Comparative Analysis of ADS-B Verification Techniques

Brandon Kovell, Benjamin Mellish, Thomas Newman, Olusola Kajopaiye
brandon.kovell@colorado.edu, benjamin.mellish@colorado.edu,
thomas.newman@colorado.edu, olusola.kajopaiye@colorado.edu

A capstone paper submitted as partial fulfillment of the requirements for the degree of Masters in Interdisciplinary Telecommunications at the University of Colorado, Boulder, 4 May 2012. Project directed by Professor Timothy X. Brown.

1 Introduction

ADS-B is one of many Federal Aviation Administration (FAA) regulated technologies used to monitor air traffic with high precision, while reducing dependencies on dated and costly radar equipment [1]. The FAA hopes to decrease the separation between aircraft, reduce risk of collision as air traffic density increases, save fuel costs, and increase situational awareness of both commercial and general aviation aircraft within United States airspace.

Several aviation technology experts have expressed concern over the security of the ADS-B protocol [2] [3]. ADS-B has an open and well known data format, which is broadcast on known frequencies. This means that the protocol is highly susceptible to radio frequency (RF) attacks such as eavesdropping, jamming, and spoofing. Eavesdropping and jamming will be reviewed in Section 3.4. While eavesdropping and jamming attacks are well studied, due to their applicability in many radio technologies, spoofing attacks against ADS-B are particular to this system. As such, the latter is the focus of our research.

This paper evaluates so-called Kalman Filtering and Group Validation techniques (described below) in order to assess which would be a better position verification method of ADS-B signals. The parameters for the comparative analysis include both technical feasibility and practical implementation of each position verification technique. The goal is to offer a practical position verification process which could be implemented with limited government funding within the next 10 years.

2 Background

At any given time, there are approximately 7,000 aircraft in flight over the United States. Delays remain at historically high levels at many U.S. airports [4]. The number of aircraft and mix of aircraft types will increase over the next 20 years, significantly increasing controller workload [4]. In order to address the eventual oversubscription of the current air transportation system, Congress passed Public Law 108-176 (49 USC 40101) in 2003, which directed the Secretary of Transportation to create the Air Transportation System Joint Planning and Development Office [5]. This organization is tasked with development of the NextGen Air Transportation System. Of the capabilities to be implemented as part of NextGen, ADS-B is designated to be the first [6], with many of the follow-on capabilities dependent on its successful fielding.

2.1 Current Surveillance Technology

In its current implementation, air traffic control uses a combination radar and pilot position reporting for surveillance. The radar component consists of two distinct, but complementary systems. The first system, known as primary radar, operates in the conventional fashion, using reflected radio waves from the target [1]. This type of radar suffers from a number of limitations, including atmospheric diffraction, reflection or attenuation by dense objects, and target radar cross section. These limitations are mitigated to a certain extent through the use of Moving Tracking Indicator techniques and the Air Traffic Control Radar Beacon System (ATCRBS) along with Mode A3/C and Mode S transponders in the aircraft [1].

ATCRBS, better known as secondary surveillance radar, uses an interrogation signal, which is sent with the primary signal to induce an onboard transponder to selectively reply to a specific pulse group. These replies, which are independent of the primary radar return, are much stronger and have the capability of providing additional information, such as aircraft altitude. Some Mode S transponders, also have the capability of receiving Traffic Information Services (TIS) from the ground.

The migration to ADS-B surveillance technology is driven by two principal factors: safety and cost-effectiveness. ADS-B allows for reduced separation minimums, increasing airspace utilization. At the same time, odds of collision are greatly reduced, due to the much higher accuracy of position reports. The use of ADS-B also allows for more direct routings between points, resulting in both fuel savings and reduced carbon emissions [7].

2.2 NextGen Surveillance Technology

ADS-B consists of three distinct categories: ADS-B Out, ADS-B In, and ADS-Rebroadcast (ADS-R). ADS-B Out builds on prior surveillance technology by having each aircraft broadcast its own three-dimensional state vector (position and velocity). Unlike current transponders, these broadcasts are not sent in response to interrogations, but blindly at periodic intervals. This, in turn, is received by ground and air-based receivers. Other aircraft then use this data along with their own state vector to calculate relative range and bearing.

Information for these transmissions is obtained using a reliable position source, such as the Global Positioning System (GPS)[1]. Per current FAA regulations, by January 1, 2020 all aircraft operating within the airspace defined in 14 CFR 91.225[2] will be required to transmit the information defined in section 91.227 using ADS-B Out avionics [1]. In the United States, ADS-B Out operates on the 1090 MHz Extended Squitter (1090-ES) protocol, which is highly congested, due to its current use by ATCRBS and TCAS. As 1090-ES is the same frequency used by Mode S transponders, it provides an upgrade path to ADS-B. In addition to Mode S, aircraft owners have the option of providing ADS-B transmissions on the Universal Access

[1] As an alternative, this data can also be obtained via an Inertial Navigation System or DME-DME (Distance Measuring Equipment) in conjunction with traditional onboard instruments [32].

[2] Class A, B, and C airspace; Class E airspace within the 48 contiguous states and the District of Columbia at and above 10,000 feet MSL, excluding the airspace at and below 2,500 feet above the surface; Class E airspace at and above 3,000 feet MSL over the Gulf of Mexico from the coastline of the United States out to 12 nautical miles; and airspace around those airports identified in 14 CFR part 91, Appendix D [33].

Transceiver (UAT) frequency, which operates at 978 MHz. The UAT is a stand-alone device unlike Mode S transponders which incorporate ADS-B functionality. The advantage to using this frequency is that it is less congested and allows for additional services, such as graphical weather uploads [1].

The second category of ADS-B, ADS-B In, provides airborne surveillance capability, unlike ADS-B Out which is primarily for ground-based surveillance. This offering allows aircraft to "use position messages to monitor neighboring vehicles in airspace and airports, improving pilot situational awareness and alertness" [8]. Future use of ADS-B In will focus on autonomous spacing of aircraft. Finally, ADS-R is the rebroadcast by ground stations of an ADS-B message from one format to another when two aircraft with different data link modes are sensed in the same area. This is required since the 1090 ES and UAT ADS-B message formats are inherently different [9].

2.3 State-of-the-Art on ADS-B Security

There has been much interest in ensuring ADS-B message validity and availability. The FAA issued a final rule containing regulations on equipage requirements and performance standards for ADS-B Out avionics based on its security assessment on ADS-B based ground surveillance [10]. Any loss of ADS-B Out data in terminal areas can be compensated for by the use of primary and remaining secondary surveillance radar infrastructure. By leveraging the use of onboard traffic avoidance systems such as Traffic Collision Avoidance System (TCAS) transceivers[3] and primary ground surveillance radars, most safety-threatening situations in surveillance, such as midair collisions, can be mitigated [11]. TCAS systems interrogate corresponding transceivers of neighbor aircraft and perform vector calculations to determine collision potentials. They then provide pilot notifications and collision avoidance maneuvers if needed.

Multilateration provides an alternative way to validate the transmitted position of an aircraft. Multilateration computes a transmitter's position by measuring the difference in a transmission's arrival time at multiple receivers. By using a combination of four or more ground controllers, the 3-D position of an aircraft can be jointly verified from the signal properties (e.g. signal strength, time of arrival) received in an ADS-B message [8]. The multilateration functionality can also be separated at the ground stations, by having one station verify the time of arrival of the ADS-B communication signal and the other the ADS-B position data [12]. While the currently envisioned approach is heavily dependent on dedicated ground-based omnidirectional antennas, it is technically possible for similar functions to be performed onboard aircraft in regions with less than four ground stations through a combination of ADS-B multilateration and Kalman filter estimation of a flight's trajectory.

The inclusion of cryptographic schemes like symmetric-key-based solutions, keyed hash, and Message Authentication Codes may also play a role in securing the ADS-B communication channel between aircraft and air traffic controllers [13]. These mechanisms can protect the integrity, authenticity, and confidentiality of ADS-B Out messages, but require both air traffic

[3] TCAS II is only required on aircraft "with more than 30 seats or weighing more than 15,000 kg" [34]. This, in conjunction with the expense of the system, means that most general aviation aircraft are not equipped with TCAS.

controllers and aircraft to have a keying mechanism, which is difficult in an environment with no pre-established trust relationship.

2.4 Vulnerabilities

ADS-B surveillance data is communicated over an open and well known message protocol, creating a likely method for data spoofing attacks. An attacker is also able to block or provide false GPS signals, resulting in loss of positional accuracy, and other unexpected behavior in air traffic surveillance [8]. Attacks can be either passive or active and can be initiated from within or outside of the Air Traffic Management (ATM) system (e.g. an unauthorized ADS-B transceiver). Passive attacks include eavesdropping, where the attacker merely listens in on periodic ADS-B messages to obtain unique identifiers or position trajectory of communicating aircraft without necessarily disrupting the system. This lack of anonymity represents an invasion of aircraft owner's privacy and is usually a precursor to an active attack [14]. Conversely, active attacks are conducted with the intent of degrading or denying performance of the air traffic surveillance system. These include injecting errors in ADS-B data during transmission that may trigger false alarms or misleading interpretations, transmitting false or manipulated messages with incorrect locations, and spoofing location information and identifiers. Loss of ADS-B data at the receivers due to RF jamming, may trigger air traffic management systems sensing an ADS-B failure to fallback or degrade to backup systems of lower performance and capacity [8].

These kinds of attacks affect air traffic information resources and can result in flight route conflicts due to the broadcast of false ADS-B aircraft positioning and intent [3]. In addition, surveillance accuracy and/or performance gain of Air Traffic Management systems may be degraded. ADS-B is also more vulnerable to attacks because it operates on a lower signal power level than radars, hence an attacker can transmit at a higher power level to overwhelm ADS-B systems [15]. This opens up some inherent safety concerns for passengers and operators alike, regarding the integrity and availability of such critical flight data in the National Airspace System (NAS). If not well secured with adequate ADS-B data verification techniques, the performance and accuracy of ATM systems could be dangerously degraded.

Finally it must be noted that a non-standard method for UAT-only ADS-B ranging is theoretically possible as shown in [9] . Each UAT ADS-B message is broadcast at a specific Message Start Opportunity (MSO) and part of the data payload is the time the message began to transmit. By comparing the message start time with the time of receipt the receiving equipment can calculate a range to the transmitter and validate the range to the ADS-B position. The main limitations of this are that it is not currently put in to practice and is still under investigation by the FAA and ICAO [9] [16]. As well, it only determines the range to the target and is inherently reliant on a common UTC time source (such as GPS) which not all aircraft may have [16]. Finally, this method is still vulnerable to spoofing if someone includes an MSO in the message consistent with the spoofed range.

3 Proposed Mitigation Methods

3.1 Kalman Filtering

The Kalman filter is based upon Bayesian inference. Bayesian inference is a process to make educated guesses about future data based on historical information. The Kalman filter is a simple

linear variant of the Bayesian filter which can be used for location estimation based upon historical location information [17].

In 2000, a proof of concept was conducted in Alaska that used Kalman filtering in conjunction with ADS-B to provide radar-like services [18]. In 2004, a Kalman filter was used in a dependent data driven approach to not only filter and smooth ADS-B message data, but also attempt to calculate state and intent estimations [19]. In 2005 signal conformance was added as an early variation on multilateration. It should be noted that Kalman filters are critical to the multilateration process since the transponder signal distance estimates are inherently noisy. The State Vector and Trajectory Change ADS-B reports are the two primary reports used for data filtering, intent estimation, and signal conformance.

Both STARS (Raytheon Standard Terminal Automation Replacement System) and CARTS (Lockheed Martin's Common Automated Radar Terminal System) use Kalman filters. These filters use data from radar, ADS-B, and multilateration to develop a single track. This is often referred to as data fusion. Lockheed's older CARTS system is currently in the process of being replaced by the STARS system. STARS is currently being used at Philadelphia International Airport, and is on contract for 11 more sites [20]. The extensive use of Kalman filters in ground systems forces us to distinguish between Kalman filtering of the general position of an aircraft received in ADS-B messages, Kalman filtering of the signal strength and direction on the antenna, and our proposed use of Kalman filtering onboard aircraft for real time positional verification.

3.2 Group Validation

One of the best known ways to verify the position of an unknown node in a network is via multilateration, which relies on time difference of arrival calculations from a commonly received signal at four or more known locations (for position calculations that include altitude). This concept can be theoretically applied to any network of nodes broadcasting a receivable signal. Aircraft in flight distant from the earth's surface have a beneficial feature in that they have a greatly increased line of sight range of each other and can share information via a three dimensional Mobile Area Network (MANET).

Sampigethaya et al. in [21] have proposed a useful method based on the above principles to verify the broadcast ADS-B position of an aircraft. They propose to use a technique called Group Validation (GV) where aircraft traveling in a common general direction form group network, led by a group leader. The basic operation of this network is described below:

> *When an ADS-B signal from an aircraft P is received by three (four) or more aircraft, {V}={V1, V2, V3}, then {V} can use time-difference-of-arrival technique to estimate the 2-D (3-D) position of P [sic]. In this technique, {V} must share the times they received the signal from P, compute the differences between times, and then perform multilateration computations to estimate actual position of P… Therefore, if four or more verifiers can communicate the time instances at which they received ADS-B signal of P, they can independently estimate P's actual position and verify claimed position in ADS-B message of P [3].*

Sampigethaya et al. proposes to use an Internet Protocol-based airborne network in order to share the needed information [21]. This method appears to have great potential; however it relies on several basic assumptions. One of the key features of this paper is to analyze the validity of these assumptions as would be required to implement the GV process in the NAS.

The feasibility of the GV concept will be the basis for comparison of this technique with Kalman Filtering as ways to validate broadcast ADS-B position.

4 Analysis

4.1 Kalman Filtering Analysis

Kalman filters are currently used by a variety of FAA mandated systems for positional verification. On the ground, data is filtered, averaged and fused from multiple sources in order to present air traffic controllers with accurate aircraft positional data. Airborne GPS systems also use Kalman filters to smooth noisy GPS data and provide more accurate positional data to onboard navigational equipment. The proposed use of a Kalman filter for positional verification would be a hybrid of these two systems, providing state estimation in a real time airborne scenario using the existing State Vector (SV) and Trajectory Change (TC) ADS-B reports.

Aircraft position verification using Kalman Filters has already been successfully implemented in ground based scenarios where aircraft can be tracked continuously between ground stations providing accurate long term position trending. Complexities arise for a strictly airborne approach where long term historical tracking information may not be available. This requires a restriction on the use of strictly airborne Kalman filtering techniques to aircraft on common trajectories within at least 90 nautical miles of each other [22]. Analysis of the valid range holds true for both Kalman and Group Validation methods, and is a physical limitation of the air-to-air capabilities of the Mode S transponder.

A standard Kalman filter needs only two valid State Vector (SV) reports to set up a valid location hypothesis, assuming a relatively accurate covariance matrix is known. SV reports can be ideally broadcast at about two per second [23], so rough initial collision detection can be established within a second of an aircraft coming into transceiver range. Broadcast rate and range is highly dependent upon congestion of the 1090 MHz band. As air traffic using this frequency increases, position validation will become slower. Providing an intent solution based upon Trajectory Change (TC) reports would take longer to establish due to complexities involving the turn radius. This would cause the threshold time until a strictly air-to-air solution of combined SV/TC reports to increase drastically from the pure SV report solution. Future work will include determining the threshold time until a combined SV/TC report solution can be trusted. This threshold value will need to be established in order to avoid wrongly alerting pilots to a suspected deviant aircraft, also known as creating false positives.

The Kalman Filtering validation method can be easily defeated using what is known as a Frog Boiling attack [24]. The Frog Boiling attack is executed by first sniffing the correctly reported solution of an aircraft then rebroadcasting the modified solution at a slightly higher power than the received solution. This attack is equivalent to jamming the original signal and using your own signal in its place, and is sometimes called broadcast signal intrusion or signal hijacking. If the attackers modified solution is drifted away from the aircrafts initial intent slowly enough, the Kalman filter will simply adjust to the changes in direction and accept the spoofed information. This can be done for one or many aircraft within the range of an attacker. This type of an attack can be extremely disruptive, especially near airports where small changes in reported aircraft separation can demand both pilot and air traffic control attention.

The verification of ADS-B involves using Kalman Filtering in order to sort out noisy or missing ADS-B Trajectory State (TS) reports in order to estimate the aircraft's state. Once a state estimate has been established, it is possible to use the ADS-B Trajectory Change (TC) report to

actually validate the aircraft position. Kalman Filtering analysis could be combined with aircraft flight models to help identify inconsistent flight parameters with the type of aircraft transmitted in the ADS-B signal. For example, airlines will seldom (if ever) make a 2G turn and often can't fly at very low airspeeds except for takeoff and landing. While Kalman Filtering is still vulnerable to spoofing it retains potential because, as shown, the algorithm can be made to distinguish very precise features of a flight path. In this respect it makes Kalman Filtering useful in discriminating ADS-B signal data that are not 100% consistent with a physically possible and probable flight paths. When a discrepancy is identified the pilot can be notified by an annunciation. This method is particularly practical as it utilizes unique ways to analyze information that is already coming in to the aircraft.

4.2 Group Validation Analysis

There are many radio frequency methods which could be used to share data required for aircraft verification; one possible method is wireless IP. The Future Communications Study (FCS) is an ICAO requested joint study between the FAA/NASA and EUROCONTROL in order to identify the future data link technology and systems for ATM. The FCS has identified the IP based L-Band Digital Aeronautical Communication System (L-DACS) as the primary candidate [25]. At the current time two versions of L-DACS are undergoing spectrum interference testing, L-DACS 1 and L-DACS 2. One of these systems will be picked by ICAO as the ATM datalink communication system to be enabled for operational use by 2020 [25]. Both of the systems have design potential for IP based air-to-air aircraft communication. Sampigethaya et. al. in [21] identified L-DACS as a possible link solution for GV, however it may not be practical for widespread future use.

The FCS [26] document COCR Version 2.0 uses ATM operating requirements and predicted future "airline operating concepts" as a guide to, "determine candidate data communications technologies –existing or future – that can meet these requirements." COCRv2 has identified limited uses for air-to-air data links in the future. Air-to-air functionality is a possible feature of both L-DACS systems however the purpose of the FCS is developing the Air-to-Ground portion of future ATM [27]. Because of this there is limited current interest in the use of air-to-air mobile communication as supported by L-DACs. There are four predicted air-to-air communication services envisioned by COCRv2. Gräupl highlights in [28] that only one type of addressed communication is identified as an actual requirement for longer term use, and that is after 2020 when the first phase of the digital ATM transformation will be complete. L-DACS will be a very capable IP data link system. However, there is limited interest and near term need to develop detailed specifications and design standards to make L-DACS air-to-air data links a reality. This leaves the message protocol for GV in question which must be examined further.

The central vulnerability of GV which must be addressed is the validity of the data coming from validating aircraft. How does the group leader decide that the aircraft providing the signal information isn't a spoof itself? An adversary could theoretically not only spoof a single Target of Concern (TOC), but also spoof the signals coming from other aircraft used to validate the TOC. An adversary could fake the required validation signals by calculating and broadcasting the supposed time of arrival and message characteristics consistent with the spoofed signal. One could also spoof many targets such that the processing capability of the equipment is stressed or the pilot losses faith in the validity of the equipment and displays. Ground stations have the benefit that, unless the spoofing signal is near the receiver, they will not get the same spoofed signal an aircraft would. A ground station would only receive a signal if it is relatively

close, because the radio horizon at ground level is rather short for high frequency signals such as these. This fact could be used, through communication with ATC, to identify spoofed signals by comparison with ground receivers.

Several topics related to the complexity, maturity, and practicalities of the GV method highlight its benefits and limitations. Defining interoperable, global aviation telecommunication standards and equipment no doubt takes years and faces significant legal, economic, technical, and diplomatic hurdles. Also, the message standards and processes for forming, merging, and disbanding Groups have yet to be defined on a specific and technical level. For this to work every aircraft operating in the group would have to be equipped with L-DACS equipment and radios. Airlines can reasonably be expected to implement any newly required technology. However, much of general aviation operates at lower altitude over smaller distances and has less of a need for datalink functions. Ultimately L-DACS is not a near term solution, nor could it realistically be used by all aircraft.

One of the little studied practical aspects of airborne ad-hoc MANETS is the dynamics of changing link topology and node availability. Forming MANETS is especially applicable to airlines that often follow densely used, common air routes between hubs (airports) in their network [8]. This means certain air routes between some airports are heavily traveled and the routes between other airports are rather sparse. As such GV may not be universally useful as there may not always be enough aircraft in the correct range and geometry to form a group.

This suggests the significant question, how often will the necessary geometry for GV exist? What types of air traffic and airspace benefit from GV? The risk of a hazardous situation from a spoofed signal could be presented anywhere, therefore any mitigation steps must be effective anywhere as well. To explore this issue, actual air traffic surveillance data obtained from FlyteComm Inc. [29] was obtained[4] in order to analyze the geometrical distribution of aircraft. Sampigethaya et al. in [8] makes a general statistical analysis of the availability of aircraft for the GV method. Figure 4 (c) in [8] shows that for an aircraft transmission range of 50 nm there is a 100% probability of 4 aircraft being within range of each other [8]. For reference, the FAA describes ADS-B as having a 200 NM nominal reception range [30]. It is important to remember that this is really the theoretical maximum line-of-sight range. Sampigethaya et al. in [8] describes the range of 100 miles or more as do many ADS-B manufacturers [31]. Finally the ICAO standard for Class 3A ADS-B equipment, the most capable, calls for a range of 120 NM or more [9]. Therefore a realistic minimum value of 120 NM direct air-to-air communication range is most applicable.

A specially designed Python program was used to analyze the data and determine what percentage of airborne aircraft can directly communicate with four or more other aircraft. The program iterates through the FlyteComm position data making numerous distance calculations. It compiles data in to groups of aircraft whose position can be validated by four or more validators. This represents, under the best circumstances, the maximum percentage of airborne aircraft which can use the GV process. For this to be true the antenna location and the validating aircraft must exist in the volume of space defined by the intersection of four spheres (the validating aircraft communication range) in order to use one hop communication. In the data analyzed the aircraft (or antenna) with at least four others in sight could be triangulated but the

[4] Data is a snapshot of IFR traffic taken at 1845Z on 27 Mar 12 for the United States.

validating aircraft may be out of range of the other aircraft needed to validate the signal. To solve this, a multi-hop routing system would be needed, or the minimum aircraft would need to be close enough to communicate with each other directly. However, multi-hop routing would be more complicated and would increase the vulnerability of intercepting or manipulating the data. The findings show it is not possible for all airborne aircraft to use the GV process. At 120 NM the NAS could theoretically have 91% utilization of the GV concept as shown in Fig. 1. Another problem which may exist is one caused by an overabundance of aircraft which may induce problems due to excessively large group sizes. At 120 NM on average number 84 aircraft connections exist with each aircraft that can communicate with at least four others. Problems arise because of limited processing capability and channel congestion if an aircraft made a group with as many as possible.

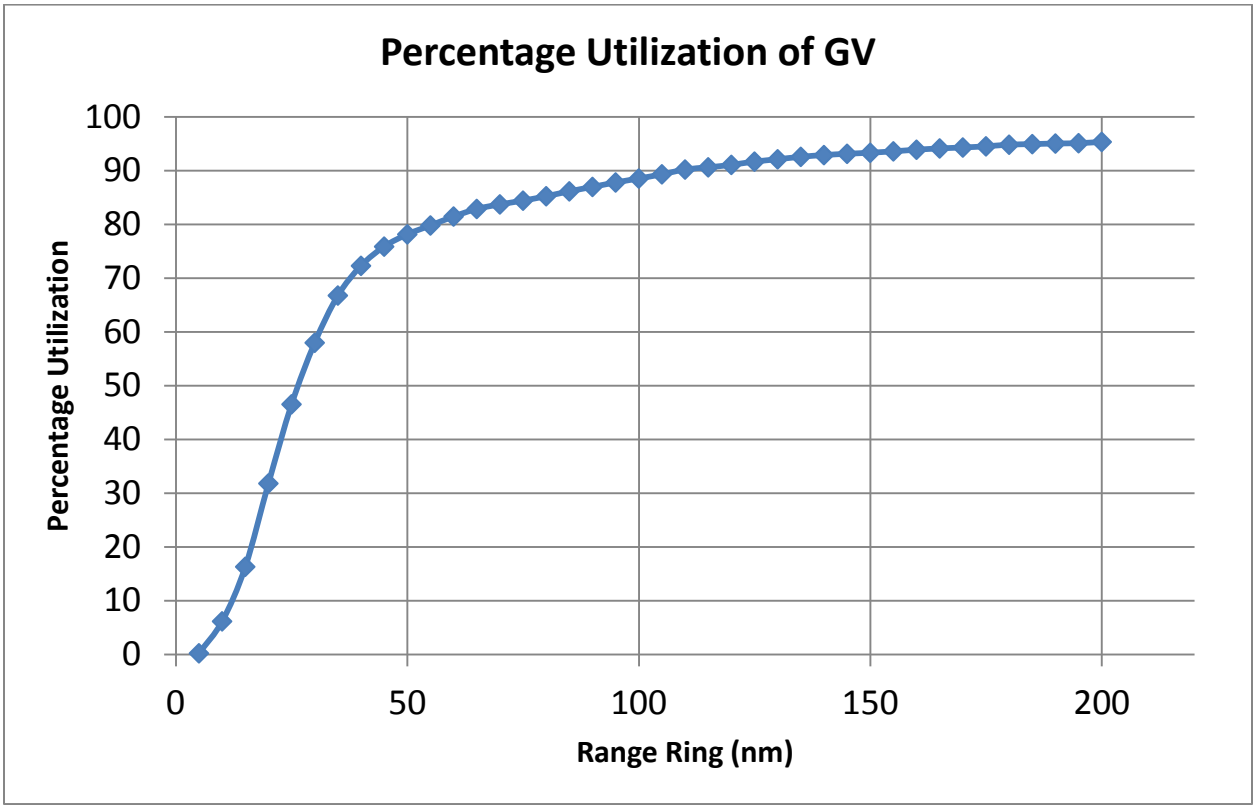

Figure 1: Percentage Utilization of GV at 1845Z on 27 Mar 12 for the United States

5 Conclusions

This analysis highlights the limitations of the airborne ad-hoc MANETS due to the vast differences in air traffic density across the United States. There are certain portions of airspace that, due to their geographic location and low traffic volume are unsuitable for GV. With these exceptions, commonly useable reception ranges of aircraft will allow for GV most of the time. L-DACS is a possible means for a GV data link, but not in the near term nor is it practical to all aircraft (primarily just commercial aircraft).

The primary strength of the Kalman Filter method when compared against the Group Validation method is that no additional messages need to be made in order for it to function. Therefore positional validation can take place in existing TCAS equipment. However, TCAS only being required on large aircraft (as well system cost), limits its use in the general aviation market. Yet, in relative terms, this would yield a highly reduced cost when compared with Group Validation, which would require both new messages and most likely new avionics hardware. These advantages need to be weighed against the ease of spoofing and defeating the Kalman filter validation, especially on a short term basis.

Keeping these considerations in mind it appears that implementing both solutions in a complimentary manner is the most viable near term solution. The FAA should investigate the specific equipment changes and economic concerns required to incorporate a Kalman filter validation and pilot notification function in new TCAS equipment. TCAS would be the natural choice equipment to incorporate the processing since the TCAS position broadcasts can serve as a possible historical point from which to start the filtering. Due to the interrogation/reply function of TCAS it would appear more difficult to spoof. As part of this the TCAS equipment must continue to interrogate airborne aircraft in order to cross check the ADS-B position. As well, a way to validate ADS-R broadcasts would also be needed (possibly using an interrogation/reply scheme for the ground transmitter). This new processor feature would serve as the spoofing detection method for aircraft with Mode-S. In a complimentary way ADS-B UAT could be used for GV for general aviation aircraft. The FAA should create a working group to investigate equipment specifications (a new TSO) for GV, new UAT Downlink/Uplink message formats, and the modifications required for ADS-B ground station software and network functions. Assuming ADS-B message formats can be created then the GV feature could be required in new UAT equipment. By incorporating these functions in only new equipment the FAA can successfully field a solution in a gradual and cost effective manner for aircraft owners commensurate with the threat.

More specific proposed future work will be calculating a threshold time until a solution could be trusted based upon Trajectory Change reports in order to avoid false positives when using Kalman Filters. If the FAA does specify new message formats and TSOs for use in the NAS it could use that as an opportunity to incorporate other security mitigation steps; such as some form of encryption to address ADS-B message anonymity (eavesdropping). As well, the FAA should continue to investigate range validation of UAT messages as a partial solution.

References

[1] Federal Aviation Administration, *Aeronautical Information Manual,* Washington: Government Printing Office, 2012.

[2] J. Krozel, et al., "Aircraft ADS-B Data Integrity Check," in *AIAA Aircraft Tech., Integration, and Operations Conf.*, Chicago, 2004.

[3] K. Sampigethava, et al., "Future e-enabled aircraft communications and security: the next 20 years and beyond," *Proc. of the IEEE,* vol. 99, no. 11, pp. 2040-2055, November 2011.

[4] Federal Aviation Administration, *FAA Aerospace Forecast - Fiscal Years 2012-2032,* Washington: Government Printing Office, 2012.

[5] US Government, *Public Law 108-176, Title VII, Section 709,* Washington: Government Printing Office, 2003.

[6] A. L. Mozdzanowska, et al., "Dynamics of Air Transportation System Transition and Implications for ADS-B Equipage," in *7th AIAA Aviation Technology, Integration and Operations Conference*

(ATIO), Belfast, 2007.

[7] G. Wright, "NAV CANADA implements ADS-B," in *Integrated Commun., Navigation and Surveillance Conf.*, Arlington, 2009.

[8] K. Sampigethaya and R. Poovendran, "Visualization & assessment of ADS-B security for green ATM," in *Digital Avionics Syst. Conference*, Salt Lake City, 2010.

[9] ICAO, *Manual on the Universal Access Transceiver (UAT): Doc 9861,* Quebec: ICAO, 2010.

[10] US Government, *Federal Aviation Regulations, 14 CFR 91.227,* Washington: Government Printing Office, 2010.

[11] RTCA Special Committee 219, *Terms of reference,* Washington, 2008.

[12] M. Sharples, et al., "Integrity and security of ADS-B," in *SurTech Proceedings*, 2004.

[13] E. Valovage and D. Hall, "Enhanced ADS-B research," in *IEEE Aerospace Conf.*, Big Sky, 2006.

[14] K. Sampigethava and R. Pooverndran, "Privacy of future air traffic management broadcasts," *IEEE Digital Avionics Syst. Conf.*, pp. 6.A.1-1-6.A.1-11 , October 2009.

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

[16] M. Teshome, "Preliminary Analysis of Automatic Dependent Surveillance - Broadcast (ADS-B) Independent Validation Techniques," in *ICNS 2007 Conference*, Herndon, 2007.

[17] D. Fox, et al., "Bayesian Filtering for Location Estimation," *Pervasive Computing*, pp. 24-33, July 2003.

[18] Federal Aviation Administration, *Capstone ADS-B Evaluation Report*, 2000.

[19] D. Andrisani, et al., "Aircraft ADS-B Data Integrity Check," in *AIAA Aircraft Technology, Integation, and Operations Conference*, Chicago, 2004.

[20] A. Schofield, "New ATC System for Key FAA TRACONs," *Aviation Week*, 10 March 2011.

[21] K. Sampigethaya, et al., "Assessment and Mitigation of Cyber Exploits in Future Aircraft Surveillance," in *IEEE Aerospace Conf.*, Seattle, WA, 2010.

[22] RTCA, *DO-260A Minimum Operational Performance Standards for 1090 MHz Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services (TIS-B),* FAA, 2003.

[23] European Organisation for the Safety of Air Navigation, "ADS-B for Dummies," Eurocontrol/CASCADE, [Online]. Available: www.ssd.dhmi.gov.tr/getBinaryFile.aspx?Type=3&dosyaID=123. [Accessed 22 03 2012].

[24] E. Chan-Tin, et al., "The Frog-Boiling Attack: Limitations of Secure Network Coordinate Systems," in *SecureComm*, 2009.

[25] EUROCONTROL, "L-Band Continental System," EUROCONTROL, 2009 November 2009. [Online]. Available: http://www.eurocontrol.int/communications/public/standard_page/LDACS.html. [Accessed 25 March 2012].

[26] Eurocontrol, *Action plan 17: future communications study,* Brussels, Belgium: Eurocontrol, 2007.

[27] M. Sajatovi, et al., "L-DACS 1 System Definition Proposal: Deliverable 3-Design Specifications for L-DACS 1 Prototype," Brussels, Belgium, 2007.

[28] T. Gräupl, *L-DACS1 air-to-air data-link protocol design and performance,* Salzburg, Austria: Univ. of Salzburg, 2011., pp. B3-2.

[29] J. Bunker, Interviewee, *FlyteComm Traffic Data.* [Interview]. 28 March 2012.

[30] Federal Aviation Administration, *Air Traffic Bulletin: Issue #2005-3,* Washington D.C.: Federal Aviation Administration, 2005.

[31] "Sensis to deliver ADS-B ground station with range greater than 100 miles at Louisville Airport, KY," Saab Sensis Corporation, [Online]. Available: http://www.saabsensis.com/docs/107/. [Accessed 2 April 2012].

[32] E. A. Lester and R. J. Hansman, "Benefits and incentives for ADS-B equippage in the National Airspace System," MIT International Center for Air Transportation, Cambridge, 2007.

[33] US Government, *Federal Aviation Regulations, 14 CFR 91.225,* Washington: Government Printing Office, 2010.

[34] J. S. Searight, "TCAS Home Page," Federal Aviation Administration, 4 August 2010. [Online]. Available: http://adsb.tc.faa.gov/TCAS.htm. [Accessed 5 April 2012].