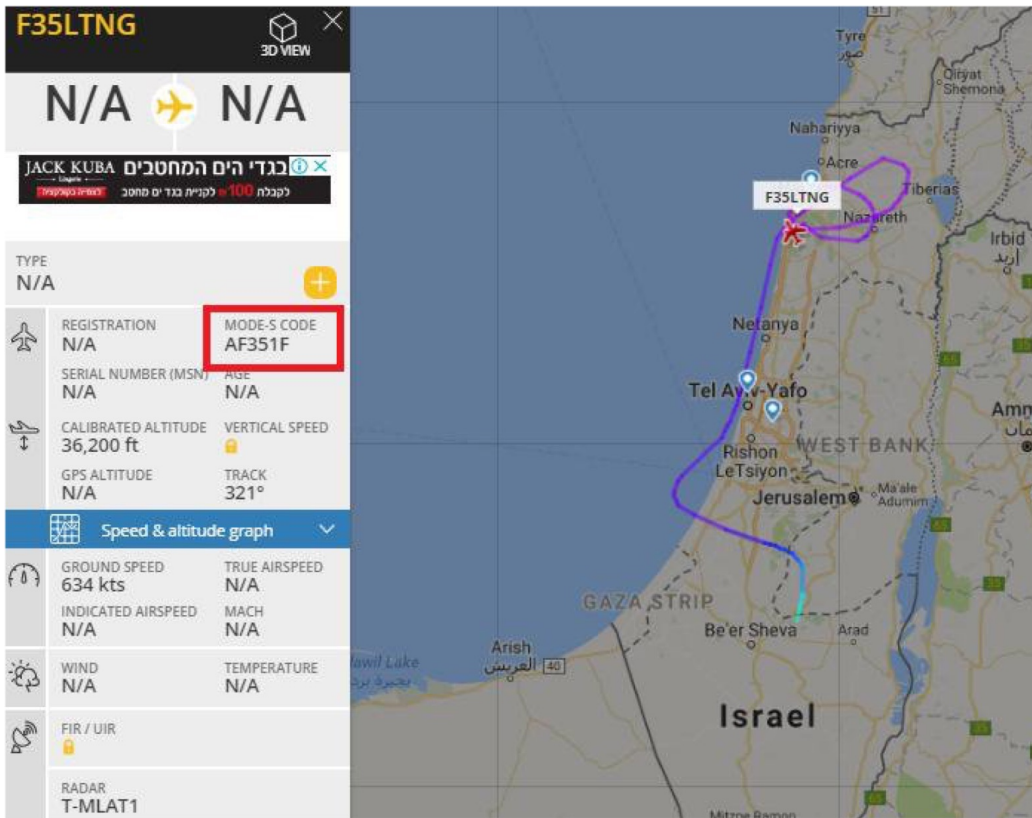
Figure 5. Israeli F-35 - USAF ICAO Address
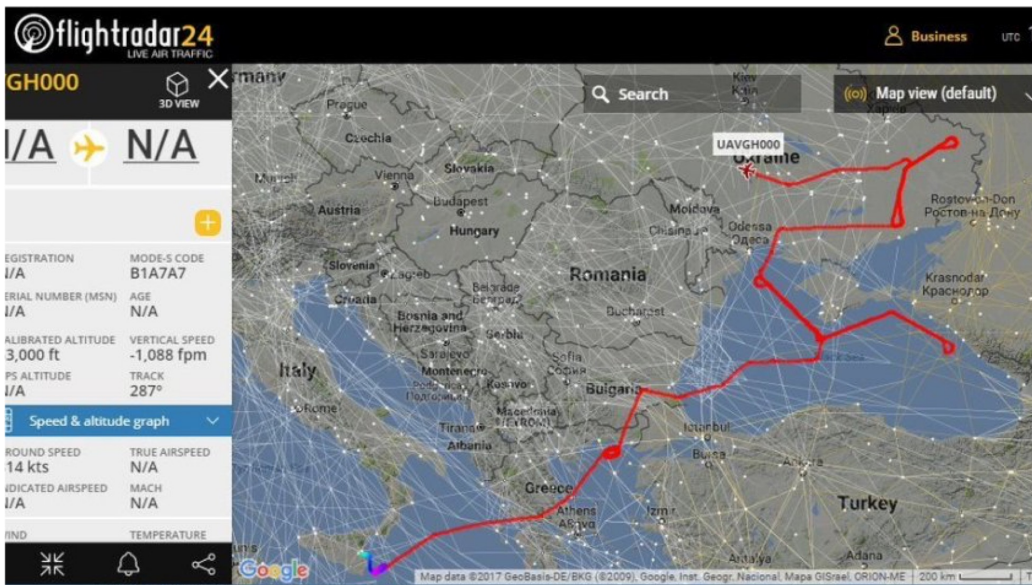
Figure 6. RQ-4 Over the Black Sea

1.2 Research

This research involves the fields of cyber security, digital communications, and aviation with focus on two primary research questions:

1. How can Mode S-ES be extended to allow confidential operations without requiring a change to existing standards while retaining interoperability with existing systems?

2. What is the open-air Mode S-ES link performance and how does this impact the real-world implementation of the proposed protocol?

Developing a security protocol is an applied research effort which continues previous work in security and cryptography and implements systems engineering processes. The resulting security protocol makes use of the ability to conduct packet switching over a binary pulse position modulated (PPM) radio frequency (RF) signal on 1090 MHz. The open-air characterization of this channel is a use-inspired basic research [6]. It seeks fundamental understanding while considering use cases, one of which is ADS-B. This research will increase general knowledge regarding the waveforms of interest in the real world while serving as a new performance metric for Mode S-ES.

Preparatory work is critical to enable this and follow on research involving ADS-B. This includes:

- Development and fielding of the Experimental ADS-B Testbed System (EATS)

- Integration of EATS with a carriage aircraft

Open-air test missions required to gather experimental data for stateless packet switching research were conducted during Project Have Crypto. Have Crypto was a test management project (TMP) executed at the United States Air Force (USAF) Test Pilot School (TPS).

1.3 Results

This research was successful in developing a confidentiality protocol for Mode S-ES. The resulting proposal meets the requirements laid out in Chapter III. Its current form requires no changes to Mode S-ES specifications.

The effort to characterize stateless packet switching performance was marginally successful. Sufficient data was gathered to partially determine link performance, however constraints imposed by external processes place certain limits on data usability. Details of these limitations are in Chapter IV.

1.4 Organization

This document is organized to effectively show the development of the security protocol along with the enabling packet error ratio (PER) research. Chapter II will discuss a brief history, information security principles, previous ADS-B security work, and a discussion of how security principles relate to ADS-B. This discussion is critical to the process presented in Chapter III. Chapter III is dedicated to the process of decomposing security principles, determining requirements, and designing a protocol with which to implement privacy and confidentiality for Mode S-ES. Chapter IV gives methodology, results, and analysis of experimental link performance determination. Analysis includes a discussion on the viability of connectionless packet switching over binary PPM physical channels. Chapter V brings the two lines of effort together and proposes follow on research related to this work.

II. Background

2.1 Air Surveillance History

Chapter I noted that legacy technology is a significant factor in the lack of security for ADS-B. The use of legacy technology in modern "next generation" air surveillance systems is brought about by a continuous need for backward compatibility.

2.1.1 Identification Friend or Foe (IFF).

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 [7]. Eventually, this challenge and response system allowed the directional replies to be correlated with radar, giving a more accurate picture of participating aircraft. The original IFF system was extended into the military system of today, using the various modes detailed in Table 1.

Mil Term	Civil Term	Type	Data
Mode 1	-	Interrogate/Reply	2-Digit Octal
Mode 2	-	Interrogate/Reply	4-Digit Octal
Mode 3/C	Mode A/C	Interrogate/Reply	4-Digit + Altitude
Mode 4	-	Interrogate/Reply	Encrypted Pulse Train
-	Mode S	Interrogate/Reply	See RTCA DO-181 [8]
-	Mode S-ES	Broadcast	See RTCA DO-260 [9]
Mode 5	-	Both	Encrypted Mode S & ES

Table 1. IFF Modes

2.1.2 Air Traffic Control Radar Beacon System (ATCRBS).

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 uses 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.

2.1.3 Mode S.

Mode S developed due to frequency overloading and garbling which occurred as air traffic grew. The major change, which allowed additional growth, was a selective addressing scheme: interrogations can be directed to an individual aircraft. A major requirement for Mode S was backwards compatibility with ATCRBS. The committee which developed mode S "concluded that incremental upgrade was feasible, and the the benefits of reduced risk and cost outweighed the increased design difficulty of the new system [2]."

2.1.4 Automatic Dependent Surveillance - Broadcast (ADS-B).

Mode S-ES was the MIT Lincoln Labs submission for use as an ADS-B standard. Developed as an extension of Mode S, it favored backwards compatibility over new technology. The Mode S-ES packet was increased in length from 56 to 112 bits to allow for the inclusion of global navigation satellite system (GNSS) based positioning information. Mode S-ES is the global standard for ADS-B.

The designs of each follow on technology: IFF, ATCRBS, Mode S, and ADS-B prioritized interoperability over new technology. This allows excellent safety features to propagate rapidly throughout the air transport industry. In many systems, safety and security are competing objectives. In aviation, they are more often directly correlated, necessitating a focus on modern security technology [10]. For more detailed history, see [2].

2.2 Mode S and ADS-B Basics

ADS-B is an air surveillance technology which both extends and is a subset of secondary surveillance radar (SSR) Mode S (Figure 7). A short technical background discussion is necessary to fully understand the impetus for, and results of, this research. More information can be found in the overview provided by the FAA [11] and the technical discussion by Sun [12].

2.2.1 ADS-B Technologies.

ADS-B as a technology stack is composed of several capabilities that differ in various properties of the physical, link, and presentation layers (Figure 7). Universal access transceiver (UAT) is an alternative implementation of ADS-B used in the US to relieve frequency congestion and allow for faster bit rates. It is used for air surveillance below 18,000 feet and the transmission of weather data to aircraft. Mode S-ES, also known as 1090ES, is an implementation of the Mode S protocol that implements ADS-B for most aircraft. In the case of this research, the term ADS-B refers to the Mode S-ES protocol in particular. UAT is not addressed, though many concepts and implementations are adaptable to it.
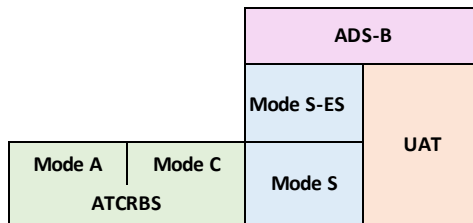
Figure 7. ADS-B Technology

2.2.2 Mode S Surveillance.

Mode S is a follow-on technology to ATCRBS which allows selective addressing of individual aircraft via a unique 24-bit *ICAO address*. Most of the various Mode S packet formats are used in an interrogate-response scheme. The extended squitter format is used in Mode S-ES, a broadcast scheme.

DF-0	0 0000	VS: 1	CC: 1	-1-	SL: 3	-2-	RI: 4	-2-	AC: 13	AP: 24	Short Air-Air Surv (ACAS)
DF-1	0 0010	*-27 or 83-*								P: 24	*Unused*
DF-2	0 0001	*-27 or 83-*								P: 24	*Unused*
DF-3	0 0011	*-27 or 83-*								P: 24	*Unused*
DF-4	0 0100	FS: 3		DR: 5		UM: 6		AC: 13		AP: 24	Surv Altitude Reply
DF-5	0 0101	FS: 3		DR: 5		UM: 6		AC: 13		AP: 24	Surv Identity Reply
DF-6	0 0110	*-27 or 83-*								P: 24	*Unused*
DF-7	0 0111	*-27 or 83-*								P: 24	*Unused*
DF-8	0 1000	*-27 or 83-*								P: 24	*Unused*
DF-9	0 1001	*-27 or 83-*								P: 24	*Unused*
DF-10	0 1010	*-27 or 83-*								P: 24	*Unused*
DF-11	0 1011	CA: 3		AA: 24						PI: 24	All-Call Reply
DF-12	0 1100	*-27 or 83-*								P: 24	*Unused*
DF-13	0 1101	*-27 or 83-*								P: 24	*Unused*
DF-14	0 1110	*-27 or 83-*								P: 24	*Unused*
DF-15	0 1111	*-27 or 83-*								P: 24	*Unused*
DF-16	1 0000	VS: 1	-2-	SL: 3	-2-	RI: 4	-2-	AC: 13	MV: 56	AP: 24	Long Air-Air Surv (TCAS)
DF-17	1 0001	CA: 3	AA: 24		ME: 56					PI: 24	Extended Squitter
DF-18	1 0010	CF: 3	AA: 24		ME: 56					PI: 24	Extended Squitter: Non-Txpdr
DF-19	1 0011	AF: 3	Military Application: 104								Military Application
DF-20	1 0100	FS: 3	DR: 5	UM: 6	AC: 13	MB: 56				AP: 24	Comm-B Alt Reply
DF-21	1 0101	FS: 3	DR: 5	UM: 6	ID: 13	MB: 56				AP: 24	Comm-B Identity Reply
DF-22	1 0110	*-27 or 83-*								P: 24	Reserved for Military
DF-23	1 0111	*-27 or 83-*								P: 24	*Unused*
DF-24	1 1	-1-	KE: 1	ND: 4	MD: 80					P: 24	Comm-D (ELM)

Figure 8. Mode S Reply Formats [8]

11

Figure 8 shows the various *downlink formats*, or DFs, which a Mode S packet may have. Note that ADS-B currently only uses DF-17 and DF-18. All remaining formats are used for other Mode S protocols or are unused. Mode S uplink (from the interrogator to the aircraft) takes place on 1030 MHz, is modulated with differential phase-shift keying (DPSK), and is not used in ADS-B.

2.3   Information Security & ADS-B

2.3.1   Previous Work.

Several excellent overviews have been published in the past, most notably Strohmeier, et al. in [13]. The purpose of this section is to build on Strohmeier's work and use decomposition of security principles to understand the precious work in ADS-B security.

2.3.2   Security Principles.

Traditional information security discussion will use the *CIA Triad* to frame security best practices [14]:

- **Confidentiality:** information is only accessed by entities with '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
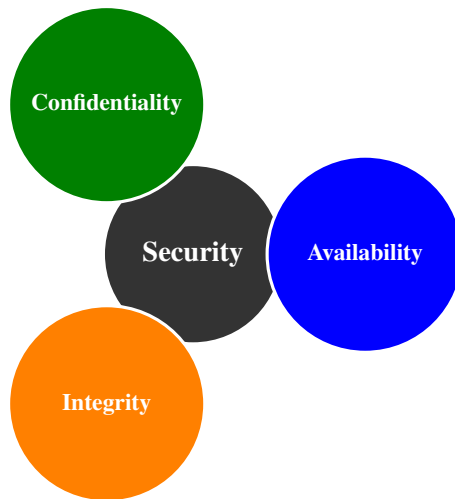
Figure 9. CIA Triad

In the realm of ADS-B it is helpful to further decompose these terms (Figure 10):
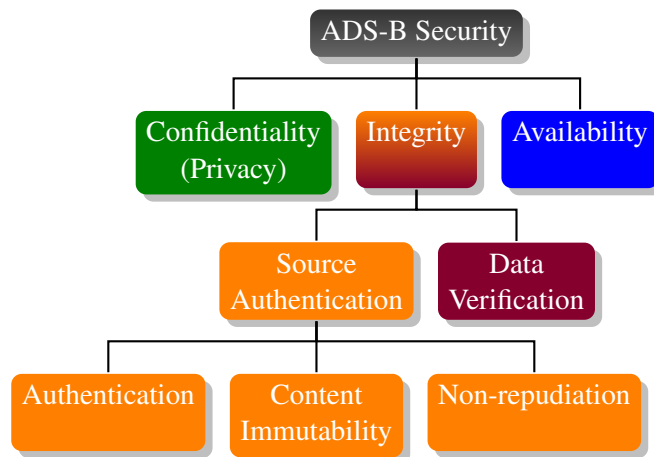
Figure 10. ADS-B Security Decomposition

2.3.2.1 Confidentiality.

ADS-B confidentiality, treated here as synonymous with privacy, 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 are many 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 for their movement or operation. This user requires the ADS-B data associated with them remain confidential, only revealed to those with need to know.

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.

2.3.2.2 Source Authentication.

The *integrity* of ADS-B data can be uniquely 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.

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.

2.3.2.3 Data Verification.

Data verification is is a concept added under the umbrella of integrity when using untrusted broadcast communications. Data verification ensures that the information transmit-

ted 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. A data verification scheme should also be able to verify other parameters such as track/heading, vertical speed, intent, etc. 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. Data verification is independent of source authentication; an unauthenticated source's data can be verified and verified data does not necessarily imply entity authentication, message immutability, or attribution.

2.3.2.4   Availability.

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. Only reductions in availability due to malicious activity are addressed here.

2.3.3   Attack Classification.

After describing the basic decomposition of security with regard to ADS-B, it is then useful to classify various attack types according to the security area they exploit. Figure 11 shows a simplified breakdown of various specific attack categories into overarching classes that generally correlate to the security principles discussed above. Further classification of some of these attacks based on severity and complexity can be found in [13]. This section focuses on attacks against the datalink segment of ADS-B. Network attacks against the ground infrastructure are beyond the scope of this section.

Figure 11. ADS-B Attack Classification

- **Eavesdropping** exploits the lack of a *confidentiality* scheme in ADS-B.

  - Preparatory reconnaissance sets the groundwork for a follow on attack [15].

  - Targeted collection seeks data about a certain platform, person, or organization.

  - Mass collection is used to determine pattern of operations or other information and is not necessarily nefarious.

- **Data Manipulation** exploits the lack of *source authentication* or *data verification*.

  - False Target Injection, also known as ghost aircraft injection, is the insertion of messages that cause a non-existent platform to appear within the ADS-B system. This target does not need to represent a certain aircraft and can be used to cause alternative behavior in controllers and platforms [3, 15, 16].

  - Spoofing, or impersonation, is the false target injection of a specific, existing, platform. Spoofing allows an attacker to show a certain platform taking a certain action. This can be used to create alternative behavior just like false target injection, but can potentially have more predictable and narrow effects. Alternatively, this attack can be used against the entity that controls the platform being spoofed [3].

  - Target Removal is a difficult attack that consists of the removal of a valid target from the displays of controllers and aircrew. While categorized as data manipulation due to its targeting of a specific platform, this attack requires precise positioning and has more in common with denial of service (DoS) attacks [17].

  - Target Data Modification is a combination of target removal and spoofing. By removing correct data and replacing it with spoofed data, an attacker can make it appear that an existing platform is taking an action which it is not [17].

  - Valid Target with False Data is an attack that can be accidental or purposeful. This is when a platform that exists and is the true transmitter of messages

17

places false content in those messages. Whether due to positioning inaccuracies, aircrew input errors, or a more nefarious purposes, this attack can lead to dangerous behavior modifications of controllers and other platforms.

– A Replay attack can be used to simplify the other types of attacks listed here but the attacker loses granular control over most variables [3]. A replay attack can also be a form of DoS.

• **Denial of Service** attacks attempt to disrupt the *availability* of ADS-B. This disruption may target a specific geographic location, time period, or platform. Its intent may be to cause confusion or alternative behavior among controllers. DoS may be used to enable or enhance other types of attack.

– Noise/Tone Jamming attempts to either overload the front end of receivers or raise the noise floor to the point that actual messages cannot be decoded [18]. The RF power required for this attack makes it either very difficult or very localized [15].

– Garbling is a form of jamming that makes use of the interference naturally present when several ADS-B and/or SSR transmissions overlap. The use of this interference to actively deny ADS-B reception to an entity or area constitutes an attack [18].

– Preamble Flooding is very similar to a garbling attack, however instead of causing interference that corrupts messages, it utilizes a string of Mode S preambles to overload the computational capability of the receiver's signal processor [18].

– Message Flooding is like preamble flooding but uses a train of full messages to target the application layer of the ATC system rather than the signal processor.

– Multiple False Target insertion is not intended to cause hardware or software failure, but to overload the human operator, namely a controller. Similar to false target injection, this attack is intended to cause cognitive overload to change behavior [15, 18].

It must be noted that while these attacks have been broadly classified according to the security principle they exploit, many of them cross the boundaries between attack classes. This should be taken into account when choosing or designing countermeasures.

2.4 Security Solutions

It is useful to discuss security solutions within the construct of security principles and attack classification. Some solutions mitigate attacks across classes while others have narrower focus.

2.4.1 Confidentiality Solutions.

Communications confidentiality can be ensured via properly implemented encryption that is open and reviewed [19]. The majority of ADS-B security solutions that address confidentiality utilize either symmetric or asymmetric cryptography.

Finke et al. analyzed the use of format preserving encryption (FPE) while acknowledging the difficulty of symmetric key distribution on an untrusted network [20]. Follow on work regarding the military applicability of symmetrically encrypted ADS-B was done in [21, 22]. Yang et al. utilize FPE in conjunction with timed efficient stream loss-tolerant authentication (TESLA) [7]. Baek, Hableel, et al. propose a staged identity based encryption (SIBE) construct [23] based on the work of Boneh and Franklin [24]. Several have explored various implementations of public key infrastructure (PKI) for use in ADS-B [13].

2.4.2 Integrity Solutions.

Strohmeier et al. explore source authentication and data verification solutions in depth [13]. They specifically divide their work into an exploration of "secure broadcast authentication", equivalent to *source authentication*, and "secure location verification", a subset of *data verification*. In the case of data verification, most efforts specifically seek location
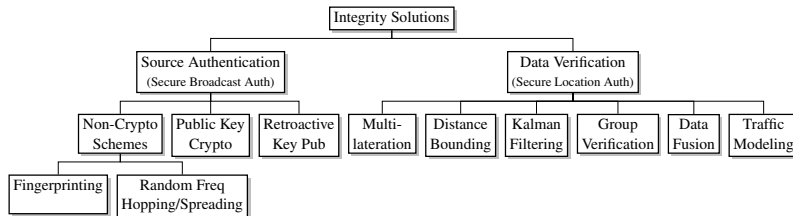
Figure 12. Taxonomy of ADS-B Integrity Solutions [13]

verification and we will treat these terms as synonymous. Note that there exists other data (callsign, intent, status) transmitted by ADS-B that ought to be verified as well. A thorough discussion of these techniques can be found in [13] and the references therein.

2.4.3 Availability Solutions.

Solutions to the problem of ensuring availability increase in difficulty with the sophistication of the attack. A discussion of anti-jam techniques is beyond the scope of this section.

2.4.4 Security Solution Distribution.

Figure 13 shows the distribution of current research into ADS-B security. It reveals that relatively few have done work in confidentiality; all of the proposals shown here require key distribution or significant changes to the current Mode S-ES specifications. **The result of Chapter III is different from previous solutions because it avoids both secure key distribution and changes to currently implemented specifications.**
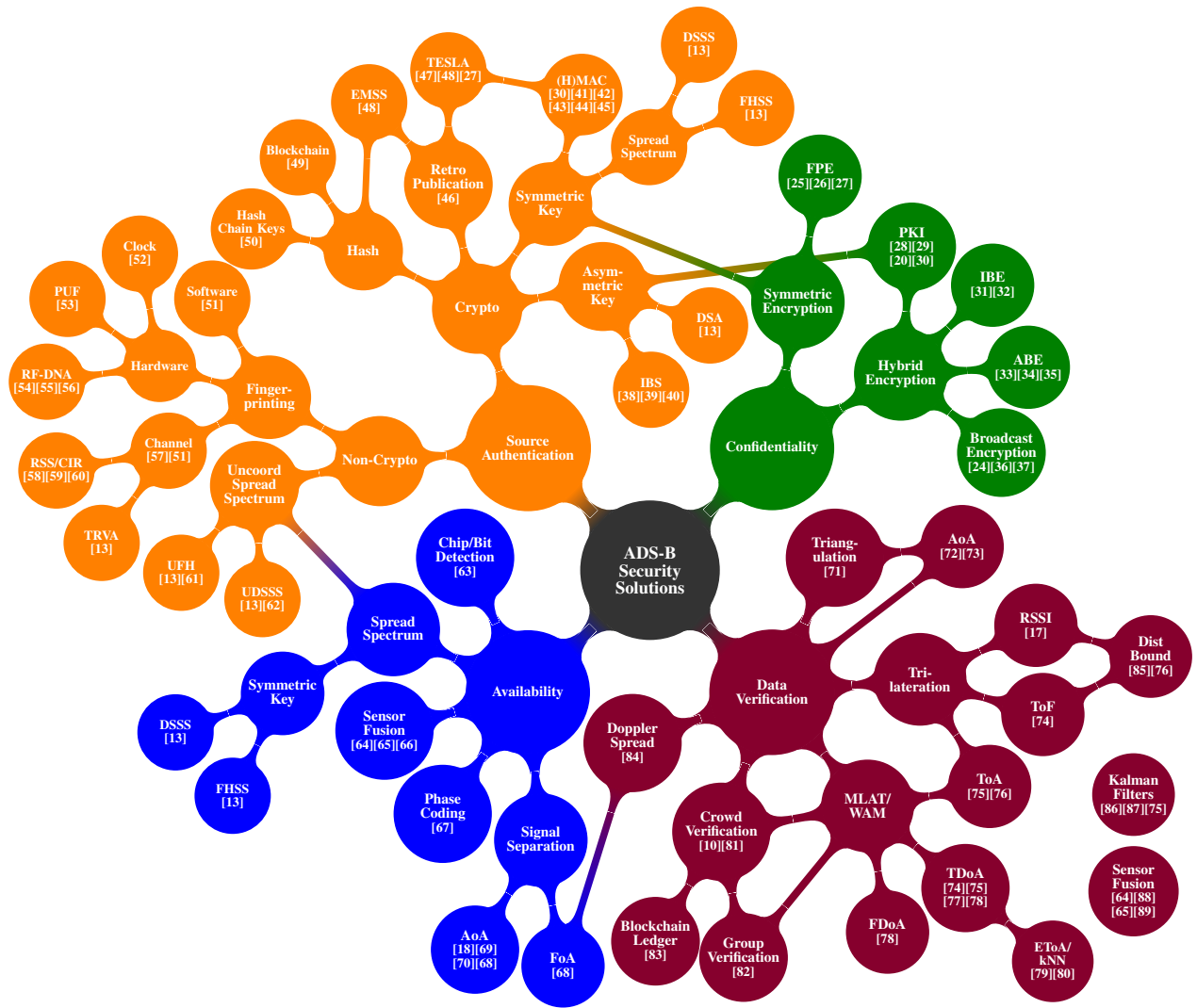
Figure 13. ADS-B Security Solutions

III. Confidentiality Protocol

3.1 Overview

Chapter II shows a significant security gap in the current iteration of ADS-B. The lack of confidentiality in particular drives the research question:

How can Mode S-ES be extended to allow confidential operations without requiring a change to existing standards while retaining interoperability with existing systems?

Answering this question requires an applied research process. This chapter will use a formal systems engineering model to answer the research question. The intent of this process is to be efficient, thorough, and precise, not necessarily to be verbose. To that end, a lightweight adaptation of a defense research and development systems engineering process [90] will form the structure through which the question can be addressed and results demonstrated.

3.2 Process

While the process here is driven by a research question, it is still useful to define various *stakeholders*. Various stakeholders in ADS-B are discussed below. Many of these are directly tied to the motivation addressed in Chapter I.

Following the discussion of stakeholders is one of *scope*. Scoping is important for research in general and applied research in particular.

Process inputs include research questions and objectives, scope, and stakeholders. Requirements and constraints are derived from these inputs.

Requirements analysis uses process inputs to derive various categories of requirements. These are divided into:

Functional Requirements: the necessary tasks, actions, or activities that must be accomplished.

Performance Requirements: The extent to which a mission or function must be executed; generally measured in terms of quantity, quality, coverage, timeliness, or readiness. These will often quantify the qualities expressed in functional requirements.

Design Requirements: The 'build to' and 'code to' requirements expressed in technical data packages and technical manuals. This research does not go so far as to derive design requirements for newly innovated subsystems but will mention those currently in place.

Constraints: constraints are specific limitations placed upon a design by process inputs and should be considered simultaneously with requirements.

```
┌─────────────┐
│   Process   │
│   Inputs    │
└─────────────┘
       │
       ▼
┌─────────────┐
│ Requirements│
│  Analysis   │
└─────────────┘
       │
       ▼
┌─────────────┐
│  Functional │
│  Allocation │
└─────────────┘
       │
       ▼
┌─────────────┐
│   Design    │
│  Synthesis  │
└─────────────┘
       │
       ▼
┌─────────────┐
│   Process   │
│   Outputs   │
└─────────────┘
```
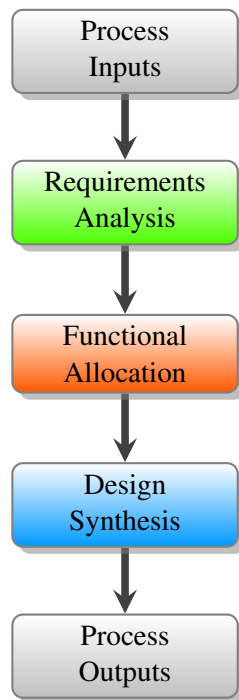
Figure 14. System Development Process

Functional analysis and allocation is the process by which requirements are transformed into a coherent description of functions which are synthesized into a final design. Based on the scope of this research, the functional allocation process is fairly lightweight,

23

essentially bridging the gap between requirements analysis and design synthesis.

Design synthesis is the process by which as design is developed based on the products of functional analysis and allocation. Outputs from design synthesis are expressed via DoD Architecture Framework (DoDAF) Operational Viewpoints, psuedocode, and other visual system depictions.

3.3 Stakeholders

The stakeholders for ADS-B are numerous and multiply greatly when considering national boundaries. When considered here, entities that belong to a specific state are genericized to maintain global relevance. A key consideration is each entities' policy and technical relationship with ADS-B and information security.

3.3.1 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 physical separation from other users while operating on the ground and in the air.

3.3.1.1 Air Carriers.

Air carriers include corporations who provide scheduled transportation services for the public. Also referred to as airlines, air carriers have a public flight schedule and publish real time status data for the majority of their flights. Given the inherently public nature of their operations and their ability to internally protect their passengers' privacy, they do not have a significant need for privacy or confidentiality when it comes to surveillance data.

3.3.1.2 Charter Operators.

Charter operators execute on-demand flights for a paying customer or cargo agent. These operators do not necessarily have scheduled service, though they may execute the same route at similar times repetitively. Charter operators' requirement for privacy most often rests with their customer. If their customer desires confidentiality, the operator may in turn require confidentiality of associated surveillance data.

3.3.1.3 Corporate Flight Departments.

Corporate flight departments, as defined here, includes indigenous flight operations within a business or corporation as well as charter operators who exclusively or majoritively operate on the behalf of the same. Corporate operators have a significant requirement for privacy with surveillance data; often their ability to innovate and compete depends upon the confidentiality of their movements and actions [91].

3.3.1.4 Private Operators.

Private operators are individuals or families who own or rent aircraft for transportation or leisure. The operations conducted are diverse, ranging from regional transportation to aerobatics, soaring, training, etc. While many private operators do not have a *requirement* for privacy, they may *desire* privacy for many reasons. As the ongoing global debate over privacy rights continues, it is important that technical solutions be in place to support any policy outcomes.

3.3.1.5 Military & Defense.

An obvious use case for confidential communications, military and defense related operations have significant requirements for confidentiality. Operations security seeks to deny adversaries information regarding current operations, pattern of operations, plans, tactics,

25

and movements. While military command and control has access to robust, symmetrically encrypted surveillance, the ability for aircraft to securely participate in civil surveillance schemes is almost non-existent.

3.3.1.6 Intelligence & Diplomatic Agencies.

Like military operations, intelligence and diplomatic operations have serious requirements for confidentiality. Unlike the military, there likely does not exist a persistent command and control network that can share data with civil air traffic control. Current practices might include the faking of data or quite literally "flying under the radar," but a technical confidentiality solution could increase safety while meeting mission requirements.

3.3.2 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.

3.3.2.1 Air Traffic Control (ATC).

ATC is an organization tasked by a government to provide separation of air traffic inside a nation's airspace. This is conducted in accordance with regulations and standard procedures for that nation, many of which may be standardized with ICAO and other nations. ATC currently consists of a surveillance network, voice and data communications, and controllers. Controllers use surveillance data to monitor airspace and communication systems to instruct airborne aircraft to modify their course of action as required. ATC's concern with the implementation of a security protocol is likely limited to the cost and training required to operate.

3.3.2.2 Surveillance Network Operator.

ATC is an organization tasked to design, build, deploy, and maintain the hardware and software associated with the ground segment of a network. Hardware may include radars, ADS-B transceivers, remote communications outlets, dedicated communications networks, and controller workstations. Software includes everything required for the hardware to interface with controllers, users, and supervisors. The network operator will bear the burden of implementing updates to hardware and software if a security protocol is implemented.

3.3.2.3 Equipment Manufacturers.

Equipment manufacturers build the hardware and software for both the ground segment and airborne transponders. They must implement the technical standards imposed by regulatory bodies and validate compliance via testing. This process for safety-critical equipment is generally rigorous and expensive. Equipment manufacturers would probably receive beneficial contracts for additional hardware and software if a security protocol is developed.

3.3.3 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.

3.3.3.1 Civil Aviation Authority (CAA).

Likely the main aviation regulating body of a given state, the CAA is chartered to ensure aviation safety. Depending on the nation, the focus on safety is often separated from security by functional separation of security to another governmental body [10]. CAAs will regulate operations, certify operators, do quality assurance on maintenance, provide

or charter ATC organizations, provide aeronautical data, and the like. For most proposed authentication schemes, the cost and impact to safety outweigh the benefits which can be partially accomplished via current verification methods. Likewise, because most CAAs do not have a legal requirement to protect privacy or confidentiality, any solution in that realm must be cost-effective and interoperable to have a chance at political success.

3.3.3.2 Lawmaking Body.

Lawmakers' status is dependent upon the constitution of the state in question. These may be executives, ministers, legislatures, judiciaries, etc. Generally these lawmaking bodies will give broad directives to a CAA to allow further regulatory action. These will be the entities that drive the policy of privacy for given nation. Often they also are the approval authority for any funding to required to make system updates.

3.3.3.3 International Civil Aviation Organization (ICAO).

ICAO is an United Nations agency which exists to foster global consensus on policies to support a "safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector [92]." Their Standards and Recommended Practices (SARPs) are partially or fully adopted by most national CAAs to enhance interoperability.

3.3.3.4 Radio Technical Commission for Aeronautics (RTCA) & European Organisation for Civil Aviation Equipment (EUROCAE).

RTCA and EUROCAE are non-governmental standards bodies which create, modify, and ratify technical standards for avionics and associated electronic equipment. Most CAAs have regulations that require compliance with these technical standards. RTCA DO-260 is the document which provides the standards for Mode S-ES.

3.4 Scope

Scoping is critical in research. In this research, there are two layers of scoping. The first is the scope of the research questions and objectives. This is a scoping that takes place *as part of* the development process and is the result of the research question, previous work, and stakeholders. As discussed thoroughly in Chapter II, the decomposition of security principles and analysis of previous work combine with stakeholder desires to scope the research question and objectives. This scoping results in a research question and requirements which focus on privacy and confidentiality, allowing for, but not directly addressing authentication or verification security solutions.

The second layer of scoping in this research is *external to*, and designed to limit, the process itself. This protocol development process is modeled after DoD systems engineering processes. Not all of the process details are useful for this research: most management and policy factors are not addressed. This allows a narrow focus on technical solutions to the ADS-B confidentiality problem.

3.5 Process Inputs

The inputs to the development process include:

- Research Question: How can Mode S-ES be extended to allow confidential operations without requiring a change to existing standards while retaining interoperability with existing systems?

- Previous Work: Security can be decomposed into confidentiality and integrity, each with a separate technical solution.

- Stakeholder Priorities: Various stakeholders have competing priorities, but the "customer" stakeholders prioritize confidentiality and interoperability.

29

3.6 Requirements Analysis

Requirements must be achievable, verifiable, unambiguous, and consistent. They ought also to be abstracted to the appropriate level of system hierarchy. This analysis retains a sufficiently high level of abstraction to remain succinct while giving enough detail that a technical solution to the research question is attainable. Requirements pertaining to baseline ADS-B are referenced, but not restated. The following requirements are derived from the process inputs:

3.6.0.1 Functional Requirements.

FR-1: The confidential ADS-B system must render a participating node's identification anonymous to third parties while remaining unambiguous to authorized receivers.

FR-2: The system must selectively obfuscate data fields within the 'ME field' (payload) of a DF-17 ADS-B message, rendering them unreadable to third parties yet readable to authorized receivers.

FR-3: The system must be able to switch between unencrypted and encrypted modes manually and based on performance criteria.

FR-4: When not in an encryption mode, the system must behave in accordance with RTCA DO-181E and DO-260B, i.e. currently ratified standards for Mode S and Mode S-ES, respectively.

3.6.0.2 Performance Requirements.

PR-1: The confidential ADS-B system must have ≤ 0.1 probability of identification collisions between two separate airborne aircraft and the event of a collision must be mitigated. Assume 20,000 aircraft airborne at any given time.

PR-2: The confidential ADS-B system implementation must be capable of deployment in transponders fielded post 2010 and maintain a transmit rate of at least 6.2 messages per second in accordance with DO-260.

PR-3: If encryption is used to obfuscate transmitted information, it must resist a brute-force attack using current, commercially available compute capability for 25 years.

PR-4: Two obfuscation modes must be available: one which anonymizes the ICAO address and obfuscates the callsign, and a second which also obfuscates position.

PR-5: While set in a 'resolution advisory (RA) mode, the system must cease obfuscating location and altitude information when within 3 nautical mile (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.

3.6.0.3 Design Requirements.

DR-1: The confidential ADS-B system must adhere to the design requirements and implementation specified in RTCA DO-181E and DO-260B in every respect other than the modules added to enable the above functions.

DR-2: Regardless of added modules, all RF characteristics of the system must adhere to RTCA DO-181E and DO-260B.

DR-3: Any hardware or software cryptographic modules must be designed and coded in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) for secure development and deployment.

DR-4: Secure key distribution is not feasible to the general public and will not be part of any encryption scheme used.

3.6.0.4   Constraints.

CR-1: Interoperability and Backwards Compatibility:

- The system will allow unmodified transponders and traffic collision avoidance systems (TCASs) which are currently approved for use to continue operating without further updates.

- The system must not require a modification to the processing and display of non-participating tracks to the ground segment.

- While it is allowable for provisions to be *added* to technical standards, the current provisions must not be deleted or modified.

CR-2: Return Data Channel and Broadcast Architecture

- The constraints in CR-1 imply that the system, being a broadcast protocol, will not have access to a return communications channel, since one does not and cannot exist within Mode S-ES 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.

3.7   Functional Analysis & Allocation

Allocating performance requirements, design requirements, and constraints to functions is the next step in the development process. This is best visualized via Table 2. A brief discussion on the impact of the allocated requirements upon the functions is warranted.

Table 2. Functional Allocation

Function		Perf Reqts / Design Reqts / Constraints	
FR-1	ID Anonymization	CR-1	Interoperable
		CR-2	Remain broadcast, no contract
		DR-2	No change to phy layer
		PR-1	P(Collision) $\leq$ 0.1
		PR-2	$\geq$ 6.2 messages/second throughput
FR-2	Data Obfuscation	CR-1	Interoperable
		CR-2	Remain broadcast, no contract
		DR-2	No change to phy layer
		DR-3	NIST recommended
		DR-4	No key distribution
		PR-2	$\geq$ 6.2 messages/second throughput
		PR-3	Brute-force safe $\geq$25 years
FR-3	Mode Selection	FR-3	Manually selectable between all three
		PR-4	Select Clear, No ID, and No ID or Pos
		PR-5	RA & $\leq$2 NM & $\leq$2000 ft, Pos Clear
FR-4	Baseline Mode S-ES	CR-1	Interoperable
		DR-1	IAW DO-181 and DO-260

3.7.1   Identification Anonymization.

Each aircraft participating in ADS-B has a globally unique 24-bit ICAO address that is used in every Mode S packet transmitted. These addresses are assigned to national governments in blocks by ICAO. In turn, most governments abide by the provision stipulated by ICAO that an address be permanently assigned to an airframe. Some exceptions are made for military aircraft which have hardware or software programable addresses that are taken from a block assigned to a specific military service or unit by their government [93]. Each nation keeps a database matching addresses to registration, which often includes personal or corporation names and contact information. This database is generally made available to the public.

To anonymize this address while keeping it unique requires random selection of a session address from a uniform distribution. To ensure this selection does not collide with

existing addresses, a block of addresses must be set aside for use within this anonymization scheme. While the choice of block is a policy decision, [94] states that "aircraft addresses starting with bit combinations 1011, 1101 and 1111 have been reserved for future use." A randomly selected ephemeral address is henceforth described as a *session unique ICAO address (SUIA)*.

CR-1: Interoperability is maintained because valid 24-bit addresses are used.

CR-2: The lack of an acknowledgement channel may impact the ability of the system to avoid collisions among SUIAs. See PR-1 below.

DR-2: The address change does not impact compliance with physical layer specifications.

PR-1: Assume a growth to 20,000 aircraft airborne globally. Using the block 1111 11 allows an 18-bit SUIA. Therefore $P(collision) = \frac{20000}{2^{18}} = \frac{20000}{2662144} = 0.0763 \leq 0.1$. This worst case assumes every aircraft is using the security features and that there is no isolation between regions.

PR-2: Once a SUIA is generated, using it will likely incur no additional throughput limitations over an assigned address (depending on transponder implementation).

3.7.2 Data Obfuscation.

Robust encryption provides a secure way to obfuscate data. The requirements and constraints severely restrict which ciphers and cryptosystems are available for implementation. A cryptographic solution:

CR-1: Requires FPE of some type.

CR-2: Requires key distribution or key generation on the broadcasting platform.

DR-3: Requires the use of a NIST recommended cipher.

DR-4: Requires the use of a public-key or hybrid encryption system.

PR-2: Requires the use of symmetric encryption.

FF1 is the designation for the only NIST recommended FPE cipher. A draft version of FF1 was previously validated for use in ADS-B in [21], [22], and [95]. Unfortunately, using FF1 on its own requires key distribution. To meet all requirements, FF1 must be used within a hybrid cryptosystem.

Generally, hybrid cryptosystems use public key technology to agree upon a shared secret which can be used as a symmetric key, removing the requirement for symmetric key distribution. Unfortunately, hybrid cryptosystems often rely on certificate based systems to distribute public/private key pairs, thereby requiring significant two-way connectivity. CR-2 compliance requires the innovation of a modified hybrid cryptosystem. This is enabled by the CIA decomposition discussed in Chapter II. It is possible to encrypt a message with a public key and have it decrypted with a private key without requiring a signature or key agreement algorithm. This allows the combination of key transport using public key encryption with FPE, discussed further below.
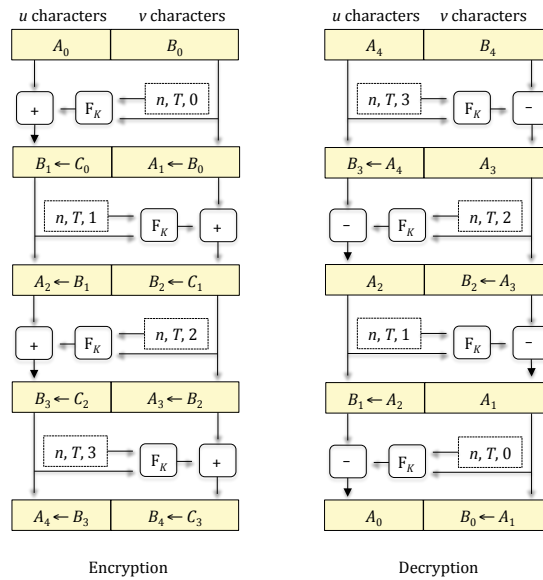
Figure 15. FF1 Feistel Structure

35

3.7.3 Mode Selection.

Mode selection, discussed further in design synthesis, is a simple exercise in loading message registers with different data based on the selected mode. Criteria for automatic mode selection (PR-5) can be implemented along with a user interface for manual mode selection (FR-3).

The multitude of flight management systems (FMSs) and transponders in use across the global aircraft fleet would require significant discussion of user interfaces and their design. Most deployed devices have the capability to change their user interface via firmware or software updates. An analysis of user experience and human factors is beyond the scope of this research.

3.7.4 Baseline Mode S.

The discussion on implementing currently ratified Mode S standard is not directly related to this research. Additional interoperability considerations arise in design synthesis; further discussion on baseline Mode S can be found in [8] and [9].

3.8 Synthesis & Results

Design synthesis is the process by which concepts or designs are developed based on the output of functional analysis and allocation. Allocating requirements to functions made some key subsystem design decisions clear in that phase. Here, the SUIA and cryptographic designs are synthesized with Mode S-ES into a confidentiality protocol summarized by Figure 16. This concept shows the existing Mode S-ES components and operations in gray. The colored portions are discussed in this section.
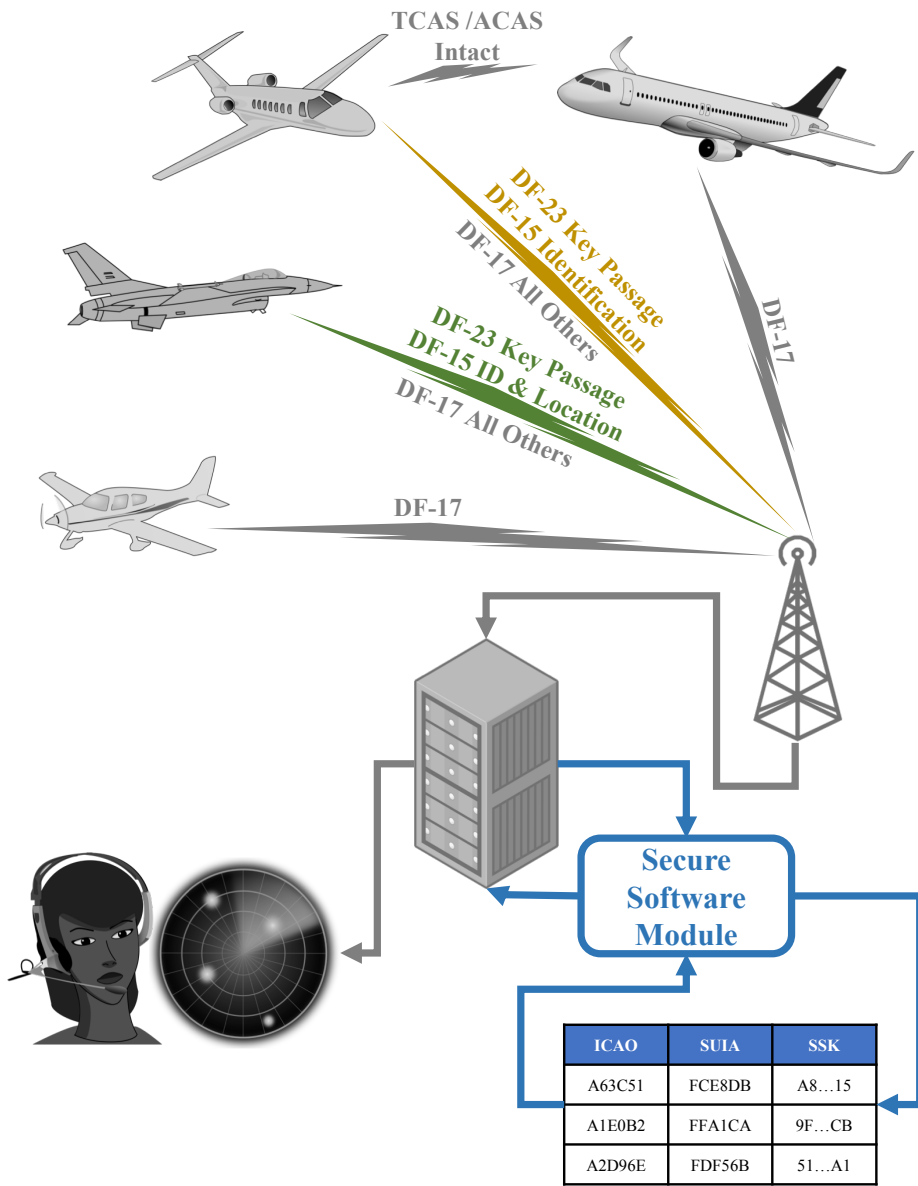
Figure 16. Operational Concept (OV-1)

3.8.1   ICAO Address Anonymization.

The session unique ICAO address (SUIA) concept discussed previously enables anonymous Mode S operation.

3.8.2   Data Encryption.

This proposal makes use of FF1 as the symmetric encryption mode. The symmetric key used to accomplish encryption is generated on-board the participating aircraft along with an SUIA and is called a *session symmetric key (SSK)*.

3.8.3   SUIA & SSK Handoff.

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

Alice (Aircraft)   **Bob (ATC)**

create key pair (k_{pub}, k_{pr})

$\xleftarrow{\quad k_{pub} \quad}$

choose random k_{sym}
$y = e_{k_{pub}}(k_{sym})$

$\xrightarrow{\quad y \quad}$

$k_{sym} = d_{k_{pr}}(y)$

message m
$z = FPE_{k_{sym}}(m)$

$\xrightarrow{\quad z \quad}$

$m = FPE^{-1}_{k_{sym}}(z)$
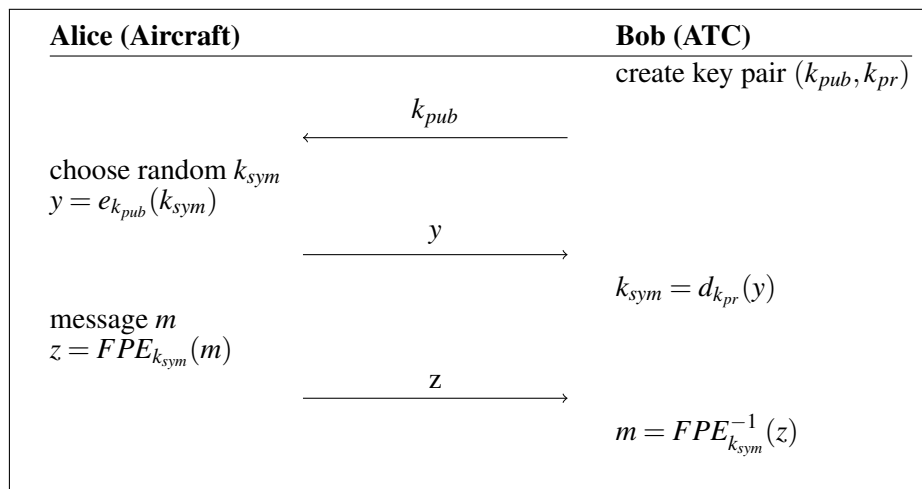
Figure 17. Broadcast Hybrid Encryption

As introduced above, a lightweight solution to transporting cryptographic keys is *unidirectional public key encryption* (Figure 17). The broadcast, stateless nature of Mode S-ES 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 SSK on board and encrypts them using the aforementioned public key. This data is transmitted to ATC, who now possesses both the SUIA and SSK. With these, they are able to correlate 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, e.g., in the US, the FAA and North American Aerospace Defense Command (NORAD) can share SUIAs and SSKs within the ATC and air defense networks without revealing them to untrusted third parties or users. It also assumes that an entropy source sufficient to the level of security required exists or can exist in on-board avionics systems.

While a specific asymmetric encryption algorithm is not specified, current elliptic curve based schemes have minimum block sizes of 512 bits. These 512 bits can be divided into 12 Mode S-ES packets.

3.8.4 Key Handoff Transmission Methods.

Several potential methods of transmission exist, each with advantages and disadvantages:

- **Mode S-ES Packets** This method is assumed for the remainder of Chapter III and is the impetus for the research in Chapter IV. This is advantageous because all required infrastructure is currently in place. SUIAs and SSKs can be updated in real-time, anytime during a session. The disadvantage is the increased spectrum use driven by the PER research discussed in Chapter IV.

- **IP During Mission Planning** This method is less flexible because keys are generated and handed off during mission planning over an internet based system. There is currently no infrastructure in place to support this, however development would be

39

relatively simple and low-cost. Once a preset list of keys is exhausted airborne, there is no ability to generate and pass new keys.

- **IP Real Time** This overcomes the finite set of keys issue, however not all aircraft are equipped with airborne internet access. It also requires the transponder to interact with the internet source, thereby increasing the cost and complexity of equipping aircraft with this capability.

- **Phase Overlay** DO-260C, the draft revision to Mode S-ES standards, incorporates a capability to encode up to three bits using phase modulation on top of each amplitude modulated bit in a Mode S-ES packet. It also includes forward error correction (FEC), dramatically reducing the overhead required to successfully accomplish a key handoff via broadcast on 1090 MHz. This will be discussed further in Chapter V.

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.

3.8.5 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 $120\mu s$ data unit consisting of a $8\mu s$ preamble and 56 or 112 bits of data

Handoff: a data unit used for key handoff that is divided into 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. 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. All DF-17 packets have the same structure, depicted in Figure 18. The payload is known as the ME field. There are currently 32 ME field content sets [9].

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 18. Added Reply Formats

In this proposed protocol, 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 identification ME field.

3.8.6 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* is added, acting as a filter for incoming Mode S packets. 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, shown in line 19 of Algorithm 1. A packet with an SUIA has its address field replaced with the actual ICAO address, shown in line 17. A packet that is encrypted has its address replaced, DF set to 17 (or as required), and ME field decrypted, shown in line 12. This is then forwarded as a normal DF-17 to current ATC software. If a DF-23 is received (line 7), the look up table is populated.

Algorithm 1 Secure Software Module

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

3.8.7 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.

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. 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 (Figure 16).

3.8.8 Overall Synthesis.

All of these considerations are brought together in Figure 19. It shows the roles of the user (who is in the aircraft), secure software module (on the ground), and air traffic controller. The information flow for both the key handoff and subsequent secure or anonymous operations are shown in relation to one another. An example of lookup table referenced is depicted in Figure 16.

Key Generation
CAA or ATC

Generate key pair (k_{pub}, k_{pr})
Publish k_{pub} with aeronautical data
Distribute k_{pr} to trusted agencies

Key Loading
User or Maintenance

Load k_{pub} into FMS or Transponder

User Init Session
User

UI input to execute key passage
No success/fail acknowledgement
Begin using encrypted mode

Transmit Mode S-ES
User

DF-17 w/ ICAO = Cleartext
DF-15 w/ SUIA = Encrypted
DF-17 w/ SUIA = ID Obfuscated

Secure Software Module

Current ATC Software

User

Controller

ATC Init Session
ATC Secure Software Module

Receive series of DF-23 packets
Attempt to reconstruct SUIA & SSK

Receive Mode S Message
Current ATC Software

All packets received and
able to reconstruct?

Yes

No

DF-23?

Yes

No

Duplicate SUIA entry?

Yes

No

DF-15?

Yes

No

Decrypt
ATC Secure Software Module

Lookup key using SUIA
Decrypt fields
Change DF to 17

Enter Into Translation Table
ATC Secure Software Module

Ready to receive messages

Any DF with SUIA?

Yes

No

Translate ID
ATC Secure Software Module

Lookup ICAO address using SUIA
Replace SUIA with ICAO address

Controller Notify User
Controller

Current or new phraseology IAW
FAA JO 7110.65 5-2-15/25/26
or equivalent

Notify Controller
Current ATC Software

Use current alerts OR
Use new alert for bad crypto

Process Mode S Message
Current ATC Software

Current ATC software sees DF-17s
(or other Mode S message DFs)

Failed Table Lookup

Figure 19. Operational Flow Diagram (OV-6)

3.8.9 Development & Deployment.

A discussion on the actual details of the development, testing, and deployment of new software or firmware for each of the different integrated avionics systems and transponders is beyond the scope of this research. There are challenges associated with modification: processing power for cryptographic operations, entropy sources, user interface design, etc. A key to this protocol is that those challenges exist only for those systems used by customers desiring confidentiality.

Likewise, an in depth discussion on the same process for ground segment software is not viable here. Ideally, a modification such as the one proposed here is implemented as a software only update.

The process to discuss and ratify additional standards in RTCA documents is potentially lengthy, but necessary to formalize this proposal and iterate to a point of operational feasibility and security. It is important to bring security and cryptographic experts into that process early.

3.9 Conclusion

This research presents a technical solution which would allow an interoperable implementation of cryptographic confidentiality over the Mode S-ES protocol. The use of a hybrid encryption system in which each packet retains its structure yet has a payload encrypted with FPE maintains compatibility with currently deployed systems. A unidirectional key generation and handoff solution removes the need for certificates and key distribution to each individual user. Remaining technical challenges include the on-aircraft generation of cryptographically secure pseudo-random numbers (CSPRN) and the methodology for key handoff transmission. Chapter IV investigates the viability of the specific key handoff transmission method suggested here.

IV. Key Handoff Characterization

4.1 Introduction

The protocol developed in Chapter III utilizes a key handoff in which data flows in a single direction. On the presentation layer, this is by design. Key distribution issues are avoided by using unidirectional key handoff. On the transport and session layers, this is a significant limitation. Mode S-ES is unidirectional: data is broadcast from one node (aircraft) to other nodes (ground stations and other aircraft). Like the user datagram protocol (UDP), there is no handshaking and no guarantee of delivery or ordering. There is no capability for a receiving node to acknowledge receipt of a packet or reply in any way. Adding multi-node stateful sessions and transport to Mode S-ES would require a significant overhaul of the protocol, violating the objectives as discussed in Chapter III.

The efforts discussed in this chapter are focused on answering the first part of the second research question: *What is the open-air Mode S-ES link performance and how does this impact the real-world implementation of the proposed protocol?* Modeling and simulation as well as open-air flight test contributed to this effort.

4.1.1 Error Ratio.

Performance, in this case, refers to the error probabilities experienced by data moved across Mode S-ES. Error probability, p_e, is a common performance metric used to evaluate digital communications. Error probability is approximated by error ratio, an experimentally derived value [96]. Error ratio is defined as $\frac{1-r}{t}$ where r is the quantity successfully received and t is the quantity transmitted over a given time period.

Three error ratios are of interest to this research:

- Bit Error Ratio (BER) $\approx p_{eb}$

- Packet Error Ratio (PER) $\approx p_{ep}$

- Handoff Error Ratio (HER) $\approx p_{eh}$

BER is only of interest insofar as it drives PER and therefore is not directly measured or analyzed here. PER is the normal performance indicator for Mode S-ES's physical and link layers. HER is a measurement unique to the work herein; it measures error as applied to handoffs (sets of 12 packets in this case).

4.1.2 Noise.

Background noise is not a primary contributor to bit errors in Mode S packets. Mode S-ES occupies 2 MHz of bandwidth centered at 1090 MHz. This falls within the 960-1164 MHz band which is internationally reserved for aeronautical use [97] of which 1090 MHz is further set aside for transponder exclusive use. Measured man-made background noise is lower than thermal noise on most frequencies in L-Band (1-2 GHz) [98]. Thermal noise, the primary contributor to the background noise floor at 1090 MHz, is

$$P_{bn} = kBT = 8.28 \cdot 10^{-15} \text{ Watts} \tag{1}$$

where k is Botlzmann's constant, $B = 2$ MHz of bandwidth, and $T = 300$ K $\approx 80°$ F.

4.1.3 Link Budget.

The received power, $P_r = C$ must account for free space path loss:

$$C = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 R^2 L} \tag{2}$$

where G are gains, L is losses, and R is range in meters. Assuming $P_t = 177$, isotropic antennae, and negligible component losses:

$$C = \frac{177\lambda^2}{157.91R^2} \tag{3}$$

Assuming 1090 MHz, then $\lambda = 0.28$ meters.

$$C = \frac{0.085}{R^2} \tag{4}$$

Convert meters to nautical miles.

$$C = \frac{0.000000025}{R_{NM}^2} \tag{5}$$

4.1.4 Signal to Noise Ratio.

The resulting carrier sigal-to-noise ratio (SNR), $\frac{C}{N}$, is shown in Figure 20:

$$\frac{C}{N} = \frac{\frac{0.000000025}{R_{NM}^2}}{8.28 \cdot 10^{-15}} = 3019323.67 \left(\frac{1}{R_{NM}^2} \right) \tag{6}$$

Also shown is SNR per bit, $\frac{E_b}{N_0}$:

$$\frac{E_b}{N_0} = \frac{C}{N} \cdot \frac{B}{f_b} \tag{7}$$

Equation 8 assumes non-coherent detection due to the proliferation of non-coherent Mode S receivers. The resulting theoretical BER [99] is shown in Figure 21.

$$BER \approx \frac{1}{2} e^{-\frac{1}{2} \cdot \frac{E_b}{N_0}} \tag{8}$$

where $f_b = 1$ Mb/s, the bit rate of Mode S-ES. Because $\lim_{snr \to \infty} p_{eb} = 0$, the expected BER and PER approach zero. Noise is *not* a significant contributor to errors in Mode S, largely due to power requirements for transmitters.
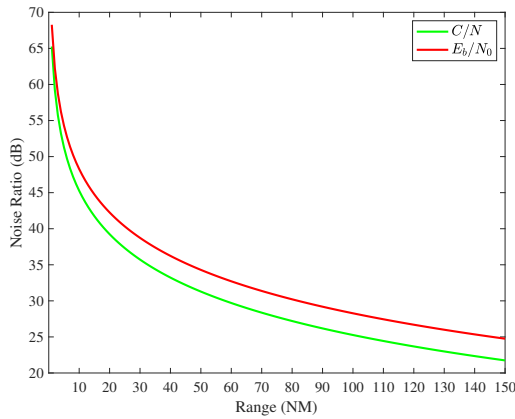

Figure 20. Theoretical SNRs
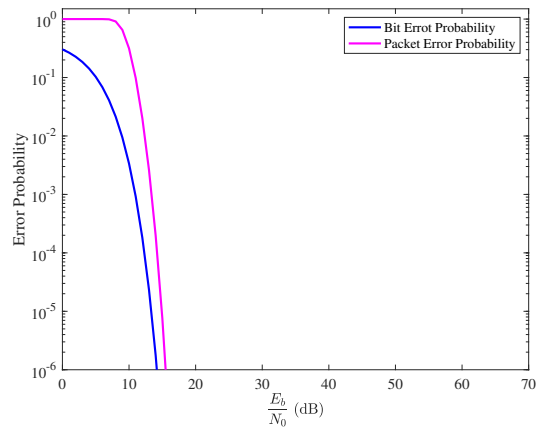
Figure 21. Error vs E_b/N_0

4.1.5 FRUIT.

The lack of a multiple access scheme for Mode S means that all nodes have access to the channel at all times, essentially pseudo-random access. Depending on air traffic density and composition in a given location, this causes severe interference which results in relatively high PERs. This interference, caused by the superposition of multiple authorized
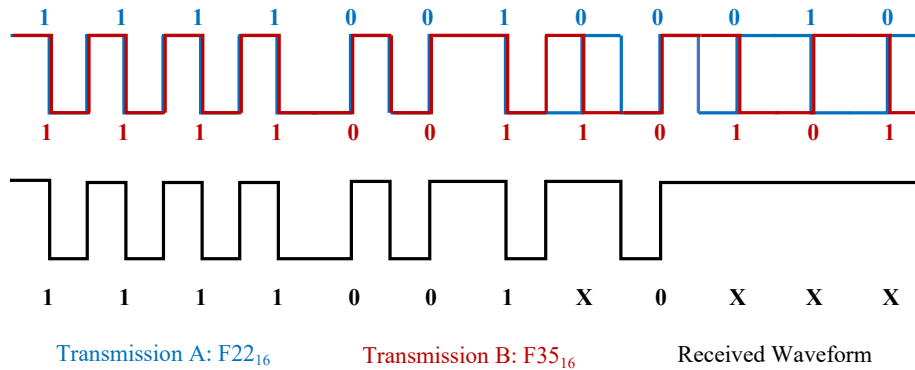

Figure 22. Interference Due to FRUIT

transmissions, is known as *false replies unsynchronized in time (FRUIT)*. Figure 22 shows an example of two superimposed transmissions at a receiver. In this case, the power levels are identical, resulting in ambiguous bit values. In reality, power levels are unlikely be identical; the symbol detector will choose a bit value which is potentially erroneous.

Figure 23 shows FRUIT rates gathered by an instrumented test aircraft flying within 150 NM of the Los Angeles Airport [100]. Figures 24 shows FRUIT rate data from a ground receiver in Lexington, Massachusetts [63]. In these figures, and in this document, the terms "FRUIT" and "replies" are used to refer to Mode S-ES broadcast transmissions as well, even though they are not replying to interrogation. ATCRBS comprises of transponder Modes 1-4 and C. Mode S includes both short and extended squitter transmissions.

Given that background noise is minimal and FRUIT rates are as high as 20,000 transmissions per second at -85 dBm, it is highly likely that *FRUIT is the primary cause of bit errors in Mode S-ES packets*.

51
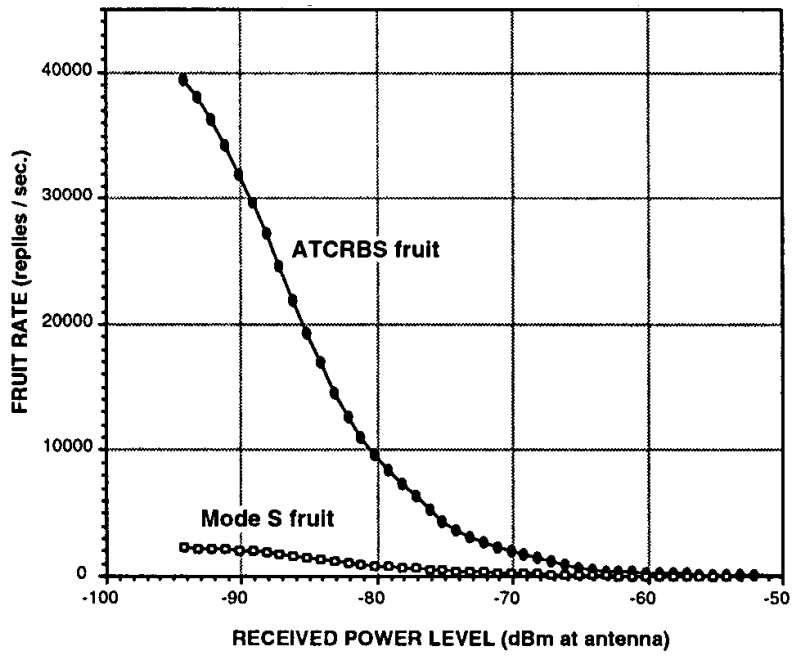
Figure 23. FRUIT over LA Basin
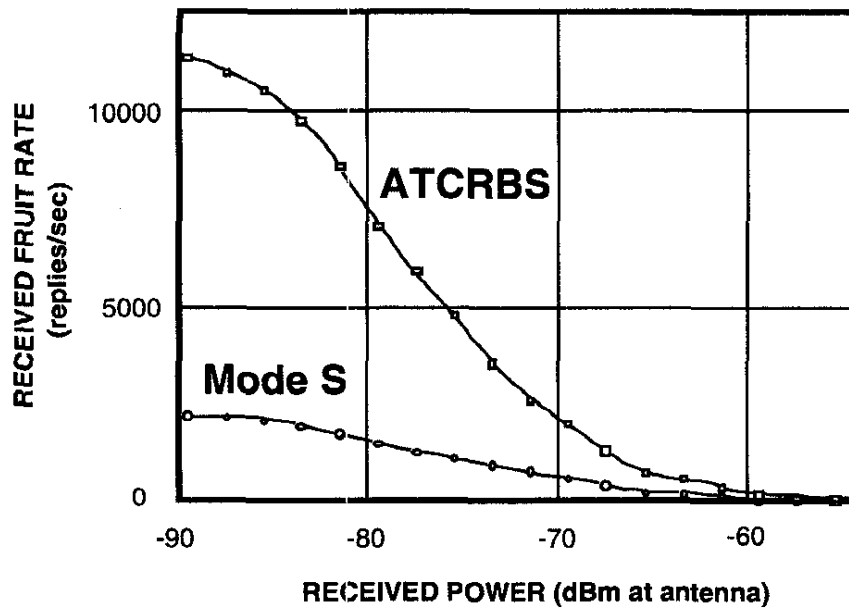
Figure 24. FRUIT at Lexington

52

4.2 Modeling & Simulation Methodology

Mode S-ES PER was first characterized using a simulation. This allowed predictions of real-world performance and offered an opportunity to reduce the technical risk associated with open-air experimentation.

4.2.1 Model.

The simulation utilized a model of the airspace around the Los Angeles (LA) basin with three major components:

- Test Aircraft

- FRUIT Producing Aircraft

- Receiver Site

Figure 25 shows the overarching concept of the model. The green dot in the middle represents a Mode S-ES receiver site. This site is collecting RF on 1090 MHz and decoding packets. The blue line represents the flight path of the test aircraft whose packets are used to determine PER. The red aircraft symbols are other aircraft who are also transmitting on 1090 MHz, producing FRUIT which will impact the decoding of the test aircraft's packets. Note that although Figure 25 is depicted with azimuth consideration, this is for conceptual clarity. The model does not include antennae and therefore neither angle of arrival in azimuth nor elevation are included factors. The traffic distribution shown in Figure 25 is an illustration; the actual model contained an average of 1276 aircraft per run. The test aircraft had the following parameters:

Range from Receiver: 10-150 NM

Altitude: Always Above RF Horizon

Transmitter Power: 200 Watts = 54 dBm

**Transmission Rate:** 20 Packets per Second
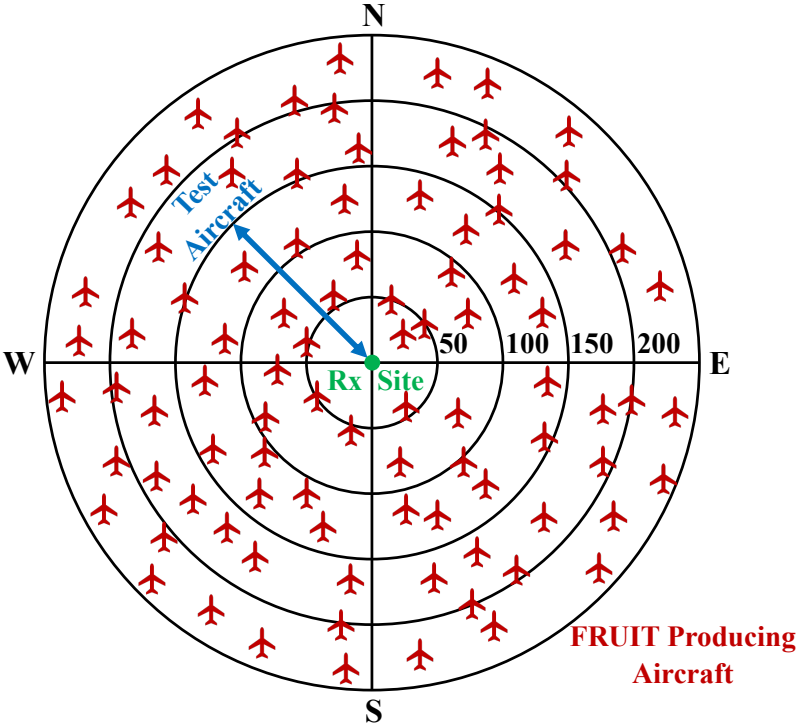
Figure 25. Model Overview

The FRUIT producing aircraft had the following parameters, based on FAA traffic data [100]:

Quantity: $\mathcal{N}(5.25, 1.41)$ per NM to 243 NM from Receiver

Altitude: $\mathcal{N}(10000, 30000)$ feet (Negatives Removed)

Transmitter Class: 20% A0, 40% A1, 10% A2, 30% A3

Transmitter Power: A0: 70-140 W, A1/A2: 125-250 W, A3: 200-400 W

Transmission Spacing: $\mathcal{N}(Evenly, 3000\mu s)$

FRUIT Type: 83% Mode 3 and 17% Mode S

Aircraft whose range to receiver and altitude combination would put them below the RF horizon were removed. Additive white Gaussian noise (AWGN) at a level of -111 dBm was used to create an RF background.

4.2.2 Simulation.

The model of the LA basin air traffic and RF environment was used to simulate reception of test packets and FRUIT. PER was determined based on successful decoding of test packets. An SDR front end outputs a complex, discrete-time, digital representation of the received signal. This simulation utilized the same representation, allowing the use of the exact same receive software used in open-air test. In both cases, the SDR was commanded to sample at six mega-samples per second or six samples per microsecond. Since each encoded bit occupies one microsecond, this means there are six samples per bit. Over 1000 vectors, each representing FRUIT, noise, or the target signal were generated and summed. This summed vector simulated the received waveform from an SDR and was processed by the receive software.

Table 3 shows an example of this process for two bits of data. Two microseconds are shown, each containing six samples. The first four lines represent FRUIT. An average of 1275 FRUIT vectors were combined with a single noise vector and a single target vector. The target "transmitted" a binary '00', Manchester encoded into the target transmission. Due to the energy introduced at the receiver by FRUIT, the output bits are '10', showing a bit error. Note that the values in the table are notional for clarity.

Table 3. Model Example

Sample #	1	2	3	4	5	6	7	8	9	10	11	12
Mode A FRUIT	1.43	1.43	1.43	0	0	0	0	0	0	1.43	1.43	1.43
…	0.525	0.525	0.525	0.525	0.525	0	0	0	0	0	0	0.525
Mode S FRUIT	0.411	0.411	0.411	0	0	0	0	0	0	0.411	0.411	0.411
…	0	0	2.2	2.2	2.2	0	0	0	2.2	2.2	2.2	0
AWGN	0.000	0.001	0.004	0.002	0.006	0.000	0.008	0.003	0.008	0.006	0.007	0.001
Target Bits	0						0					
Target Transmission	0	0	0	1	1	1	0	0	0	1	1	1
Sum at Receiver	2.366	2.367	4.570	3.727	3.731	1.000	0.008	0.003	2.208	5.047	5.048	3.367
Bits at Receiver	1						0					

Other than noise, the simulation did not use a model of the transmit and receive SDRs analog front end or antenna. The simulation results were processed in the same manner as open-air experimental data, detailed below.

4.3   Experimental Methodology

4.3.1   Overview.

Open-air test flights were conducted to gather real-world PER data in support of model generation. The model generated from flight test data can be compared to the modeling and simulation results, however, enough data was collected to determine the model from flight test alone.

Test flights occurred using a T-38C aircraft equipped with the EATS, further detailed in Appendix B. EATS allowed the test aircraft to transmit custom Mode S-ES packets on

Figure 26. T-38C with RASCAL Pod

1090 MHz and was certified by regulators as compliant with physical layer Mode S-ES and ADS-B specifications. These custom packets were received by four receivers located at two ground stations; the positions of which were carefully selected to have a large difference in relative FRUIT environment. The test aircraft flew a specific, repeatable flight profile while remaining within the beam width of all antennas at both ground stations. Comparing packets transmitted to packets received and decoded gives PER information.

4.3.2 Test Aircraft.

The test aircraft was a T-38C with a Reconfigurable Airborne Sensor, Communication, and Laser (RASCAL) pod loaded on the centerline station. RASCAL pod power was controlled via a control panel installed in the front cockpit. Test operations were conducted via the EATS graphical user interface (GUI) installed on a Getac tablet in the rear cockpit, connected to the pod by Ethernet. The EATS GUI allowed system operators to manipulate the content of Mode S-ES packets while ensuring the transmitted waveform was compliant with RTCA, DoD, FAA, and ATCRBS, IFF, Mark XII/XIIA SPO (AIMS) specifications. Aircraft position was accessed by EATS software using a Bluetooth Global Positioning System (GPS) receiver. Additional details of EATS are in Appendix B.

4.3.3   Ground Stations.

Two ground stations were established south of the test airspace (the R-2508 complex). The "high" FRUIT ground station was on top of a tower on Strawberry Peak, exposed to FRUIT from air traffic in the LA basin to the south. The "low" FRUIT ground station 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 are in Appendix D. Each receiver site possessed one yagi (directional) antenna and one dipole (omni) antenna. Transmissions were received by a SDR and processed by Matrix Laboratory (MATLAB)-based receiver software on a laptop computer. Figure 27 shows the low FRUIT ground station.
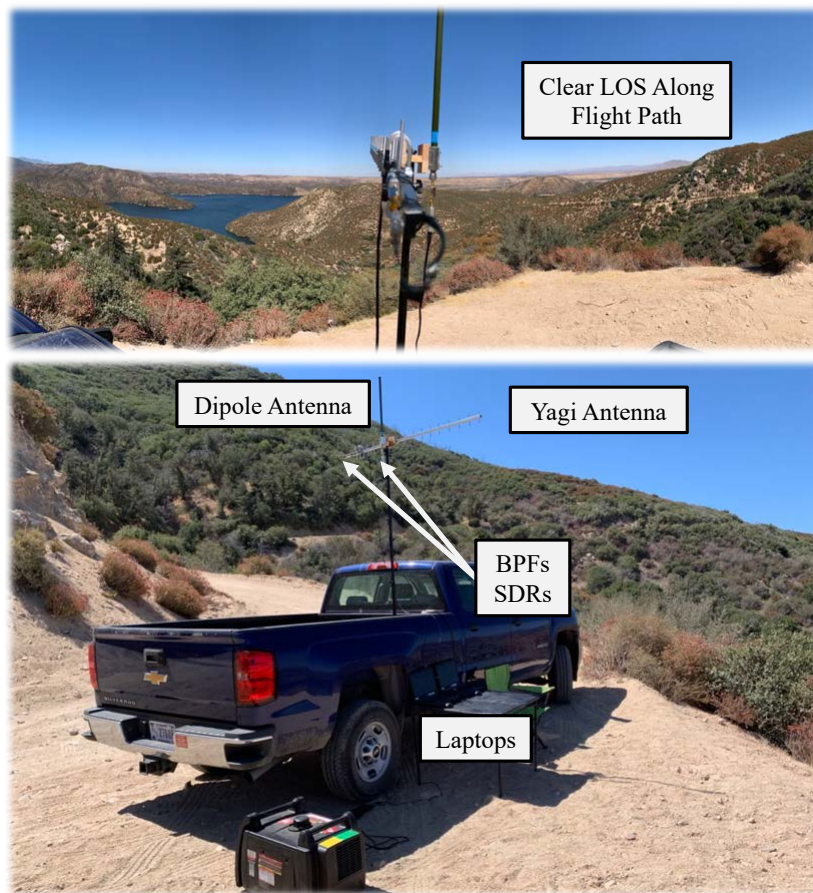

Figure 27. Ground Station

4.3.4 Flight Profile.

A specific flight profile was flown to ensure repeatability between test sorties. The flight profile was designed to:

- Gather data between 10 and 150 NM

- Stay inside the combined beam width of all four antennae

- Use real-world representatives altitudes

- Conserve fuel

Figure 28 shows the resulting profile as a green line, Edwards Air Force Base (AFB) in black, the R-2508 complex airspace in blue, and the ground stations are denoted "L" and "H" for low and high FRUIT, respectively. Figure 29 shows the same profile overlaid on the combined grounds station beam width. Altitudes varied from 12,500 feet within 20 NM of the ground stations and 28,000 feet when 150 NM from the ground stations. True airspeed (KTAS) was maintained between 320 and 430 knots.

4.3.5 Data Collection.

After the test aircraft took off, but prior to beginning transmission, the ground stations began recording data. SDRs fed in-phase and quadrature (I/Q) data to their respective laptops via universal serial bus (USB) 3.0. MATLAB's native SDR capability forwarded the samples into a software-based matched filter for preamble detection. Upon preamble detection and time alignment, another matched filter decoded the Manchester encoded samples, resulting in 56 or 112 bit binary output. Any packet which was not DF-17 (the format transmitted by the test aircraft) was discarded. All DF-17s were further processed to determine the originating ICAO address and compute the cyclic redundancy check (CRC) checksum. If the CRC was successful (i.e. resulted in a zero), then the packet was logged for post-processing, detailed below.
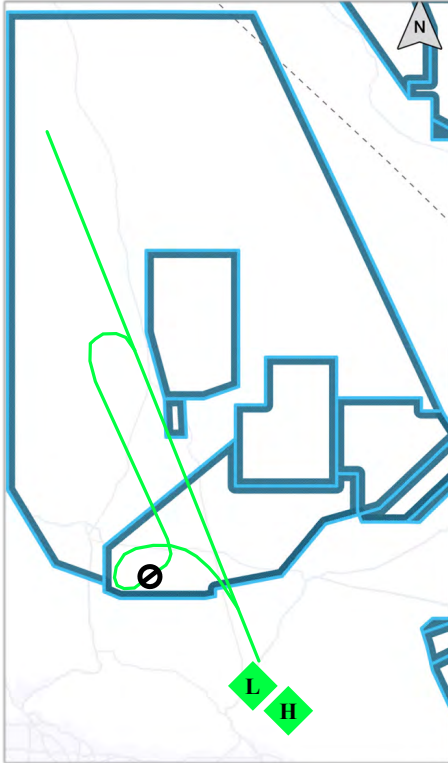
Figure 28. Profile Map - Ground Stations
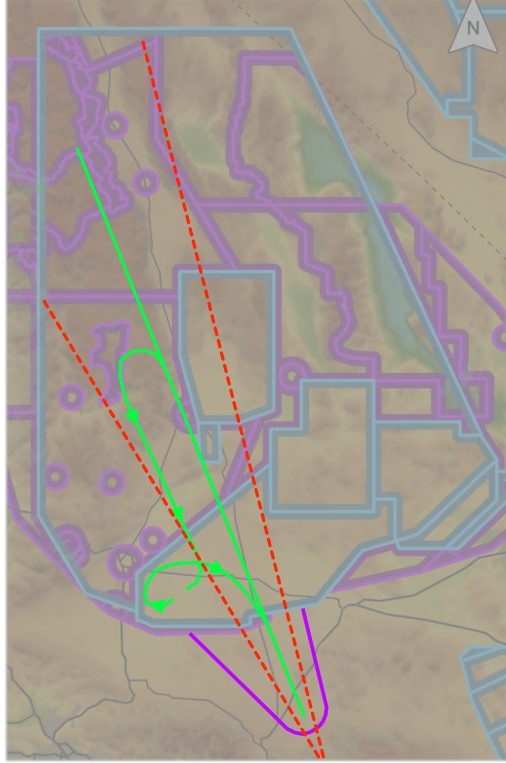
Figure 29. Profile Map - Beamwidth

4.4 Data Analysis

4.4.1 Background.

The goal of the previously discussed data collection was to use simulation or experimental data to create a model which is useful for prediction of Mode S-ES PER performance. Collected raw data is transformed into parameters specific to the transmission of a given packet (independent variables) and decode success or failure (dependent/response variable). In the case of binary error data, it is appropriate to use logistic regression analysis to determine the model of interest. Logistic regression is useful for predictive analysis when there is a relationship between a single binary dependent variable and one or more nominal, ordinal, or interval independent variables [101].

4.4.2 Data Consolidation and Transformation.

Each simulation run or flight produced transmit and receive logs containing all packets transmitted from the aircraft and those received at each of four receivers. In total, each flight generated five separate log files:

- 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 transmit log consisted of geographic position and packet payload. Entries in each receive log contained position, FRUIT environment, antenna type, and packet payload. Figure 30 shows the contents of the log files. Direction of flight was determined post-flight by analyzing whether aircraft range from the receiver sites was increasing or decreasing. During data processing, it was determined that antenna installation error caused data gathered while the aircraft was pointing toward the ground station to be invalid. Final results include only data gathered while the ground station was aft of the test aircraft.

Tx Log			Rx Log			
Position	*Unused*	Payload	Position	FRUIT Enviro	Antenna Type	Payload

Figure 30. Transmit and Receive Log Contents

The payload (ME Field) within each packet contained transmission rate, Julian date (day, hour, minute, second, millisecond), key handoff attempt number, and packet sequence number (Figure 31). The Julian date provided both a coherent time stamp of and an identifier unique to each message. This allowed synchronization of transmit and receive logs without collisions.

DF &CA	ICAO Addr	*Unused*	Day	Hour	Minute	Second	Millis	Attempt	Sequence	CRC

Figure 31. Packet Contents

At the conclusion of simulation runs or flight operations, all log files were consolidated into a single transmit and single receive data file containing all of the collected data. For each entry in the consolidated transmit log file a search was conducted on the receive log file to find entries that matched the coherent time stamp of the transmission. A match indicated successful packet transmission while a failed search indicated a packet error. These were then transformed into a single file containing range, FRUIT environment, direction of flight, antenna type, and binary success/error for each packet transmitted. Figure 32 shows the data transformation flow. Range was calculated using the logged World Geodetic System (WGS-84) coordinates and height above ellipsoid (HAE). Direction of flight was determined by calculating the true heading between position fixes.

Tx Log		
Position	Tx Rate	Payload

+

Rx Log			
Position	FRUIT Enviro	Antenna Type	Payload

⇓

Model Input				
Range	FRUIT Enviro	Antenna Type	Direction	Success
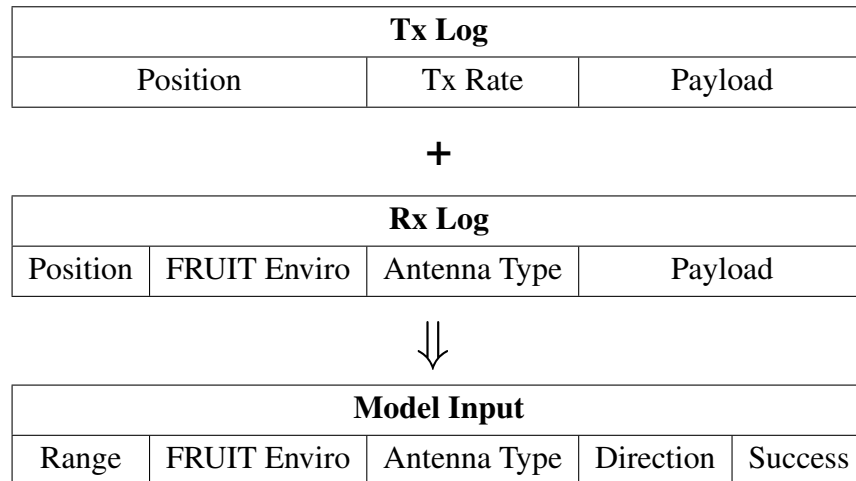
Figure 32. Data Transformation

4.4.3 Model Determination.

Logistic regression analysis was used to determine the model of interest. In the case of this model for PER and HER, the response variable has two categories: *success* or *error* and the following predictors:

- Range (Continuous: 8-150 NM)

- FRUIT Environment (Categorical: High, Low)

- Antenna Pattern (Categorical: Omni, Directional)

- Direction of Flight (Categorical: Inbound, Outbound)

Logistic regression is similar to linear regression in that one can derive it starting with:

$$y = \beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d \tag{9}$$

Unlike a linear regression, the logit function determines an expectation value for a binary response. The natural exponent is used because binary data does not follow a normal distribution and the expectation value must remain greater than zero:

$$y = e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d} \tag{10}$$

A denominator larger than the numerator is used to ensure a value less than or equal to one:

$$y = \frac{e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}}{1 + e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}} \tag{11}$$

Finally, because *success ratio* was directly measured and error ratio was of interest:

$$p_e = y = 1 - \left(\frac{e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}}{1 + e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}} \right) \tag{12}$$

The detailed derivation of of the logit function and it's associated statistics is well documented [101] and beyond the scope of this chapter. Figure 33 shows the premise of logistic regression graphically. The natural exponential function is shaped by the density of the response samples at a given predictor value.
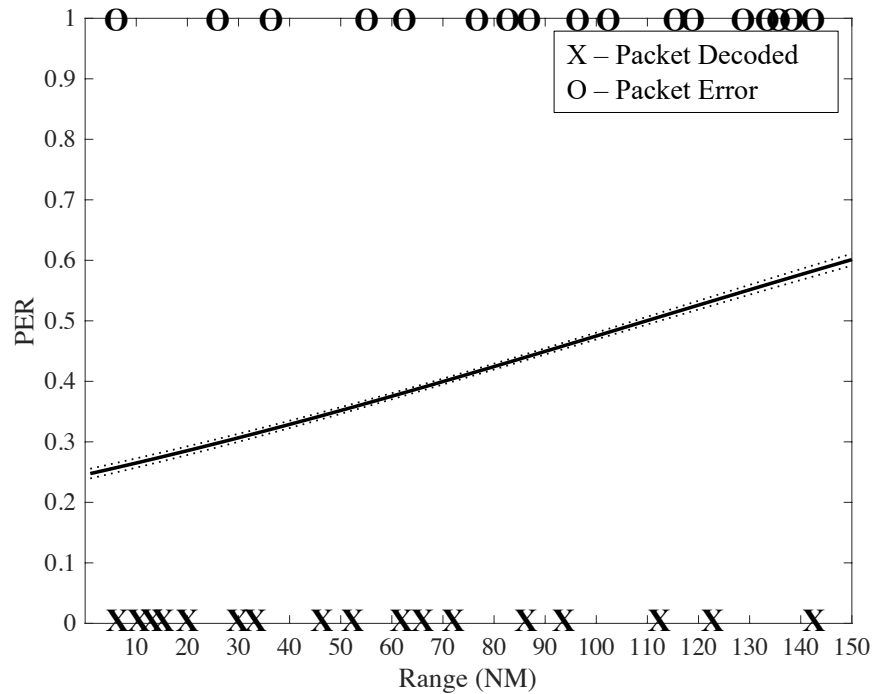

Figure 33. Logistic Regression Concept

HER was calculated as a function of PER, assuming a key handoff containing $n = 12$ Mode S-ES packets:

$$p_{eh} = 1 - (1 - p_{ep})^n \tag{13}$$

$$= 1 - (1 - p_{ep})^{12} \tag{14}$$

The use of analytical HER calculations requires the assumption that individual packets in a handoff are independent from each other. This assumption is made given the long interval between packet transmissions ($\approx$143 milliseconds). If transmission rate were to increase

dramatically, there is potentially a point where independence cannot be assumed.

The open-air flight test results have a minimum statistical confidence level of 0.9954. Details of this derivation are in Appendix A. Because FRUIT was qualitatively determined, this confidence level gives an estimate of the population mean only for test day conditions. The confidence would predict the population mean on a different day if identical FRUIT conditions were present, however there is no quantitative way of comparing test day FRUIT condition to any other day. Further statistical analysis of the logistic regression model is in Appendix A.

4.5 Limitations and Constraints

Several limitations and constraints have an impact on how operationally representative the results are.

4.5.1 Transmit Antenna.

EATS is certified by AIMS as compliant with physical layer specifications. This certification was gained via laboratory demonstrations, not open-air testing. As such, the certification applies to the RF signal as it arrives at the antenna inlet port. The antenna is itself certified, however the combination of the antenna and pod were not tested in an anechoic chamber to determine its combined polar response. This was due to both time and cost constraints associated with the 412th Test Wing. The antenna gain is unknown at each azimuth and therefore there exists a large discrepancy in results between directions of flight. It is assumed that an operational antenna would have equal or better performance to the 'better' azimuths of the test antenna. ***Consequence: Results are a lower bound on operational PER.***

4.5.2 Transmit Power.

Integration of EATS on the T-38C resulted in a measured transmit power of 177 Watts. Simulations were run using 200 Watts, disallowing a direct comparison of results. The T-38C is capable of providing the required power, however time constraints prevented pod integration troubleshooting. Time constraints also prevented the re-running of the simulations at 177 Watts (it takes several days to run on the available hardware). ***Consequence: Open-air results cannot be directly compared to simulation results.***

4.5.3 Airspace Restrictions.

Agreements with ATC and FAA authorities prevented the test aircraft from proceeding closer than eight NM from the ground stations. ***Consequence: Open-air data is not available for the ranges between zero and eight NM.***

4.5.4 FRUIT Rate Measurement.

The capability to quantitatively measure FRUIT exists, however was not available during the time and at the location of the flight test. This results in test data which cannot be standardized to conditions experienced in follow on tests or simulation conditions. The data is useful as a general comparison and to verify that FRUIT is a significant factor. ***Consequence: Data cannot be standardized.***

4.5.5 Receiver Tech Stack.

Due to the integration of TPS objectives, receiver software was required to be written in MATLAB. Limitations with MATLAB multi-threading prevented the implementation of a pipelined receiver flow. This caused the SDR to drop $\approx 42\%$ of samples each second due to buffer loss. This loss was characterized and found to be consistent, allowing a calibration to be applied during post-processing. This factor of 1.7 assumes that the results in the first

0.58 of a second are the same as the missing results in the remaining 0.42 of the second.

Consequence: *Fewer samples contribute to statistical level of confidence, however this did not significantly impact results.* Additionally, the use of relatively inexpensive SDRs at the ground station is not operationally representative. It is assumed that the tech stack employed in operational recievers would have equal or better performance. ***Consequence: Results are a lower bound on operational PER.***

4.6   Results

The results of the simulation and open-air flight test are presented here as plot of error ratio as a function of slant range between the aircraft and ground station. This presentation is unique: traditional error ratio visualizations are plotted as a function of E_b/N_0. Range is a more operationally relevant metric and, given constant transmit power, is proportional to E_b/N_0. Additionally, using range clarifies that the plots are valid only for test day conditions, generalizations cannot be made due to limitations on FRUIT measurement.

Error ratio plots are traditionally plotted with a logarithmic Y-axis. These plots use a linear Y-axis; the significant error ratios of Mode S-ES are far more readable with a linear axis. In all charts, lower on the Y-axis is considered better performance. Performance was expected to decrease (error ratio increase) as range increases.

4.6.1 Simulation Results.

Figure 34 shows the overall PER results of the simulation, without FRUIT rate considered as a factor. Also shown is a 95% confidence interval, a notation removed from all follow-on figures due to the high minimum confidence level and improved readability. Figure 35 shows the results with FRUIT rate as a factor. These plots are derived from the model shown in Equation 15 using the coefficients shown in Table 4.

$$P_{ep} = 1 - \left[1 - \frac{e^{\beta_{intx}+\beta_r r+\beta_f f}}{1 + e^{\beta_{intx}+\beta_r r}} \right] \tag{15}$$

Table 4. Sim Model Coefficients

	Range	Range FRUIT
β_{intx}	-1.122029515630627	-3.723220760070858
β_r	0.010216479825975	0.012929782362101
β_f	-	0.767630655698848
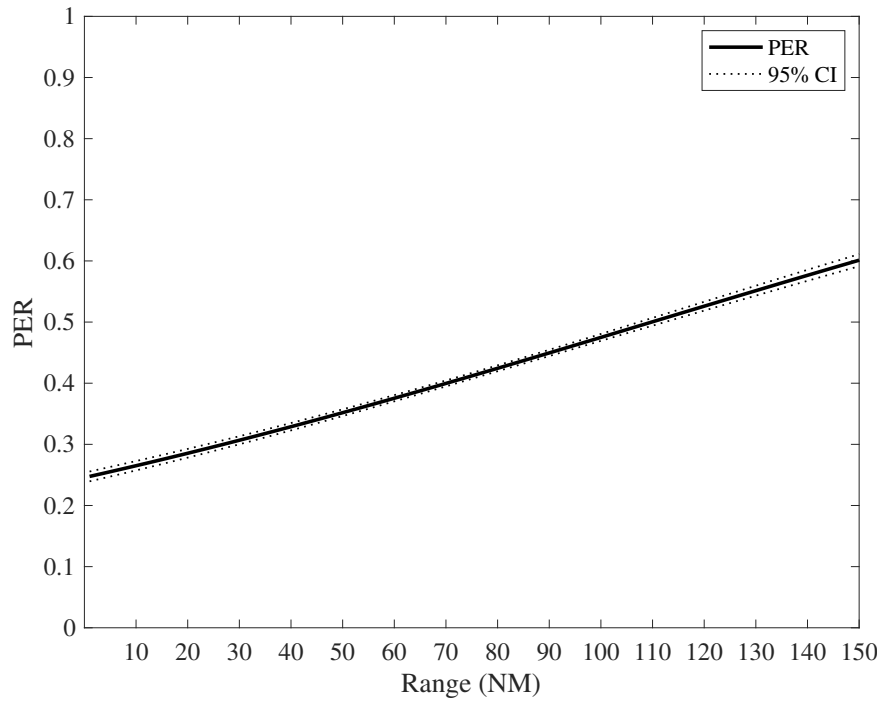
Figure 34. Simulation - Combined Results
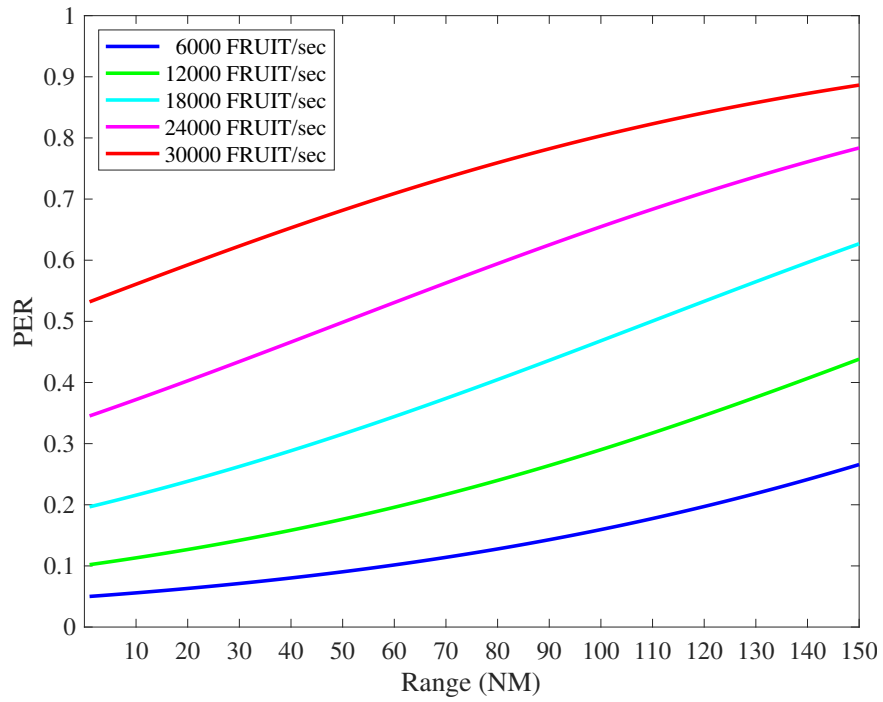
Figure 35. Simulation - FRUIT Rate Results

69

4.6.2 Flight Test Results.

These plots are derived from the model shown in Equation 16 using the coefficients shown in Table 5.

$$P_{ep} = 1 - \left[\left(1 - \frac{e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}}{1 + e^{\beta_{intx} + \beta_r r + \beta_f f + \beta_a a + \beta_d d}} \right) 1.7 \right] \tag{16}$$

Table 5. Flight Test Model Coefficients

	Range	Range FRUIT	Range Antenna	Range Direction	Range FRUIT Antenna	Range FRUIT Direction	Range Antenna Direction	Range FRUIT Antenna Direction
β_{intx}	1.088422157	0.32170932	1.36286078	3.88921704	0.59784947	3.08345370	4.19256129	3.38967477
β_r	0.01756133	0.01697433	0.01757497	0.02088855	0.01698839	0.02037372	0.02091456	0.02040034
β_f	-	0.55304155	-	-	0.55358029	0.59664200	-	0.59751668
β_a	-	-	-0.18140779	-	-0.18305126	-	-0.19863500	-0.20121717
β_d	-	-	-	-1.86187977	-	-1.87875095	-1.86398346	-1.88099134
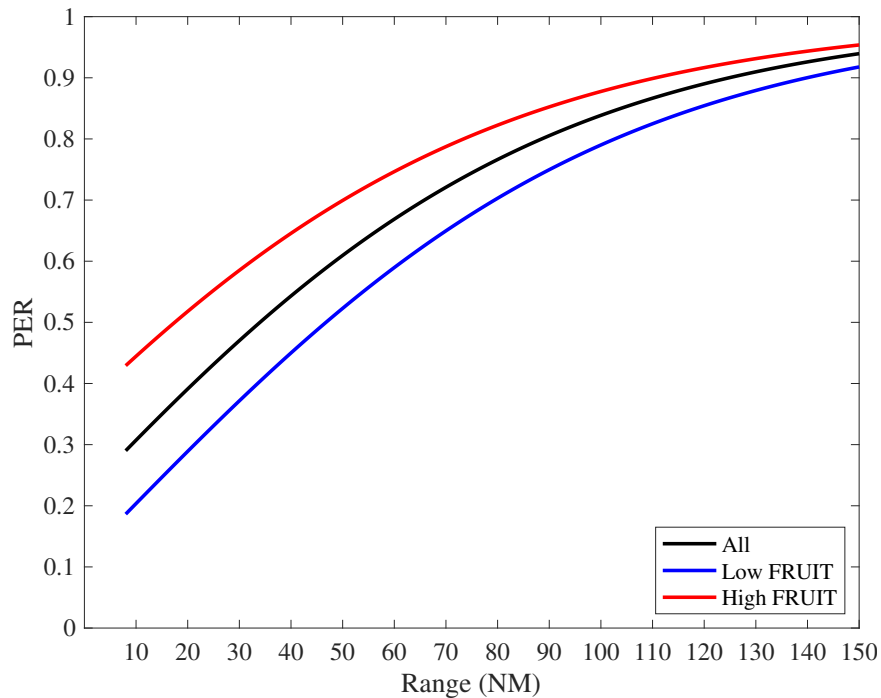
**Figure 36. Flight Test - FRUIT Enviro Results**
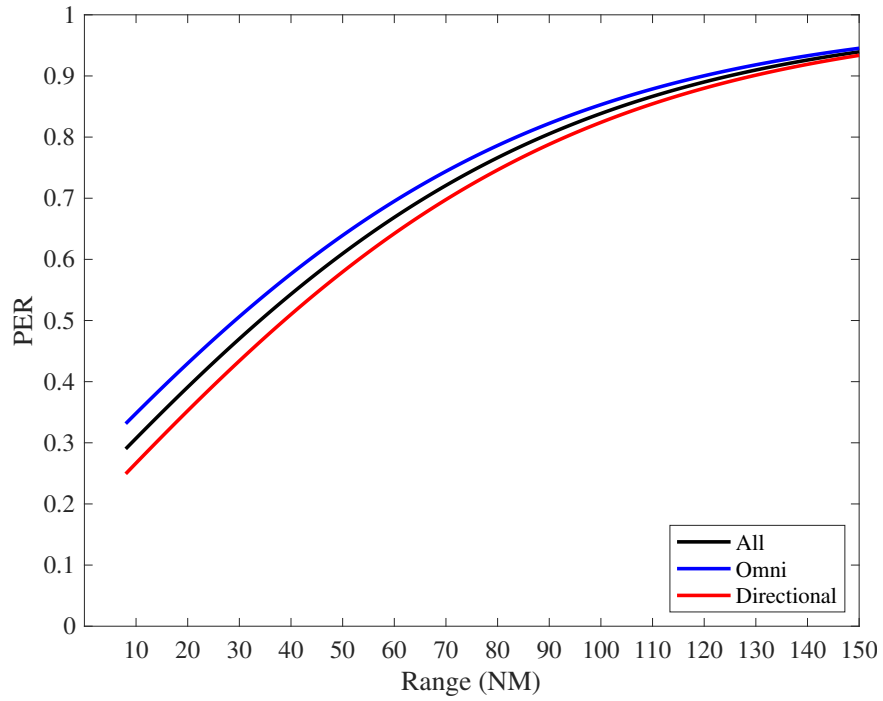
Figure 37. Flight Test - Antenna Results

4.6.3 Derived HER Results.

Flight test was unable to determine an experimental HER due to the receiver limitations described above. Using Equation 13, HER is calculated from the determined PER. This is shown in Figure 39.

71
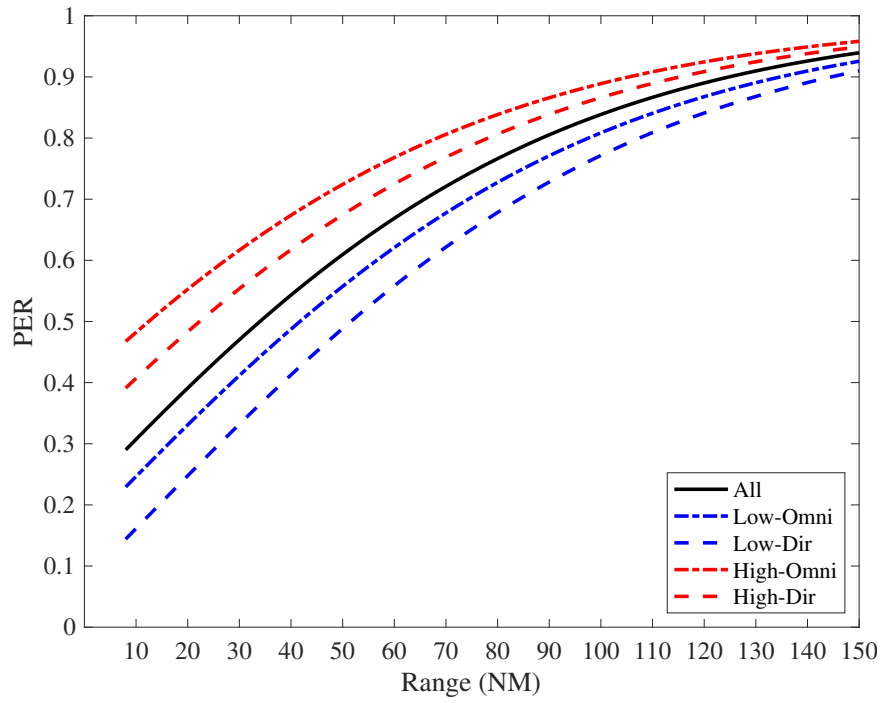
Figure 38. Flight Test - All Results
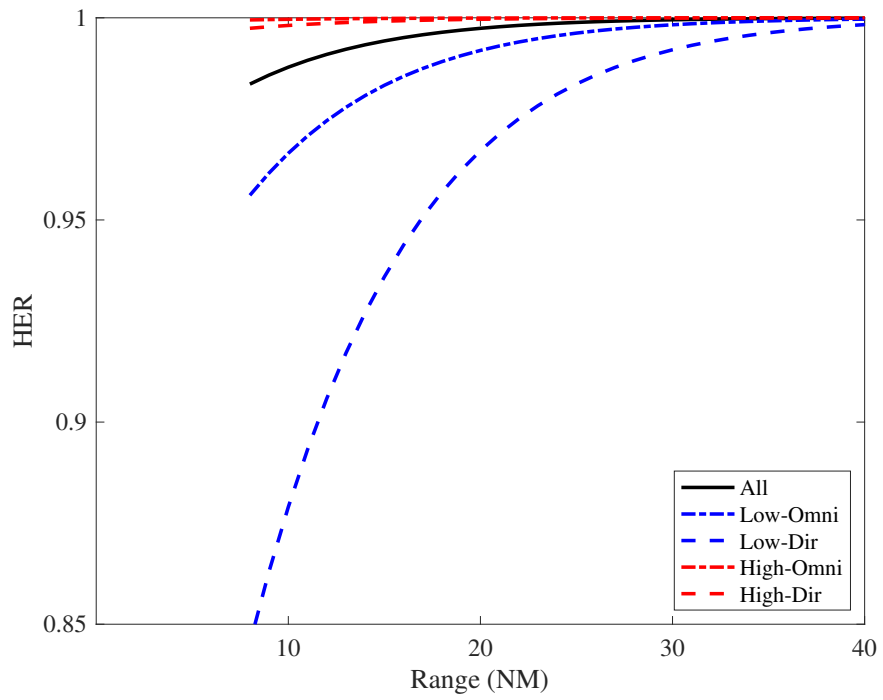
Figure 39. Derived - HER Results

4.6.4 Analysis.

What is the open-air Mode S-ES link performance and how does this impact the real-world implementation of the proposed protocol? The preceding plots and data reveal a lower bound on the performance of Mode S-ES when subject to test day conditions. If the actual Mode S-ES PER matches the performance determined here, the utility of the proposed packet switched key handoff mechanism is severely limited without modification.

Recall that key handoffs consist of 512 bits broken into 12 packets. All 12 packets must be received to achieve a successful handoff. The process is not stateful and there is no return channel with which to communicate packet status. The 12 packet sequence must be repeated until a certain probability of success, p_s is met. The actual probability used in implementation is a question of desired performance but would likely be between 0.8 and 0.95. If a successful handoff is not re-constructed after the completion of these attempts, another session is initiated (Figure 19). The ultimate metric of performance for a complete key handoff is elapsed time. This is the total time from the initiation of a secure session until all handoff attempts are complete. Several variables determine this time:

- Packets Per Attempt (assumed 12 for this research)

- Packet Transmission Rate (DO-260B calls for a maximum of 6.2 per second)

- Desired Probability of Success (0.9 is assumed unless otherwise noted)

- Packet Error Ratio

Packets per attempt is defined by the crypto scheme and PER is a characteristic of the environment. The two remaining variables are those which can be manipulated to improve time-based performance of a handoff. Table 6 shows the relative effect of decreasing p_s versus increasing packet transmission rate. It also makes clear the limited range an aircraft could be from a grounds station while executing a handoff and still have an expectation of success.

Table 6. Time Performance

Range	PER	HER	Attempts	Total Packets	Seconds
10	0.31	0.98835	197	2364	381
15	0.35	0.99431	404	4848	782
20	0.39	0.99735	867	10404	1678
25	0.43	0.99882	1957	23484	3788
30	0.47	0.99951	4686	56232	9070
35	0.51	0.99981	12018	144216	23261
40	0.54	0.99991	25651	307812	49647
45	0.58	0.99997	76422	917064	147914
		$p_s = 0.9$		$PPS = 6.2$	

Range	PER	HER	Attempts	Total Packets	Seconds
10	0.31	0.98835	197	2364	1
15	0.35	0.99431	404	4848	2
20	0.39	0.99735	867	10404	5
25	0.43	0.99882	1957	23484	12
30	0.47	0.99951	4686	56232	28
35	0.51	0.99981	12018	144216	72
40	0.54	0.99991	25651	307812	154
45	0.58	0.99997	76422	917064	459
		$p_s = 0.9$		$PPS = 2000$	

Range	PER	HER	Attempts	Total Packets	Seconds
10	0.31	0.98835	138	1656	267
15	0.35	0.99431	283	3396	548
20	0.39	0.99735	606	7272	1173
25	0.43	0.99882	1368	16416	2648
30	0.47	0.99951	3276	39312	6341
35	0.51	0.99981	8401	100812	16260
40	0.54	0.99991	17930	215160	34703
45	0.58	0.99997	53417	641004	103388
		$p_s = 0.8$		$PPS = 6.2$	

Range	PER	HER	Attempts	Total Packets	Seconds
10	0.31	0.98835	138	1656	1
15	0.35	0.99431	283	3396	2
20	0.39	0.99735	606	7272	4
25	0.43	0.99882	1368	16416	8
30	0.47	0.99951	3276	39312	20
35	0.51	0.99981	8401	100812	50
40	0.54	0.99991	17930	215160	108
45	0.58	0.99997	53417	641004	321
		$p_s = 0.8$		$PPS = 2000$	

Based on the previously mentioned constraints, it is likely that PER with production transmitters and receivers is significantly lower than the data here indicates. If so, this would increase the maximum range for an effective handoff. Additionally, increasing packet transmission rate (only for handoffs, not current Mode S packets) can lower the time requirement for a handoff. Both of these efforts are necessary prior to making a feasibility determination regarding the protocol in Chapter III.

V. Conclusion

5.1 Packet Switching & PER

Mode S is a communications protocol which lacks a multiple access scheme on 1090 MHz. Dozens, if not hundreds, of users are transmitting on the same frequency at the same time. This results in significant interference called false replies unsynchronized in time (FRUIT). The effect of FRUIT is to dramatically increase the packet error ratio (PER) compared to other digital communications techniques. A major effort of this research was to characterize the PER of Mode S-ES in a real-world, open-air environment. Several limitations detailed in Chapter IV caused the experimentally determined data to be a lower bound for the PER expected on production equipment. The experimentally determined PER is shown in Figure 40 and detailed in Chapter IV and Appendix E.
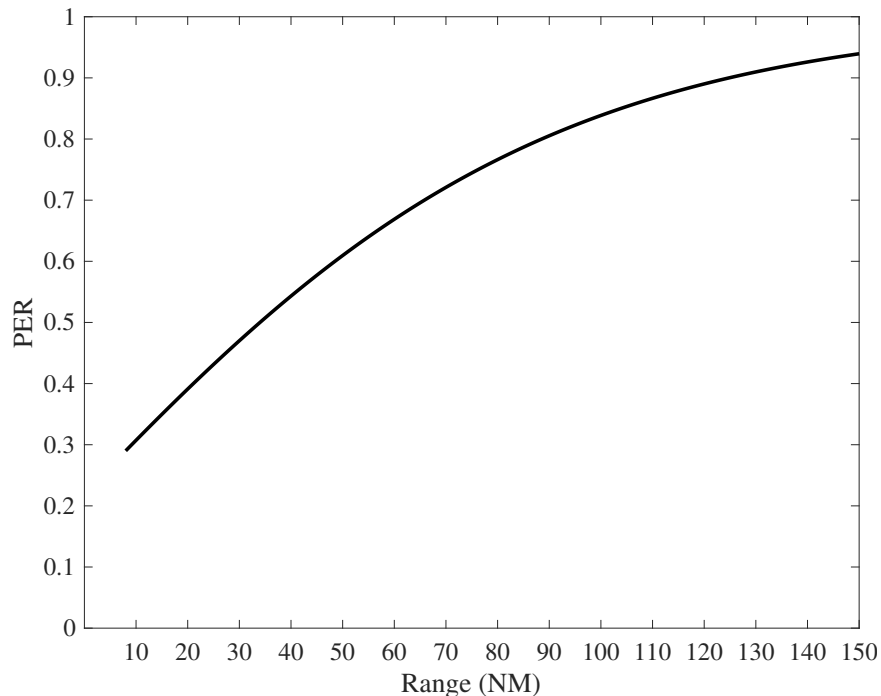

Figure 40. Overall Open-Air PER Results

Given the data found in this experiment, open-ended packet switching is not a valuable technique for use with Mode S-ES. In some limited circumstances, such as the case of a key handoff where the number of packets is limited to 12 or less, packet switching is potentially valuable. Further testing with production transmitters and receivers is required to quantify the usefulness of packet switching as a key handoff mechanism. If testing with production equipment yields results similar to those determined here, the key handoff construct is severely limited in range (no more than 40 NM). This reduces the viability of the key handoff portion of the confidentiality protocol proposed.

5.2 Confidentiality Protocol

Mode S-ES is devoid of security considerations. Data verification is accomplished via multilateration in some select areas of responsibility. Availability is slightly protected by high power levels and legacy backup systems. There are no authentication or confidentiality provisions in Mode S. Many proposals to add security to ADS-B would require significant changes to current specifications. By focusing solely on the problem of confidentiality, it becomes feasible to create a simple, secure, and interoperable protocol which is backwards compatible for current users.

Anonymity is gained by using an ephemeral, pseudo-random ICAO address known as a session unique ICAO address (SUIA). This replaces the assigned ICAO address in all Mode S packets transmitted in a session. Confidentiality or privacy are ensured by encrypting the ME Field, or payload, of Mode S-ES packets. These are encrypted using NIST approved format preserving encryption (FPE). The key used for encryption throughout the session is known as a session symmetric key (SSK). Various levels of anonymity and confidentiality can be achieved by selectively encrypting ME Fields based on their content. This is shown in Figure 41.
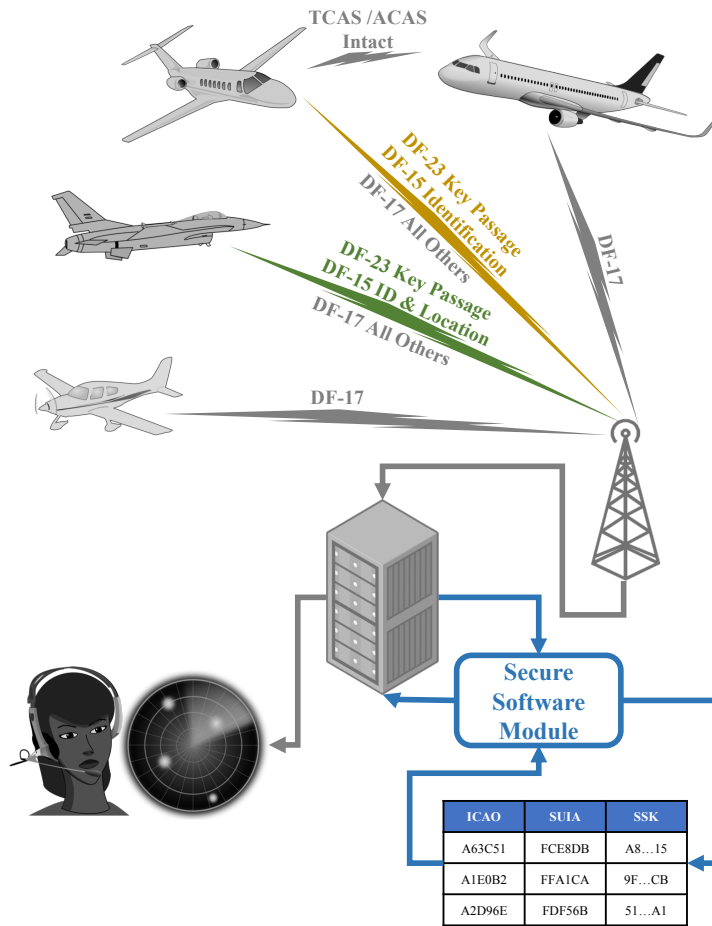
Figure 41. Operational Concept

Since confidentiality is the security tenet of interest and certificate based keys are often infeasible when distribution is to the general public, a unique unidirectional key handoff allows the transport of an SUIA and SSK. These parameters are generated on client avionics and then encrypted using the trusted air traffic control (ATC) public key. They are then transmitted to ATC for use throughout the remainder of the secure session. This transmission of the encrypted SUIA and SSK is the previously mentioned key handoff.

The use of unidirectional public key encryption for key handoff creates a challenge because Mode S-ES does not have the capability to maintain a stateful connection or acknowledge receipt of packets. The handoff is too large to be transmitted in a single packet,

requiring alternative means of transmission. These alternatives include Internet Protocol (IP) based transmission prior to or during flight, and an extension to Mode S-ES allowing connectionless packet switching. This proposal, while compatible with any method of transmission, maintains simplicity by using Mode S-ES packets to transport the key handoff to ATC. Packet switching on Mode S-ES is faced with the previously discussed PER challenges.

5.3 Attack and Research Classification

The determination of requirements for the proposed protocol was largely driven by the work accomplished to classify potential attacks and previous research into ADS-B security solutions. Starting with the classic Confidentiality, Integrity, and Availability tenants of information security, Chapter II expanded integrity into authentication and verification. Using this distinction allowed an analysis of threats and classification of most ADS-B security research, shown in Figure 13.

5.4 Synthesis

The proposed security protocol is a strong candidate for rapid implementation of confidentiality while using Mode S-ES. It meets all requirements pertaining to simplicity and interoperability while using proven cryptography. It is the only known proposal which uses the decomposition of confidentiality from authentication to attain the required simplicity. While the core of the protocol is sound, experimentally determined PER performance of Mode S-ES places undesirable limitations on the key handoff execution described in Chapter III. Range from an ADS-B ground station would be limited to 40 NM while executing a handoff with a reasonable probability of success. Fortunately, there are several alternative handoff transmission techniques which can be easily substituted. Follow on research should focus on evaluating these alternative methods.

5.5 Future Work

5.5.1 Cryptographic Implementation.

Excellent work has been done to characterize the cryptographic strength of various FPE algorithms. [95]. This work was accomplished prior to NIST approval and the algorithms were changed slightly prior to approval [102]. Follow-on analysis of these algorithms and potential hardware and software implementations is necessary to allow use in national security operations.

5.5.2 Avionics Capability.

The proposed system requires CSPRN generation and encryption using on-board avionics systems. Research into the availability of entropy sources and required computational power is required to determine any limits on the implementation of this protocol in present-day transponders.

5.5.3 Alternative Handoff Transmission.

At the time of publication, the latest revision to RTCA DO-260 is DO-260C and is in draft status. DO-260C adds a *phase overlay* capability to the current standard. The proposed addition uses eight phase shift keying (8PSK) to overlay three bits on each pulse. FEC is also included in the proposal. Overall, 204 additional data bits are added to each Mode S-ES packet. Implementation of key handoffs using the phase overlay would reduce the number of packets required for a handoff from twelve to two. Assuming the PER determined here or better, this would increase the handoff range to at least 120 NM. Even at a worst case 0.9 PER, a handoff would only take 37 seconds if desired $p_s = 0.9$. Additional systems analysis is required to determine the viability of key handoffs via phase overlay.

IP based transmission is also available for key handoff. This could be done in mission

planning or via on-board internet access. Significant disadvantages impact both and attack the core objective of simplicity. Additional research could characterize the usefulness and viability of an IP based key handoff.

5.5.4 Production Equipment PER.

Finally, there is value in determining the PER of Mode S-ES using production transmitters and receivers. It would also be valuable to quantify FRUIT while these experiments are taking place. These tests would require extensive coordination with the FAA if conducted in the US and would likely need funding for instrumented aircraft and ground stations.

5.6 Final Remarks

ADS-B is the future of air surveillance and collision avoidance. The paradox of ADS-B is that it implements modern and future applications with legacy digital communications technology in an already congested spectrum. This paradigm leaves the global air transport system with dated technology that is asked to carry growing amounts of data. Packets include information such as identification, precise location, and status. This data is transmitted without security considerations. The safety benefits of ADS-B are lost on operators who do not use it due to lack of confidentiality. The economic impact of the lack of privacy is significant to many users. Safety and security go hand in hand, there cannot be optimized safety without security considerations. This research proposes an interoperable ADS-B confidentiality protocol which can be implemented in the near future and suggests the necessary next steps toward implementation. Securing ADS-B is vital to achieve safe and secure global air operations in the twenty first century.

Appendix A. Additional Statistics

This appendix expands upon the introduction to the logistic regression analysis in Chapter IV.

A.1 Statistical Level of Confidence

The minimum confidence level across the open-air data set is 0.9954. This is based on the total quantity of samples collected across all open-air test sorties shown in Figure 42.
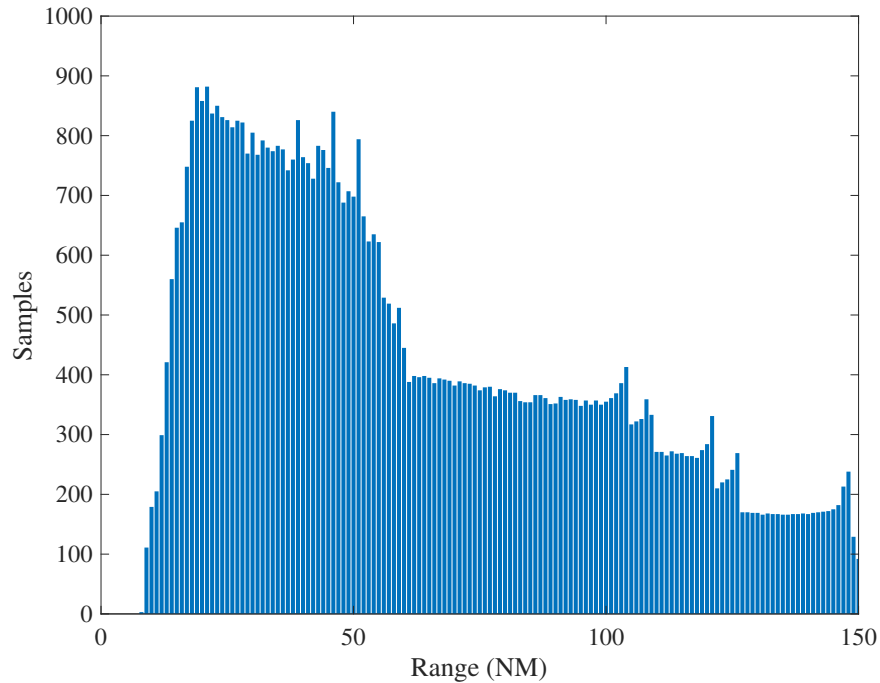

Figure 42. Sample Quantity Per 1 NM Bin

Calculation of statistical level of confidence (SLC) is based on the binomial distribution function:

$$P_n(k) = \frac{n!}{k!(n-k)!} p^k q^n - k \tag{17}$$

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 gives the error ratio, $P(e)$ when more or less than N events occur in n attempts:

$$P(e \leq N) = \sum_{k=0}^{N} \frac{n!}{k!(n-k)!} p^k q^{n-k} \qquad (18)$$

$$P(e > N) = \sum_{k=N+1}^{n} \frac{n!}{k!(n-k)!} p^k q^{n-k} \qquad (19)$$

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

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

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

$$n = \frac{1}{P(e)}\left[-\ln(1 - SLC) + ln\left(\sum_{k=0}^{N} \frac{(n \cdot P(e))^k}{k!} \right) \right] \qquad (20)$$

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.

A.2   Logistic Regression Statistics

A.2.1   P-Values.

The values in Tables 7 and 8 reveal that all independent variables investigated are significant factors. In cases where P-Values were so small as to exceed the ability of a double precision floating point to represent them, they are annotated as approaching zero: $\rightarrow 0$.

Table 7. Sim Model P-Values

	Range	**Range FRUIT**
$\boldsymbol{P}_{intx}$	$\to 0$	$\to 0$
$\boldsymbol{P}_r$	$\to 0$	$\to 0$
$\boldsymbol{P}_f$	-	$\to 0$

Table 8. Flight Test Model P-Values

	Range	**Range FRUIT**	**Range Antenna**	**Range Direction**	**Range FRUIT Antenna**	**Range FRUIT Direction**	**Range Antenna Direction**	**Range FRUIT Antenna Direction**
$\boldsymbol{P}_{intx}$	$\to 0$	$7.2151 \cdot 10^{-52}$	$\to 0$	$\to 0$	$3.9832 \cdot 10^{-96}$	$\to 0$	$\to 0$	$\to 0$
$\boldsymbol{P}_r$	$\to 0$	$\to 0$	$\to 0$	$\to 0$	$\to 0$	$\to 0$	$\to 0$	$\to 0$
$\boldsymbol{P}_f$	-	$\to 0$	-	-	$\to 0$	$\to 0$	-	$\to 0$
$\boldsymbol{P}_a$	-	-	$2.7155 \cdot 10^{-46}$	-	$1.0772 \cdot 10^{-46}$	-	$1.6220 \cdot 10^{-50}$	$3.7822 \cdot 10^{-51}$
$\boldsymbol{P}_d$	-	-	-	$\to 0$	-	$\to 0$	$\to 0$	$\to 0$

Appendix B. Experimental ADS-B Testbed System

The Experimental ADS-B Testbed System (EATS) is a Mode S transmitter designed for rapid, software-based prototyping of ADS-B improvements and variations. It uses software defined radio (SDR) technology with off-the-shelf front end components to enable airborne, open-air experimentation while remaining low cost.

EATS radio frequency (RF) components are optionally installed in a Reconfigurable Airborne Sensor, Communication, and Laser (RASCAL) pod to enable external carriage on F-16C/D, T-38C, or C-12J aircraft. The pod provides 15 Amperes of 28 volt direct current power, passive thermal management, and on/off control for the RF components.

EATS utilizes an Ettus E310 SDR to allow researchers to execute rapid prototyping while maintaining a standards compliant physical RF transmission. DoD AIMS has issued a Recommendation for Frequency Assignment and a Recommendation for Stage 2 Radio Frequency Authorization. These enable open-air testing on 1090 MHz provided the EATS configuration does not change. Testing and certification of EATS was conducted by AIMS
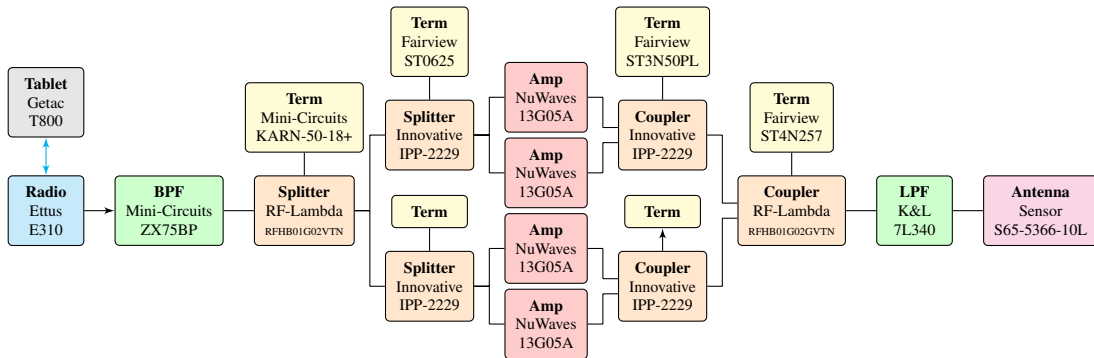
**Figure 43. EATS Transmit Hardware**

at Air Force Institute of Technology laboratories. These memorandums are included as Appendix C.

The analog front end consists of the analog portions of the E310 signal path, filters, amplifiers, and couplers. The front end was designed to provide 200 Watts of RF power at the antenna connection. RASCAL electrical power voltage limits the actual output to 177

Watts, still in the range of production Mode S transponders. The EATS block diagram is shown in Figure 43.

Any computer equipped with Ethernet can provide I/Q data to EATS. If EATS is installed in a RASCAL and carried on an ejection seat aircraft, a tablet is required for safety. A glove compatible touch-based user interface was used to accomplish this research. The user interface is shown in Figure 44.

Further characterization is required to determine the performance of the RASCAL and antenna combination. It was noted during testing that the antenna pattern was affected by integration with the pod.
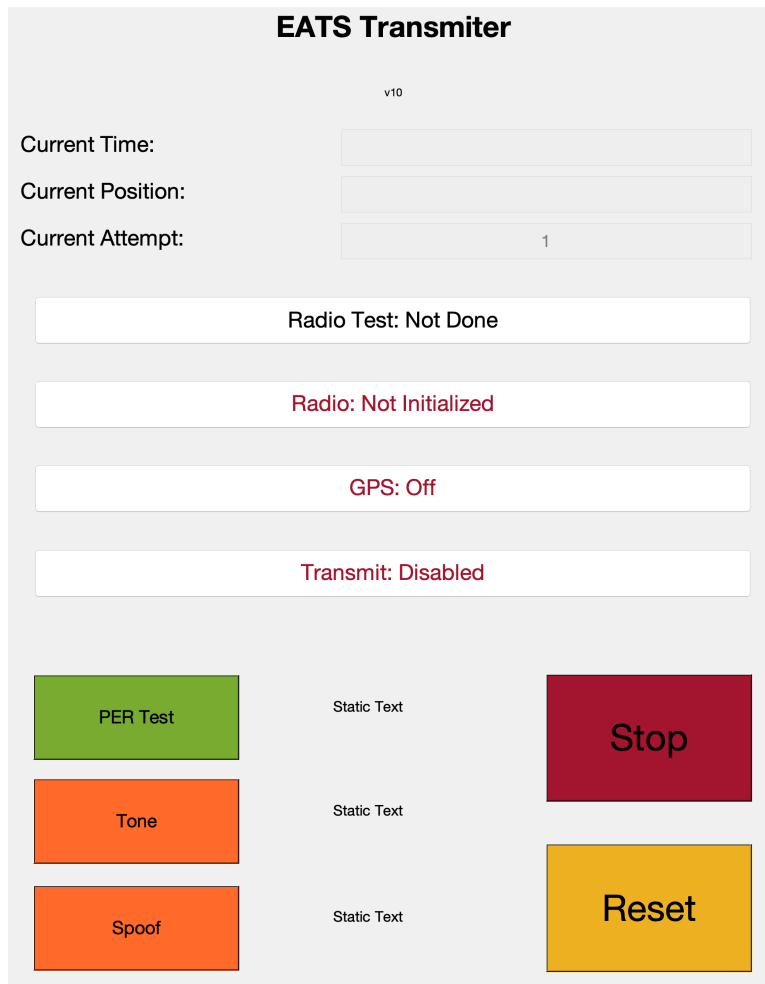

Figure 44. EATS Touch Interface

85

Appendix C. AIMS Recommendations

The following memorandums document the Recommendation for Frequency Assignment and Recommendation for Stage 2 Radio Frequency Authorization granted by DoD AIMS.

DEPARTMENT OF DEFENSE
INTERNATIONAL AIMS PROGRAM OFFICE
ROBINS AIR FORCE BASE GEORGIA

02 July 2018
OL 1818301

MEMORANDUM FOR   FEDERAL AVIATION ADMINISTRATION
SPECTRUM ASSIGNMENT AND ENGINEERING OFFICE
800 INDEPENDENCE AVENUE, SW
WASHINGTON, DC 20591

FROM: DoD International AIMS Program Office
710 Ninth Street, Bldg 937
Robins AFB, GA 31098

SUBJECT: DoD AIMS Recommendation for a Frequency Assignment for the Experimental Automatic Dependent Surveillance Broadcast Out 1090 MHz Extended Squitter (ADS-B) Testbed (EAT) Transmitter Module Set (Universal Software Radio Peripheral (USRP) Radio Part Number 156333D and Nuwaves Amplifier(s) Part Number 30B015C) Software Version 1.3

Reference: (a) DoD AIMS 03-1000B Performance/Design and Qualification Requirements Technical Standard for the ATCRBS/IFF/Mark XIIA Electronic Identification System and Military Implementation of Mode S Amendment 1, dated 1 July 2015
(b) Radio Technical Commission for Aeronautics DO-260B, Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast (TIS-B), dated 13 December 2011
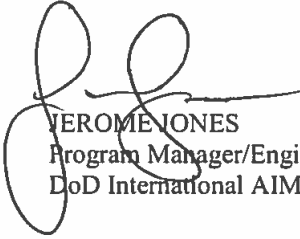
1. The DoD AIMS PO evaluated the EAT Transmitter Module Set on 27 June 2018 at the Air Force Institution of Technology on Wright Patterson Air Force Base. Maximum Power Output, Waveform characteristics, Transmission Frequency and Modulation, and Message Content was evaluated and determined to meet military and civilian standards in the 1090 MHz spectrum. The EAT Transmitter Module will be flown on several aircraft (T-38/F-16/C-12) in Special Use Airspace only to test an additional ADS-B capability designed to limit public access to their aircraft information. This information will be continually provided to Federal and DoD Agencies as needed.

2. This memo serves as the DoD AIMS PO Recommendation for a Frequency Assignment for Experimental Automatic Dependent Surveillance Broadcast Out 1090 MHz Extended Squitter (ADS-B) Testbed (EAT) Transmitter Module Set (USRP Radio Part Number 156333D and Nuwaves Amplifier(s) Part Number 30B015C) Software Version 1.3.   Any

OL 1818301 Page **1** of **2**

changes/deviations to hardware, software, and/or configuration require the approval and consent of the DoD AIMS PO to maintain the frequency assignment recommendation.

3. The DoD AIMS PO points of contact are Mark Graves, (478) 327-4488, DSN 497-4488, email: mark.graves.8.ctr@us.af.mil and Douglas Samples, (478) 926-3032, DSN 468-3032, e-mail: douglas.samples.1.ctr@us.af.mil.

JEROME JONES
Program Manager/Engineer
DoD International AIMS Program Office

FOR OFFICIAL USE ONLY

DEPARTMENT OF DEFENSE
INTERNATIONAL AIMS PROGRAM OFFICE
ROBINS AIR FORCE BASE GEORGIA

02 July 2018
OL 1818302

MEMORANDUM FOR   FEDERAL AVIATION ADMINISTRATION
SPECTRUM ASSIGNMENT AND ENGINEERING OFFICE
800 INDEPENDENCE AVENUE, SW
WASHINGTON, DC 20591

FROM: DoD International AIMS Program Office
710 Ninth Street, Bldg 937
Robins AFB, GA 31098

SUBJECT: Recommendation for Stage 2 Radio Frequency Authorization for the Experimental
Automatic Dependent Surveillance Broadcast Out 1090 MHz Extended
Squitter (ADS-B) Testbed (EAT) Transmitter Module Set (Universal Software
Radio Peripheral (USRP) Radio Part Number 156333D and Nuwaves Amplifier(s)
Part Number 30B015C) Software Version 1.3

References: (a) DoD AIMS 03-1000B Performance/Design and Qualification Requirements
Technical Standard for the ATCRBS/IFF/Mark XIIA Electronic Identification
System and Military Implementation of Mode S Amendment 1, dated 1 July
2015
(b) Radio Technical Commission for Aeronautics DO-260B, Minimum Operational
Performance Standards for 1090 MHz Extended Squitter Automatic Dependent
Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast
(TIS-B), dated 13 December 2011

1. The purpose of this letter is to provide a recommendation for a stage 2 frequency approval for
the subject ADS-B Transmitter Module set. This letter is not a box-level certification from the
DoD International AIMS Program Office (DoD AIMS PO). The EAT Transmitter Module will
be flown on several aircraft (T-38/F-16/C-12) in Special Use Airspace only to test an additional
ADS-B capability designed to limit public access to their aircraft information. This information
will be continually provided to Federal and DoD Agencies as needed.

2. The DoD AIMS PO tested the EAT Transmitter Module Set on 27 June 2018 at the Air Force
Institution of Technology on Wright Patterson Air Force Base. Maximum Power Output,
Waveform characteristics, Transmission Frequency and Modulation, and Message Content was
evaluated and determined to meet military and civilian standards in the 1090 MHz spectrum.
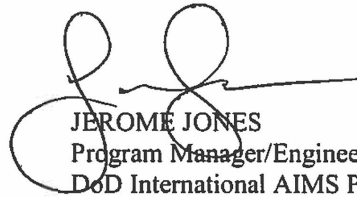
3. The DoD AIMS PO recommends frequency approval for the Experimental Automatic Dependent Surveillance Broadcast Out 1090 MHz Extended Squitter (ADS-B) Testbed (EAT) Transmitter Module Set (USRP Radio Part Number 156333D and Nuwaves Amplifier(s) Part Number 30B015C) Software Version 1.3

.

4. The DoD AIMS PO points of contact are Mark Graves, (478) 327-4488, DSN 497-4488, email: mark.graves.8.ctr@us.af.mil and Douglas Samples, (478) 926-3032, DSN 468-3032, e-mail: douglas.samples.1.ctr@us.af.mil.

JEROME JONES
Program Manager/Engineer
DoD International AIMS Program Office

Appendix D. Ground Stations

D.1   Introduction

Receiver site locations were vital to successful test operations. Two sites were selected to provide a contrasting low and high FRUIT environment. Figure 45 is an overview map of the low and high FRUIT sites within the San Bernardino National Forest.
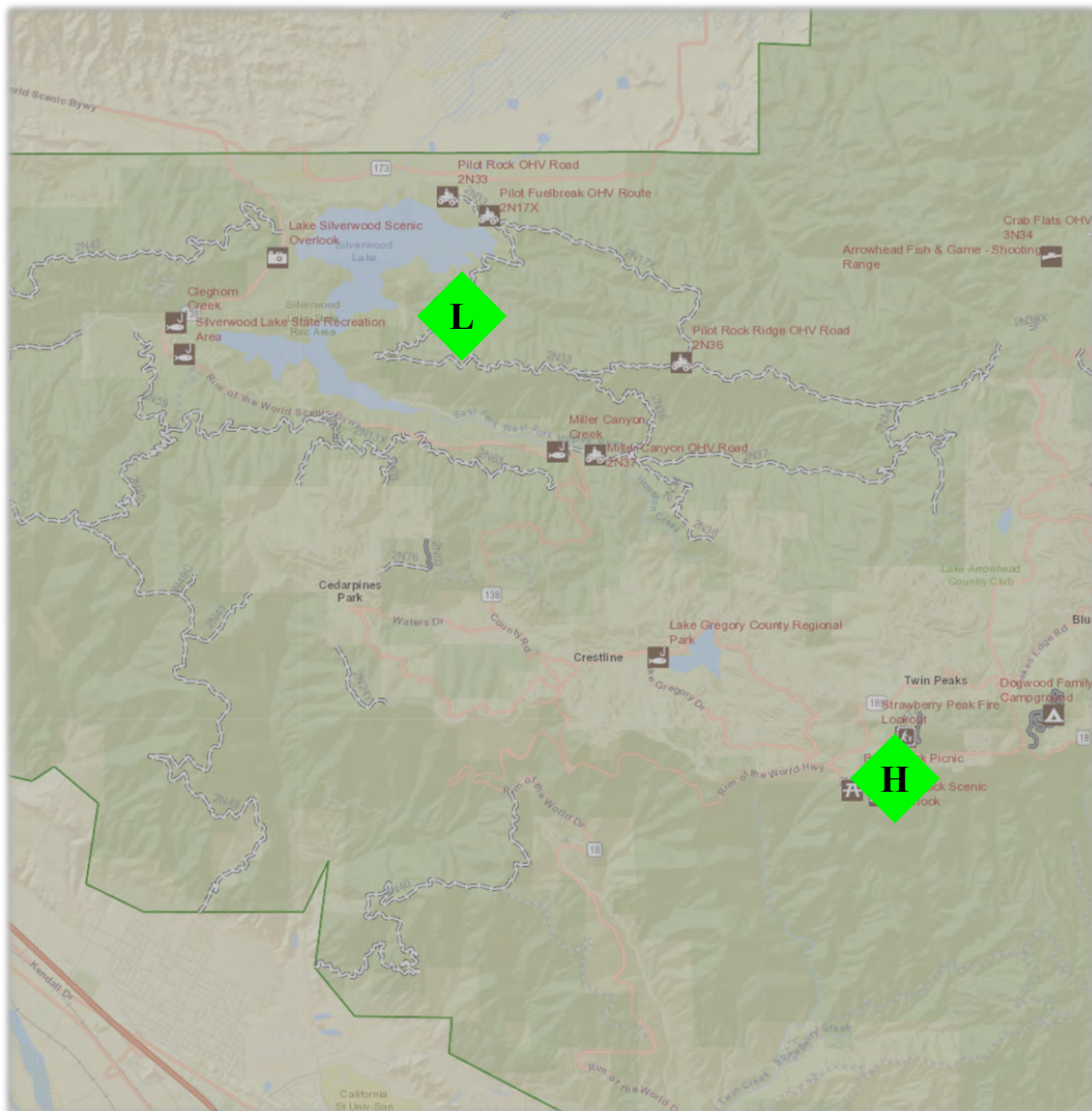
Figure 45. Low and High FRUIT Receiver Sites

D.2 Low FRUIT - Pilot Rock Trail Road

D.2.1 Description.

The low FRUIT receiver site was located along Pilot Rock Trail Road, also known as 2N33. This location provides terrain masking (Figure 46) to the majority of the LA basin air traffic creating a low FRUIT environment.

D.2.2 Coordinates.

- 34°13.93', -117°14.08'

D.2.3 Terrain Masking.

Figure 46 shows the masking profile for the low FRUIT receiver site (shown as a purple 'x'). The orange line shows line-of-sight (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.
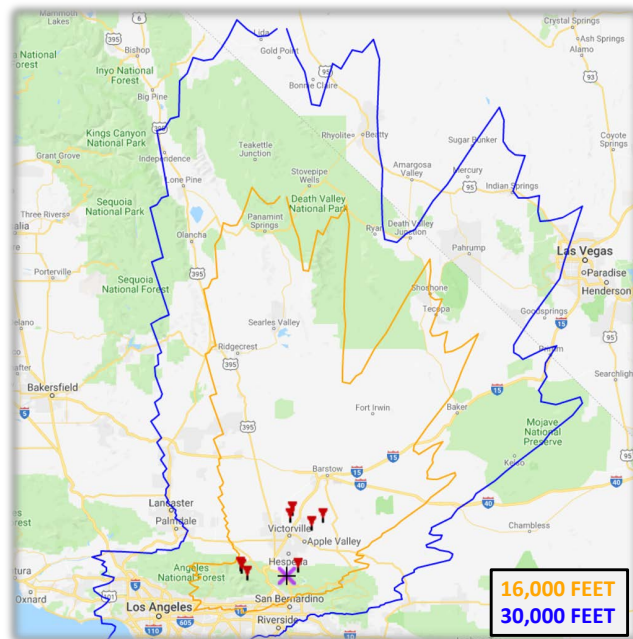
Figure 46. Low FRUIT Terrain Masking Profile

D.3   High FRUIT - Strawberry Peak Fire Tower

D.3.1   Description.

The high FRUIT receiver site was located at the Strawberry Peak Fire Tower. This location provided minimal terrain masking (Figure 47) to the majority of the LA basin air traffic creating a high FRUIT environment.

D.3.2   Coordinates.

- 34°13.93', -117°14.08'

D.3.3   Terrain Masking.

Figure 47 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.
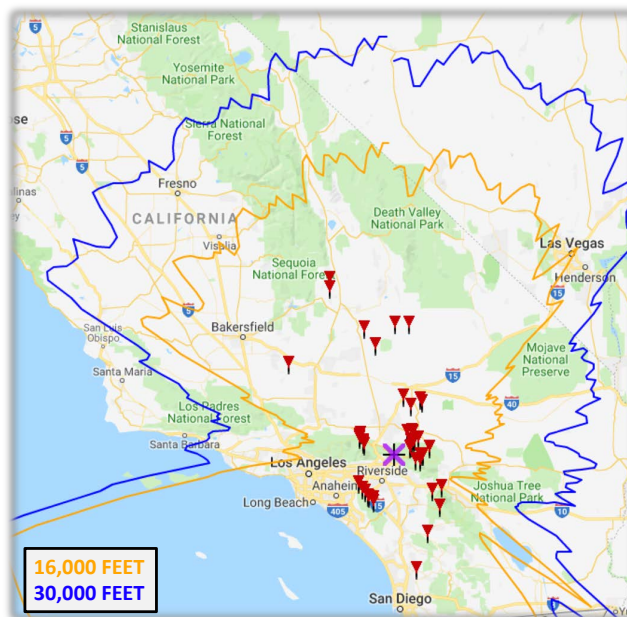
**Figure 47. High FRUIT Terrain Masking Profile**

Appendix E. Model Table

Pre-calculated tabular data is included here for ease of access. Tables 9 through 13 contain PER data rounded to the hundredths place.

Table 9. 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 10. 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 11. 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 12. 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 13. 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

Bibliography

1. S. Harrison, "Deadly 1957 Midair Collision Over Pacoima," Los Angeles, 1 2018.

2. E. Chang, R. Hu, D. Lai, R. Li, Q. Scott, and T. Tyan, "The Story of Mode S," *MIT Course 6.933*, p. 1–40, 2000.

3. A. Costin and A. Francillon, "Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Black Hat USA*, 2012.

4. B. Burfeind, B. Cunningham, E. K. Caberto, R. Forystek, and J. A. McKenzie, "A Limited Demonstration of ADS-B Security," USAF Test Pilot School, Edwards AFB, Tech. Rep., 2019.

5. C. Brose and E. King, "National Defense Authorization Act for Fiscal Year 2017 Report," Comittee on Armed Services, Washington DC, Tech. Rep. 114-255, 2017.

6. D. E. Stokes, *Pasteur's quadrant: Basic science and technical innovation*, 1st ed. Washington: The Brookings Institution, 1997.

7. K. Yang, K. Zhang, J. Ren, and X. S. Shen, "Security and privacy in mobile crowd-sourcing networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 75–81, 2015.

8. Radio Technical Commission for Aeronautics SC-209, "DO-181E: Minimum Operational Performance Standards for ATCRBS / Mode S Airborne Equipment," Washington DC, pp. 1–804, 2011.

9. Radio Technical Commission for Aeronautics SC-186, "DO-260B: Minimum Operational Performance Standards for 1090 MHz Extended Squitter ADS-B and TIS-B," Washington DC, pp. 1–1446, 2011.

10. B. Burfeind, R. Mills, and P. Beach, "Airborne Crowdsensing Networks: Safe and Secure Aircraft-Based Observations," 2018.

11. Federal Aviation Administration, "ADS-B," 2020. [Online]. Available: https://www.faa.gov/nextgen/programs/adsb/

12. J. Sun, "The 1090MHz Riddle," 2020. [Online]. Available: https://mode-s.org

13. M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

14. B. Burfeind, R. Mills, S. Nykl, J. A. Betances, and C. Sielski, "Confidential ADS-B: A Lightweight , Interoperable Approach," in *2019 Aerospace Conference*. Big Sky, Montana: IEEE, 2019.

15. D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.ijcip.2011.06.001

16. D. Magazu III, "Exploiting the Automatic Dependent Surveillance- Broadcast System Via False Target Injection," vol. 2, no. 2, p. 101, 2012. [Online]. Available: www.dtic.mil/dtic/tr/fulltext/u2/a561697.pdf

17. M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111–118, 2014.

18. M. Leonardi, E. Piracci, and G. Galati, "ADS-B Jamming Mitigation: A Solution Based on a Multichannel Receiver," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 44–51, 2017.

19. B. Schneier, *Applied Cryptography, Second Edition*, 2015.

20. C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ijcip.2013.02.001

21. R. C. Agbeyibor, "Secure ADS-B: Towards Airborne Communications Security in the FAA's NexGen ATS," Master's thesis, Air Force Institute of Technology, 2014.

22. B. Heruska, "Design and Characterization of a Secure ADS-B Prototype," Master's thesis, Air Force Institute of Technology, 2015.

23. E. Hableel, J. Baek, Y. J. Byon, and D. S. Wong, "How to protect ADS-B: Confidentiality Framework for Future Air Traffic Communication," *Proceedings - IEEE INFOCOM*, vol. 2015-Augus, pp. 155–160, 2015.

24. D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," no. 1, pp. 258–275, 2005.

25. C. Finke, J. Butts, R. Mills, and M. Grimaila, "Evaluation of a cryptographic security scheme for air traffic control's next generation upgrade," *8th International Conference on Information Warfare and Security, ICIW 2013*, pp. 259–264, 2013.

26. R. Agbeyibor, J. W. Butts, M. R. Grimaila, and R. Mills, "Evaluation of Format-Preserving Encryption Algorithms for Critical Infrastructure Protection," *Critical Infrastructure Protection VIII*, vol. 2014, pp. 245–261, 2014.

27. H. Yang, M. Yao, Z. Xu, and B. Liu, "LHCSAS : A Lightweight and Highly-Compatible Solution for ADS-B Security," 2017.

28. K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can Cryptography Secure Next Generation Air Traffic Surveillance," *IEEE Security & Privacy*, 2014.

29. C. Finke, J. Butts, and R. Mills, "ADS-B Encryption: Confidentiality in the Friendly Skies," *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*, p. 1, 2013. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2459976.2459986

30. K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *Proceedings of the IEEE Aerospace Conference*, 2006, pp. 1–7.

31. J. Baek, E. Hableel, Y. J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 690–700, 2017.

32. E. Cook, "ADS-B, friend or foe: ADS-B message authentication for NextGen aircraft," *Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, H*, pp. 1256–1261, 2015.

33. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.

34. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013.

35. ——, "Online/offline attribute-based encryption," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

36. A. Fiat and M. Naor, "Broadcast encryption," *Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, 1994.

37. C. Park, J. Hur, S. Hwang, and H. Yoon, "Authenticated public key broadcast encryption scheme secure against insiders' attack," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 113–122, 2012. [Online]. Available: http://dx.doi.org/10.1016/j.mcm.2011.01.056

38. J. Baek, Y. j. Byon, E. Hableel, and M. Al-Qutayri, "An Authentication Framework for Automatic Dependent Surveillance-Broadcast (ADS-B) Based on Online/Offline Identity-Based Signature," in *Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2013.

39. A. Yang, X. Tan, J. Baek, and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165–175, 2017.

40. D. He, N. Kumar, K. K. R. Choo, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 454–464, 2017.

41. R. Chen and C. Si, "ADS-B data authentication based on AH protocol," *Proceedings - 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, DASC 2013*, pp. 21–24, 2013.

42. T. Kacem, D. Wijesekera, and P. Costa, "Integrity and authenticity of ADS-B broadcasts," *IEEE Aerospace Conference Proceedings*, vol. 2015-June, 2015.

43. T. Kacem, D. Wijesekera, P. Costa, and J. Carvalho, "Secure ADS-B Design & Evaluation," in *Proceedings of the 2015 IEEE International Conference on Vehicular Electronics and Safety*, Yokohama, Japan, 2015, pp. 213–218.

44. T. Kacem, D. Wijesekera, P. Costa, and A. Barreto, "An ADS-B intrusion detection system," *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, pp. 544–551, 2016.

45. T. Kacem, A. Barreto, D. Wijesekera, and P. Costa, "ADS-Bsec: A novel framework to secure ADS-B," *ICT Express*, vol. 3, no. 4, pp. 160–163, 2017. [Online]. Available: https://doi.org/10.1016/j.icte.2017.11.006

46. Y.-c. Hu and K. P. Laberteaux, "Strong VANET Security On A Budget," *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, 2006.

47. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *CryptoBytes*, 2002.

48. ——, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceeding 2000 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2000, pp. 56–73.

49. M. H. Eldefrawy, M. K. Khan, K. Alghathbar, and E. S. Cho, "Broadcast authentication for wireless sensor networks using nested hashing and the chinese remainder theorem," *Sensors*, 2010.

50. T. Kacem, D. Wijesekera, and P. Costa, "Key Distribution Scheme for Aircraft Equipped with Secure ADS-B IN," pp. 2341–2346, 2017.

51. K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Communications*, 2010.

52. S. Jana and S. Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2010. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5210105

53. S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *2008 IEEE International Conference on RFID (Frequency Identification), IEEE RFID 2008*, 2008.

54. D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180–1192, 2015.

55. J. Rice, R. F. Mills, M. A. Temple, and J. D. Peterson, "Increased ambiguity resolution in digital radio frequency receivers," *Microwaves, Communications, Antennas and Electronic Systems (COMCAS), 2015 IEEE International Conference on*, no. November, pp. 1–4, 2015.

56. J. Hall, M. Barbeau, and E. Kranakis, "Radio frequency fingerprinting for intrusion detection in wireless networks," *IEEE Transactions on Defendable and Secure Computing*, 2005.

57. S. Mathur, W. Trappe, N. Mandayam, and C. Ye, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," *Proceedings of the 14th*, pp. 128–139, 2008.

58. C. Laurendeau and M. Barbeau, "Insider Attack Attribution Using Signal Strength-Based Hyperbolic Location Estimation," *Security and Communication Networks*, vol. 1, no. 4, pp. 337–349, 2008.

59. ——, "Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks," *Eurasip Journal on Wireless Communications and Networking*, 2009.

60. Z. Shen and H. Wang, "An ADS-B spoofing attack detection method based on LASSO ensemble empirical mode decomposition," *2015 International Conference on Wireless Communications and Signal Processing, WCSP 2015*, 2015.

61. M. Strasser, S. Čapkun, C. Pöpper, and M. Čagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proceedings - IEEE Symposium on Security and Privacy*, 2008.

62. C. Pöpper, M. Strasser, and S. Capkun, "Jamming-resistant Broadcast Communication without Shared Keys," *Proceedings of the USENIX Security Symposium*, pp. 231–247, 2009.

63. W. Harman, J. Gertz, and A. Kaminsky, "Techniques for Improved Reception of 1090 MHz ADS-B Signals," *Aviation*, pp. 1–9, 1998.

64. D. Jeon, Y. Eun, and H. Kim, "Estimation fusion with radar and ADS-B for air traffic surveillance," *International Journal of Control, Automation and Systems*, vol. 13, no. 2, pp. 336–345, 2015.

65. W. Liu, J. Wei, M. Liang, Y. Cao, and I. Hwang, "Multi-Sensor Fusion and Fault Detection using Hybrid Estimation for Air Traffic Surveillance," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2323–2339, 2013.

66. O. Baud, N. Honore, and O. Taupin, "Radar / ADS-B data fusion architecture for experimentation purpose," *2006 9th International Conference on Information Fusion, FUSION*, 2006.

67. M. S. Huang, R. M. Narayanan, Y. Zhang, and A. Feinberg, "Tracking of noncooperative airborne targets using ADS-B signal and radar sensing," *International Journal of Aerospace Engineering*, vol. 2013, 2013.

68. E. Piracci and G. Galati, "ADS-B Vulnerability to Low Cost Jammers: Risk Assessment and Possible Solutions," in *2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles*, 2014, pp. 41–46.

69. R. Wu, G. Chen, W. Wang, D. Lu, and L. Wang, "Jamming suppression for ADS-B based on a cross-antenna array," *ICNS 2015 - Innovation in Operations, Implementation Benefits and Integration of the CNS Infrastructure, Conference Proceedings*, pp. K31–K39, 2015.

70. A. Tart and T. Trump, "Addressing security issues in ADS-B with robust two dimensional generalized sidelobe canceller," in *International Conference on Digital Signal Processing, DSP*, vol. 2017-Augus, no. 1, 2017.

71. M. Monteiro, A. Barreto, T. Kacem, J. Carvalho, D. Wijesekera, and P. Costa, "Detecting Malicious ADS-B Broadcasts Using Wide Area Multilateration," in *34th Digital Avionics Systems Conference*, 2015, pp. 1–12.

72. J. Naganawa, H. Tajima, H. Miyazaki, T. Koga, and C. Chomel, "ADS-B Anti-Spoofing Performance of Monopulse Technique with Sector Antennas," *2017 Ieee Conference on Antenna Measurements & Applications (Cama)*, pp. 87–90, 2017.

73. C.-W. Liao and S.-S. Jan, "The use of the phase difference observation of 1090 MHz ADS-B signals for wide area multilateration," in *28th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS 2015*, 2015.

74. D. Moser, P. Leu, V. Lenders, A. Ranganathan, F. Ricciato, and S. Capkun, "Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures," *22nd Annual International Conference on Mobile Computing and Networking, MobiCom 2016*, no. CONFCODENUMBER, pp. 375–386, 2016. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84994075795&partnerID=40&md5=d41bf85a970cc0af971b3320cddb3323

75. R. Kaune, C. Steffes, S. Rau, W. Konle, and J. Pagel, "Wide area multilateration using ADS-B transponder signals," *Proc. of FUSION'12 - 15th IEEE International Conference on Information Fusion*, pp. 727–734, 2012. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6289874

76. N. O. Tippenhauer and S. Čapkun, "ID-based secure distance bounding and localization," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009.

77. R. Baker and I. Martinovic, "Secure Location Verification with a Mobile Receiver," *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy - CPS-SPC '16*, pp. 35–46, 2016. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2994487.2994497

78. Y. Nijsure, G. Kaddoum, G. Gagnon, F. Gagnon, C. Yuen, and R. Mahapatra, "Adaptive Air-to-Ground Secure Communication System based on ADS-B and Wide Area Multilateration," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3150 – 3165, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7113878

79. M. Strohmeier, V. Lenders, and I. Martinovic, "A k-NN-based Localization Approach for Crowdsourced Air Traffic Communication Networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 9251, no. c, pp. 1–21, 2018.

80. ——, "Lightweight Location Verification in Air Traffic Surveillance Networks," *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security - CPSS '15*, pp. 49–60, 2015. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2732198.2732202

81. M. Strohmeier, M. Schäfer, I. Martinovic, M. Smith, and V. Lenders, "Crowdsourcing security for wireless air traffic communications," in *9th International Conference on Cyber Conflict (CyCon)*, 2017.

82. Y. Kim, J.-Y. Jo, and S. Lee, "ADS-B vulnerabilities and a security solution with a timestamp," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, 2017.

83. E. Wallace, "Blockchain Ledgers," Edwards, California, 2018.

84. N. Ghose and L. Lazos, "Verifying Ads-B Navigation Information Through Doppler Shift Measurements," in *Digital Avionics Systems Conference*, 2015.

85. S. Brands and D. Chaum, "Distance-Bounding Protocols," in *Advances in Cryptology — EUROCRYPT '93*, 1993.

86. K. Mueller and J. Krozel, "Aircraft ADS-B intent verification based on a Kalman tracking filter," *AIAA Guidance, Navigation and Control Conference*, no. August, 2000. [Online]. Available: http://www.aric.or.kr/treatise/journal/content.asp?idx= 10888

87. J. Krozel, D. Andrisani, M. A. Ayoubi, T. Hoshizaki, and C. Schwalm, "Aircraft ADS-B Data Integrity Check," *AIAA Aircraft Technology, Integration, and Operations Conference*, no. August, pp. 1–11, 2004.

88. V. S. Bagmare, N. K. Mangali, and S. Singh, "G3 Synced Time Stamped ADS-B Data for Surveillance and Data Fusion Application," in *IEEE WISPNET*, vol. 37, 2017, pp. 1915–1919.

89. J. D. Silva, J. Brancalion, and D. Fernandes, "Data fusion techniques applied to scenarios including ADS-B and radar sensors for air traffic control," *2009 12th International Conference on Information Fusion*, pp. 1481–1488, 2009.

90. Systems Management College, *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Aquisition University, 2001, no. January. [Online]. Available: http://ocw.mit.edu/courses/aeronautics-and-astronautics/ 16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf

91. K. Lynch, "Federal Aviation Administration Exploring Possible Privacy Protections for ADS-B," 8 2015. [Online]. Available: https://www.ainonline.com/aviation-news/ business-aviation/2015-08-04/faa-exploring-possible-privacy-protections-ads-b

92. International Civil Aviation Organization, "About ICAO," 2018. [Online]. Available: https://www.icao.int/about-icao/Pages/default.aspx

93. ——, "Aeronautical Telecommunications - Communications Systems," Montreal, 2016.

94. ——, "Aeronautical Telecommunications - Surveillance and CAS," Montreal, 2002.

95. C. D. Finke, "Format Preserving Encryption: Evaluating FFX for Use Within the NextGen Air Traffic Control System," Master's thesis, Air Force Institute of Technology, 2013.

96. L. E. Frenzel, *Handbook of Serial Communications Interfaces*. Elsevier, 2016.

97. T. Mooring, "FCC Table of Frequency Allocations," 2019.

98. P. Enge, D. Akos, and J. Do, "Measurements of Man-Made Spectrum Noise Floor," National Aeronautics and Space Administration, Washington DC, Tech. Rep. November, 2004. [Online]. Available: http://corporations.ic.gc.ca/epic/internet/insmt-gst. nsf/vwapj/smse00205-novatel-nasa01.pdf/$FILE/smse00205-novatel-nasa01.pdf

99. A. Popa, "Increasing the Performance of Energy-Detection Based UWB Demodulator with a Supplementary Integration Block," *Advances in Electrical and Computer Engineering*, vol. 12, no. 3, pp. 27–32, 2012.

100. D. J. Bernays, S. D. Thompson, and W. H. Harman, "Measurements of ADS-B Extended Squitter Performance in the Los Angeles Basin Region," *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 2, 2000.

101. G. Rodríguez, "Generalized Linear Statistical Models," 2007. [Online]. Available: http://data.princeton.edu/wws509/notes/

102. M. Dworkin, "NIST Special Publication 800-38G — Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption," *National Institute of Standards and Technology Special Publication 800-38G*, p. 1..28, 2016.

REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
26-03-2020	Graduate Research Paper	Sep 2017 – Mar 2020

4. TITLE AND SUBTITLE

Interoperable ADS-B Confidentiality

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Burfeind, Brandon, C, Maj, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-20-M-009

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

AF/A3OJ Civil/Military Integration Division
Mr. James Piel, Sr Military Aviation Analyst
1480 Air Force Pentagon
Washington DC 20330-1480
james.w.piel.civ@mail.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A. Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The worldwide air traffic infrastructure is in the late stages of transition from legacy transponder systems to Automatic Dependent Surveillance - Broadcast (ADS-B) based systems. ADS-B relies on position information from GNSS and requires aircraft to transmit their identification, state, and position. ADS-B promises the availability of high-fidelity air traffic information; however, position and identification data are not secured via authentication or encryption. This lack of security for ADS-B allows non-participants to observe and collect data on both government and private flight activity. This is a proposal for a lightweight, interoperable ADS-B confidentiality protocol which uses existing format preserving encryption and an innovative unidirectional key handoff to ensure backward compatibility. Anonymity and data confidentiality are achieved selectively on a per-session basis. This research also investigates the effect of false replies unsynchronized in time (FRUIT) on the packet error ratio (PER) for Mode S transmissions. High PERs result in range and time limits being imposed on the key handoff mechanism of this proposal. Overall, this confidentiality protocol is ready for implementation, however further research is required to validate a revised key handoff mechanism.

15. SUBJECT TERMS

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

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE
U	U	U

17. LIMITATION OF ABSTRACT

UU

18. NUMBER OF PAGES

122

19a. NAME OF RESPONSIBLE PERSON

Dr. Robert F. Mills, AFIT/ENG

19b. TELEPHONE NUMBER *(include area code)*

(937) 255-3636 x4527 robert.mills@afit.edu