VERIFYING ADS-B NAVIGATION INFORMATION THROUGH DOPPLER SHIFT MEASUREMENTS

Nirnimesh Ghose and Loukas Lazos
Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, Arizona

Abstract

Recent efforts to modernize aviation traffic control have mandated the gradual replacement of the existing analogue radar system with a next-generation (NextGen) digital one. Part of this NextGen system is the Automatic Dependent Surveillance-Broadcast (ADS-B) standard. ADS-B aims at improving aviation safety by enabling aircraft broadcast navigation information. However, the current ADS-B standard does not provide mechanisms for verifying the integrity of navigation broadcasts. Consequently, *aircraft trajectories can be easily spoofed*.

In this paper, we address the problem of verifying the navigation information of ADS-B transmissions. Fundamentally, this is a classical message integrity problem that can be addressed with cryptographic methods. However, cryptographic primitives are not part of ADS-B, primarily due to standardization and key management challenges. To address the shortcomings of ADS-B, we propose a PHY-layer verification method that exploits RF attributes of ADS-B transmissions to verify the aircraft's velocity and position. Specifically, we exploit the short coherence time of the wireless channel and the Doppler spread phenomenon to detect spoofed ADS-B messages broadcasted by a rogue ground station. We show that the security offered by our verification method is equivalent to the hardness of underdefined quadratic equation systems, which are used in public-key cryptography.

Introduction

The International Air Transport Association has forecasted that over 3.6 billion passengers will use air transport annually by 2016 [1]. To cope with the anticipated increase in air traffic, the relevant governing bodies around the world have agreed to a novel air traffic control technology that shifts traffic surveillance from the uncooperative and independent radar system to a cooperative and dependent digital one. At the heart of this new technology lies the Automatic Dependent Surveillance Broadcast (ADS-B) standard [2]. In ADS-B, aircrafts independently determine their navigation information (location, air speed, heading, etc.) using onboard satellite equipment (GPS) [3]. To facilitate air traffic management, this navigation information is broadcasted to nearby aircrafts and ground air traffic control (ATC) centers.

ADS-B is expected to significantly reduce the cost of traffic control, as radar systems are expensive to deploy and maintain. Moreover, it will improve aviation safety by delivering fine-grained navigation information in a timely fashion. Due to its profound advantages, many aviation carriers have already introduced ADS-B equipment into their air fleet [4]–[7]. Despite its critical function, ADS-B does not integrate strong security mechanisms. The aircraft's location is verified by ground stations using a multilateration technique. In this technique, three or more ground stations compute the time difference of arrival from an ADS-B broadcast to validate the claimed aircraft's position [3]. However, an aircraft has no way of verifying the ADS-B broadcast of another aircraft.

Researchers have highlighted and even implemented numerous attacks that can be launched with COTS equipment and rudimentary knowledge [3], [8]–[12]. Costin et al. [3] have experimentally demonstrated the feasibility of replay/injection attacks on the ADS-B using USRPs and COTS equipment. Sampigethaya et al. [10] have enumerated various threats in ADS-B such as eavesdropping, radio-frequency jamming, aircraft impersonation, active manipulation of data, etc. In fact, none of the fundamental security properties, namely source authentication, data integrity, data confidentiality and resistance to jamming can be guaranteed under the present standard. Consequently, ADS-B transmissions can be eavesdropped, spoofed, replayed, modified, deleted, and jammed [3], [8], [9], [12].

The ADS-B security vulnerabilities can be abstracted to classical cryptography problems for which solutions are readily available [12]. These solutions require the introduction of cryptographic primitives. However, implementing cryptographic solutions at a global scale requires coordination between multiple governing agencies, administrators and operators. Key management operations including key establishment, key refresh, key revocation, certificate management, etc. introduce a substantial layer of complexity and cost to the ADS-B standard [13]. Moreover, any recommended changes to the current ADS-B standards, require extensive retrofitting and upgrade efforts for the already deployed ADS-B equipment. Such changes involve universal software updates for introducing security modules or even hardware updated if the deployed solutions require secure hardware.

To cope with these challenges, we examine non-cryptographic solutions for verifying the navigation information broadcasted in ADS-B. We make the following contributions.

Our Contributions: We address the problem of verifying the integrity of ADS-B navigation information *without modifying the ADS-B standard.* We develop a PHY-layer based method for verifying the aircraft position and velocity advertised in unencrypted ADS-B frames, by exploiting the Doppler spread phenomenon. We show that a malicious ground station cannot spoof a “ghost" aircraft by transmitting ADS-B frames containing rogue navigation vectors. Defeating our verification method is equivalent to forging signatures in unbalanced oil and vinegar signature schemes [14].

Paper Organization: Section 3 gives a brief overview of ADS-B architecture. In Section 4, we state the problem. The method for verifying the integrity of aircraft velocity and position is presented in Section 5. In Section 6, we evaluate our method via simulations. Related work is described in Section 7 and in Section 8, we conclude.

ADS-B Architecture Overview

The ADS-B standard regulates the exchange of broadcast messages between aircrafts and ATC ground stations. An entity can operate as a transmitter, referred to as ADS-B OUT, or as a receiver, referred to as ADS-B IN (see Fig. 1). At the PHY layer, periodic navigation broadcasts are transmitted using either the 978 MHz Universal Access Transceiver (UAT) data link or the 1090 MHz Extended Squitter (1090ES) data link [15]. The suggested range for ADS-B transmissions reaches the 90 nautical miles for aircraft-to-aircraft communication and 150 nautical miles for aircraft-to-ATC communication [15]. It is suggested that ADS-B frames are transmitted every 0.5 sec.

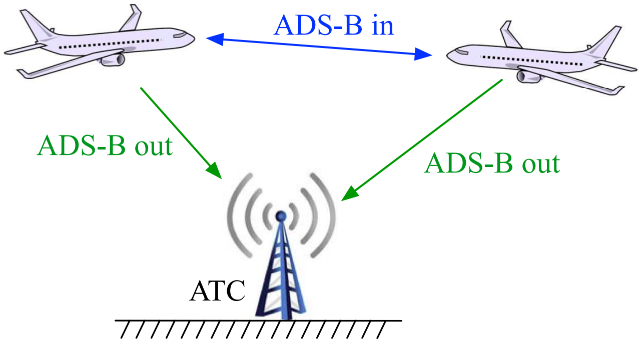


Figure 1. The ADS-B Architecture

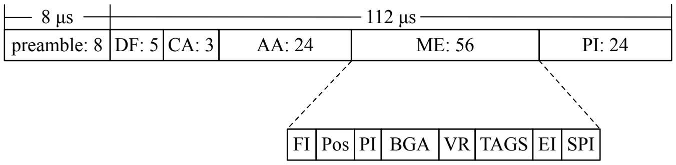


Figure 2. The ADS-B Frame Format

ADS-B frames are modulated with pulse-position modulation (PPM), with a pulse length of 1μs. Therefore, ADS-B achieves a data rate of 1 Mbps. ADS-B frames consist of an 8.0μs long preamble used for frame synchronization and a 56/112 bit payload. The various fields of the payload are shown in Fig. 2. DF refers to the downlink format used to encode broadcast messages. CA indicates if capability 17 is set for 1090ES. The AA field contains the 24-bit globally unique ICAO aircraft address. The aircraft navigation information is contained within the 56 bit-long ME field. Finally, the last 24 bits contain a CRC for detecting and correcting errors.

The ME field consists of the following subfields: (a) flight identification (flight number call sign)(FI), (c) position (latitude/longitude)(POS), (d) position integrity/accuracy (GPS horizontal protection limit)(PI), (e) barometric and geometric altitudes (BGA), (f) vertical rate (rate of climb/descent) (VR), (g) track angle

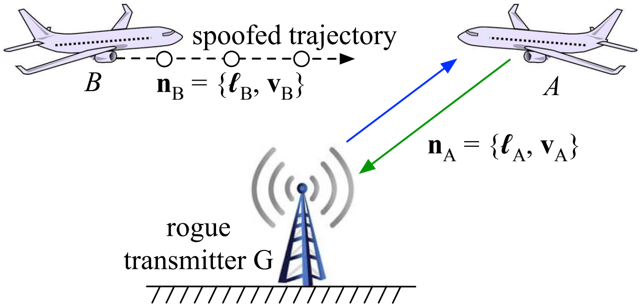

spoofed trajectory
B
$\mathbf{n}_B = \{\boldsymbol{\ell}_B, \mathbf{v}_B\}$
A
$\mathbf{n}_A = \{\boldsymbol{\ell}_A, \mathbf{v}_A\}$
rogue
transmitter G

Figure 3. Spoofing Aircraft *B* at *A* by Transmitting ADS-B Messages From *G*

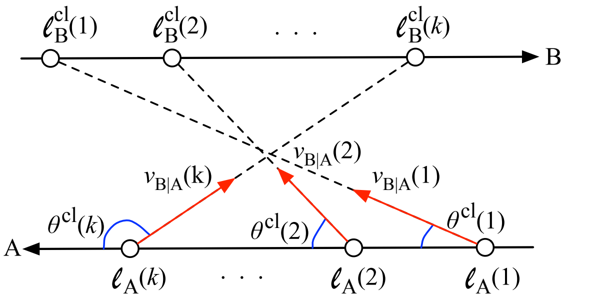


Figure 4. Position and Relative Radial Velocity at *k* Distinct Locations

and ground speed (velocity), (TAGS) (h) emergency indication when the emergency code is selected (EI), and (i) special position identification when IDENT is selected (SPI).

Problem Statement and Assumptions

We consider the scenario depicted in Fig. 3. An aircraft A with navigation information $\mathbf{n}_A$=$\{\ell_A, \mathbf{v}_A\}$ is within the range of a rogue ground station G. For simplicity, the navigation information of A contained in the ME field of an ADS-B frame is abstracted to a position vector ℓ_A with Cartesian coordinates $\{x_A, y_A, z_A\}$ and a velocity vector $\mathbf{v}_A$. The rogue ground station attempts to spoof the existence of a ghost aircraft B with navigation information $\mathbf{n}_B^{cl}$, by transmitting a crafted ADS-B compliant signal from a static location[1] ℓ_G. Spoofing of B is targeted specifically at A, whose navigation information is known at G. We address the problem of enabling A, who acts as the *verifier*, to reject the $\mathbf{n}_B^{cl}$ transmitted by G, who acts as the *prover*. We only consider solutions that do not require modifications to the ADS-B standard. As a result, cryptographic mechanisms that verify source authenticity and message integrity cannot be employed. Such mechanisms would require the re-standardization of the ADS-B protocol, costly redeployment efforts, and the establishment of a worldwide key management system.

Velocity and Position Verification

In this section, we propose a verification method for validating the velocity and position claims included in ADS-B frames. The central idea of our method is to exploit the Doppler spread phenomenon for measuring the relative radial velocity between the verifier and the prover. We show that it is difficult to manipulate the maximum Doppler spread measurements performed by the verifier. Using the relative radial velocity, a verifier aircraft A can check both the velocity and position claims of a prover aircraft B, which are connected through well-defined kinematic equations. Fig. 4 shows the relationship of the position and relative radial velocity between two aircrafts A and B at k distinct locations. Specifically, let the magnitude of the relative radial velocity $|\mathbf{v}_{B|A}|$ between A and B be:

$$|\mathbf{v}_{B|A}| = |\mathbf{v}_A - \mathbf{v}_B| \cos\theta, \tag{1}$$

where $|\mathbf{x}|$ is the magnitude of vector $\mathbf{x}$, and

$$\cos\theta = \frac{\ell_A \cdot \ell_B}{|\ell_A||\ell_B|}, \tag{2}$$

is the angle of the line connecting A and B. The maximum Doppler spread ω_D measured at A is proportional to $|\mathbf{v}_{B|A}|$.

$$\omega_D = \frac{2\pi|\mathbf{v}_{B|A}| f_c}{c}, \tag{3}$$

where f_c is the carrier frequency and c is the signal propagation speed. Hence, given f_c, c, ℓ_A, ℓ_B, and $\mathbf{v}_A$, estimating $\mathbf{v}_B$ is equivalent to estimating ω_D. Doppler spread estimation has been extensively used in wireless communications for improving functions at the PHY layer (adaptive coding, modulation, antenna diversity, power control, handoff [16]–[18]).

A. Maximum Doppler Spread Estimation

Several methods have been proposed for estimating the maximum Doppler spread [19]–[21]. For our

[1] We do not consider possible spoofing attacks from airborne adversaries.

purposes, we have selected the method proposed by Tepedelenlioğlu et al. [21] because (a) it is shown to be more accurate for high-velocity vehicles, (b) it is robust to additive white noise, and (c) it relies on channel measurements that are difficult to manipulate and predict. We briefly describe the estimator in [21], which uses the I/Q components of the channel response $h(t)$ to measure ω_D through

$$\omega_D = \sqrt{\frac{-2r_h''(0)}{r_h(0)}}, \qquad (4)$$

where $r_h(\tau) = E[h(t) * h(t+\tau)]$ is the autocorrelation function for the channel $h(t)$ and $r_h''(0)$ is the second derivative of r_h at zero. These values are obtained by the following steps.

Step 1: Compute $M+1$ channel correlation estimates

$$\{\hat{r}_h(iT)\}_{i=0}^{M}, \qquad (5)$$

by sample averaging the channel $h(t)$ with a sampling period T. That is,

$$\begin{aligned} \hat{r}_h(iT) &= \frac{\sum_j h(jT)h((j+i)T)}{\alpha N_s - i}, \\ & \quad j = 0, \ldots, (\alpha N_s - i) \end{aligned} \qquad (6)$$

The channel samples $h(jT)$ are computed by sampling N_s symbols of a known signal (e.g., frame preamble). The value $\alpha = \frac{T_s}{T}$ denotes the number of samples collected per sampled symbol, when the symbol duration is T_s. Note that the values of M and T are selected such that $MT << 1$.

Step 2: Compute matrix

$$A = (L^T L)^{-1} L^T R_H, \qquad (7)$$

where

$$A = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix}, \quad L = \begin{bmatrix} 0^0 & 0^1 & 0^2 \\ 1^0 & 1^1 & 1^2 \\ \vdots & \vdots & \vdots \\ M^0 & M^1 & M^2 \end{bmatrix},$$

$$R_H = \begin{bmatrix} \hat{r}_h(0) \\ \hat{r}_h(T) \\ \vdots \\ \hat{r}_h(MT) \end{bmatrix}.$$

Step 3: Estimate $r_h(0)$ and $r_h''(0)$ from:

$$\left\{ r_h^{(n)}(0) = n! a_n / T^n \right\}, \quad n = 0, 2, \qquad (8)$$

where a_0 and a_2 are obtained from Step 2.

Step 4: Substitute $r_h''(0)$ and $r_h(0)$ in (4) to estimate ω_D.

B. Verification Process

Using the estimated ω_D, the verifier A computes the magnitude of its relative radial velocity to the prover B. The relative radial velocity is used to verify the claims of the prover. The verification steps executed by A are as follows.

Step 1: Verifier A receives k ADS-B frames from prover B and records the claimed positions and velocities included in the payload:

$$\mathscr{L}_B^{cl} = \{\ell_B^{cl}(1), \ell_B^{cl}(2), \ldots, \ell_B^{cl}(k)\}. \qquad (9)$$

$$\mathscr{V}_B^{cl} = \{\mathbf{v}_B^{cl}(1), \mathbf{v}_B^{cl}(2), \ldots, \mathbf{v}_B^{cl}(k)\}. \qquad (10)$$

Step 2: For all claimed positions, the verifier A calculates the claimed headings Θ^{cl}:

$$\Theta^{cl} = \{\theta^{cl}(1), \theta^{cl}(2), \ldots, \theta^{cl}(k)\}, \qquad (11)$$

$$\theta^{cl}(i) = \cos^{-1} \frac{\ell_A(i) \cdot \ell_B^{cl}(i)}{|\ell_A(i)||\ell_B^{cl}(i)|}. \qquad (12)$$

Step 3: The verifier A estimates $\mathscr{V}_{B|A}^{est}$ for all received k frames using the maximum Doppler spread estimation method.

$$\mathscr{V}_{B|A}^{est} = \{|\mathbf{v}_{B|A}^{est}(1)|, |\mathbf{v}_{B|A}^{est}(2)|, \ldots, |\mathbf{v}_{B|A}^{est}(k)|\}. \qquad (13)$$

Step 4: The verifier A estimates the velocity of B for each of the k received ADS-B frames using $\mathscr{V}_{B|A}^{est}$ and its own velocity.

$$\mathscr{V}_B^{est} = \{|\mathbf{v}_B^{est}(1)|, |\mathbf{v}_B^{est}(2)|, \ldots, |\mathbf{v}_B^{est}(k)|\}. \qquad (14)$$

Step 5: The verifier A computes the normalized root mean square error for the velocity estimator:

$$RMSE_v = \sqrt{\frac{\sum_i \left(\frac{|\mathbf{v}_B^{cl}(i)| - |\mathbf{v}_B^{est}(i)|}{|\mathbf{v}_B^{est}(i)|} \right)^2}{k}}, \; i = 1, \ldots, k. \qquad (15)$$

In (15), the difference in magnitude between the claimed and estimated velocities is normalized to the magnitude of the velocity estimated via the maximum Doppler spread method.

Step 6: The verifier A calculates the estimated and claimed distance covered in interframe time t_P, using kinematic equations:

$$d^{est}(i) = \frac{|\mathbf{v}_B^{est}(i)| + |\mathbf{v}_B^{est}(i-1)|}{2} * t_P, \qquad (16)$$

$$d^{cl}(i) = \ell_B^{cl}(i) - \ell_B^{cl}(i-1), \quad i = 2, \ldots, k. \qquad (17)$$

Step 7: The verifier A computes the normalized root mean square error for the distance

$$RMSE_\ell = \sqrt{\frac{\sum_i \left(\frac{d^{cl}(i) - d^{est}(i)}{d^{est}(i)}\right)^2}{k}}. \qquad (18)$$

In (18), the difference in magnitude between the distance covered in t_p is normalized to the magnitude of the distance estimated from the relative radial velocity.

Step 8: If the $RMSE_v \leq \gamma_v$ and $RMSE_\ell \leq \gamma_\ell$, then accept $\mathscr{V}_B^{cl}$ and $\mathscr{L}_B^{cl}$. Else, reject them.

We emphasize that in Step 6, we employed kinematic equations modeling straight line trajectories for aircraft flying at constant velocity. This model is valid when aircraft fly at cruising speed, given the small duration of the verification process (a few seconds). However, this model may not be accurate during takeoff and landing. For the latter, a more complex flight trajectory model can be employed. In this work, we focus on demonstrating the potential of exploiting the PHY-layer attributes on the verification process, rather than exhausting all possible aviation situations. The number of ADS-B frames k necessary for robust verification and the threshold values γ_v, γ_ℓ are system parameters that are empirically tuned depending on the aviation scenario. We study the impact of both parameters in Section 6.

Security Analysis

In this section, we examine if a stationary rogue station G can spoof the trajectory of a ghost aircraft B, while passing the verification process presented in the previous section. We examine two possible spoofing methods. In the first method, G selects a desired trajectory represented by $\mathscr{L}_B^{cl}$ and crafts ADS-B frames that prove $\mathscr{L}_B^{cl}$ to the verifier A. In the second method, G estimates the maximum Doppler spread measured by the verifier A at k positions and attempts to find a valid trajectory $\mathscr{L}_B^{cl}$ that satisfies the estimated relative radial velocities.

Spoofing a desired trajectory $\mathscr{L}_B^{cl}$: Let G transmit k ADS-B frames, claiming position and velocity sets $\mathscr{L}_B^{cl}$ and $\mathscr{V}_B^{cl}$, respectively. First, note that sets $\mathscr{L}_B^{cl}$ and $\mathscr{V}_B^{cl}$ are not independent, but are bound by the kinematic equations (16) and (17). By fixing $\mathscr{L}_B^{cl}$, the claimed positions translate to a set of relative radial headings Θ_B^{cl} according to (2). Computation of these headings require the knowledge of the trajectory of A. The latter can be predicted based on the navigation information broadcasted by A, assuming a straight line trajectory with constant velocity during the expected broadcast of the k ADS-B frames by G. From Θ_B^{cl}, the rogue station G computes the magnitude of the relative radial velocities $\mathscr{V}_{B|A}^{cl}$ that need to be estimated by A to pass the verification process. The $\mathscr{V}_{B|A}^{cl}$ translate to a set of maximum Doppler spread measurements using (3).

The problem of spoofing a desired trajectory $\mathscr{L}_B^{cl}$ reduces to the problem of spoofing a set of maximum Doppler spread values at A. However, the maximum Doppler spread depends on the h_{GA} channel, which is not under the control of G. The only way that G can influence the estimation of h_{GA} at A is by modifying the preamble $x(t)$ of the ADS-B frames. We now show that spoofing ω_D^{sp} by altering $x(t)$ to $x'(t)$ is hard.

Let us consider the transmission of a single ADS-B frame and a desired ω_D^{sp} to be measured at A. The rogue station G can estimate $h_{GA}(t)$ using the ADS-B frames broadcasted by A ($h_{GA}(t)$ and $h_{AG}(t)$ can be considered equivalent due to the channel reciprocity principle[2]). G can then alter the amplitude and phase of the preamble $x(t)$ to $x'(t)$, so that A estimates a desired channel $g_{GA}(t)$ instead of $h_{GA}(t)$.

$$x'(t) = \frac{h_{GA}(t)}{g_{GA}(t)} x(t). \qquad (19)$$

The problem of backtracking the maximum Doppler spread estimation method becomes equivalent to finding the channel samples $g(jT)$ at A that yield the desired ω_D^{sp}. This can be attempted via the following steps:

[2] The channel reciprocity principle primarily holds for low-Doppler spread channels. However, several methods exist to compensate for RF impairments in other cases [22].

Step 1: Fix $r_h(0)$ to any value between 0 and 1. Using the known $r_h(0)$, ω_D^{sp}, f_c and c, calculate $r_h''(0)$ from equation (4).

Step 2: Calculate the values of a_0 and a_2 from $r_h(0)$ and $r_h''(0)$, respectively, using equation (8). Fix a_1 to any value between 0 and 1. This yields matrix

$$A = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix}.$$

Step 3: Using A and L, calculate $R_H = A(L^T L)(L)^{-1}$.

Step 4: R_H yields the $M' = M+1$ correlation estimates $\hat{r_h}(iT)$ that need to be computed by A when sampling $g_{GA}(t)$. Each $\hat{r_h}(iT)$ is calculated by averaging over αN_s channel samples (see eq. (6)). This forms the following system of M' equations and αN_s unknowns, which are the samples of the desired $g_{GA}(t)$ at A.

$$(S)\begin{cases} \sum_j g(jT)g((jT) - \alpha N_s \hat{r_h}(0) = 0 \\ \vdots \\ \sum_j g(jT)g((j+M)T) - \alpha N_s \hat{r_h}(MT) = 0 \end{cases} \tag{20}$$

The equations in S form a multivariate underdefined quadratic equation system. The general problem of solving such systems is NP-hard [14], with the best known algorithms performing almost equivalently to exhaustive search, even for small values of M' [14]. The problem difficulty has motivated their use in public cryptosystems.

Specifically, the so called “Unbalanced Oil and Vinegar" (UOV) scheme is thought to be secure if $3M' \leq \alpha N_s \leq \frac{M'(M'+2)}{2}$ [14]. For a system with M' equations and αN_s unknowns, the M' variables are said to be the “oil" unknowns and the $\alpha N_S - M'$ variables are said to be the “vinegar" unknowns. In our setup, the number of preamble symbols N_s and the symbol duration T_s are fixed by the ADS-B standard. Therefore, to satisfy the conditions of a difficult-to-solve UOV system, we control the sampling period T for each preamble symbol and the number of correlation values M' used to estimate the channel in 6. These values are fixed such that $3M' \leq \frac{T_s N_s}{T}$ and $\frac{T_s}{T} N_s \leq \frac{M'(M'+2)}{2}$, so that the UOV condition [14] is satisfied.

To spoof the desired Doppler shift ω_D^{sp}, the rogue ground station has to find a solution $\Psi^* = \{g(T_s), g(2T_s), \dots, g(\alpha N_s T_s)\}$ for S. However, S has many solutions Ψ due to its underdefined nature, with only Ψ^* leading to the computation of ω_D^{sp}. Finding Ψ^* can only be done via exhaustive search, using methods such as the Levenberg–Marquardt algorithm [23]. For a large number of variables, the size of the search space is prohibitive for a timely solution. We emphasize that this spoofing method requires knowledge of the h_{GA} channel for crafting the preamble at G for all k frames. The channel h_{GA} has been assumed to be known based on the reciprocity principle (using the ADS-B transmissions of A). However, the channel coherence time is particularly short (less than 1 ms) due to the high aircraft velocity. Hence, even if G estimates h_{AG} from A's transmissions, the h_{GA} channel is expected to quickly decorrelate from the observed state.

Shifting the central frequency: We now examine if G can spoof a desired trajectory $\mathscr{L}_B^{cl}$ by shifting the central frequency used to transmit the k ADS-B frames. The idea behind this attack is to exploit equation (3) used for converting the maximum Doppler spread to the relative radial velocity. Similar to the attack of the previous section, G selects a desired $\mathscr{L}_B^{cl}$ for the ghost aircraft B. By fixing $\mathscr{L}_B^{cl}$, the claimed positions translate to a set of relative radial headings Θ_B^{cl} according to (2). From Θ_B^{cl}, the rogue ground station G computes the magnitude of the relative radial velocities $\mathscr{V}_{B|A}^{cl}$ that need to be estimated by A to validate $\mathscr{L}_B^{cl}$. The problem of spoofing $\mathscr{L}_B^{cl}$ becomes equivalent to finding a set of central frequencies

$$\mathscr{F}_c^{sp} = \{ f_c^{sp}(1), f_c^{sp}(2), \dots, f_c^{sp}(k)\},$$
$$f_c^{sp}(i) = \frac{|v_{B|A}^{cl}|(i)}{|v_{B|A}|(i)} f_c, \quad i = 1, \dots, k. \tag{21}$$

However, equation (21) is linear with f_c. To change a true relative radial velocity $|v_{B|A}|$ by p%, the rogue ground station has to shift f_c by p%. Because $f_c = 1090$ MHz, even a small shift in f_c will cause an uncorrectable frequency offset (FO) at A. The ADS-B standard specification requires that receivers can tolerate a FO up to 312.5 KHz [15]. This FO value translates to a possible change in the true relative radial velocity of up to 0.03%. Any larger shifts in the center frequency will render the ADS-B frame undecodable.

Alternate trajectory for true maximum Doppler spread: An alternate strategy for G, is to spoof a trajectory that is compliant with the true maximum Doppler spread measured at A over k ADS-B frames. This strategy is possible because validation of the prover's trajectory is performed via the magnitude of the relative radial velocity. Therefore, there can exist more than one trajectories that yield the true ω_D's. In this spoofing attack, G first computes the set of relative radial velocities $\mathscr{V}_{B|A}^{est}$ that will be estimated by A, given A's trajectory and G's fixed position. From $\mathscr{V}_{B|A}^{est}$, the rogue ground station G attempts to find a trajectory $\mathscr{L}_B^{cl}$ that yields $\mathscr{V}_{B|A}^{est}$ and satisfies the kinematic equations (1), (16), and (17). Specifically, it formulates the following overdefined quadratic equation system.

$$(P)\begin{cases}\mathbf{v}_{B|A}^{est}(i)=|\mathbf{v}_A(i)-\mathbf{v}_B^{cl}(i)|\frac{\ell_A(i)\cdot\ell_B^{cl}(i)}{|\ell_A(i)||\ell_B^{cl}(i)|}\\ \ell_B^{cl}(i)-\ell_B^{cl}(i-1)=\frac{|\mathbf{v}_B^{cl}(i)|+|\mathbf{v}_B^{cl}(i-1)|}{2}*t_P\\ \mathbf{v}_B^{cl}(1)=\mathbf{v}_B^{cl}(2)=\ldots=\mathbf{v}_B^{cl}(k)\end{cases}$$

The system P has $k+1$ unknowns (the k locations in the trajectory $\mathscr{L}_B^{cl}$ plus the constant aircraft velocity $\mathbf{v}_B^{cl}$) and $2k-1$ equations. Finding one solution (but not necessary all solutions) to a system of multivariate polynomial equations is known to be NP-hard [24]. In general, systems with random equations of this type are not expected to have any solution, and for systems for which one solution is known to exist, other interference solutions are not expected to exist. In our context, at least one solution exist, which yields the true location for G. That is, the trajectory $\mathscr{L}_B^{cl}$ for the spoofed aircraft B degenerates to the static location of G. By symmetry, it is easy to show that any point lying on a circle passing through G and centered at the intersection of A's trajectory with the perpendicular plane, satisfies P (see Fig. 5). This is because the headings used for the computation of the relative radial velocity based on transmissions from G do not change if G lies at any point of the circle. However, trajectories which degenerate to single points are of little use to the adversary.

Evaluation

In this section, we evaluate thresholds γ_v and γ_ℓ used in the position and velocity verification. We also demonstrate that truthful location/velocity claims pass the verification process, while spoofed ones are rejected.

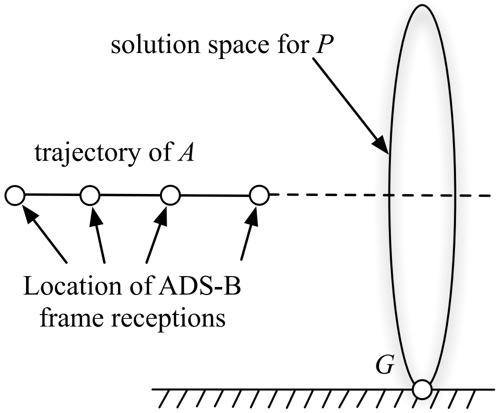
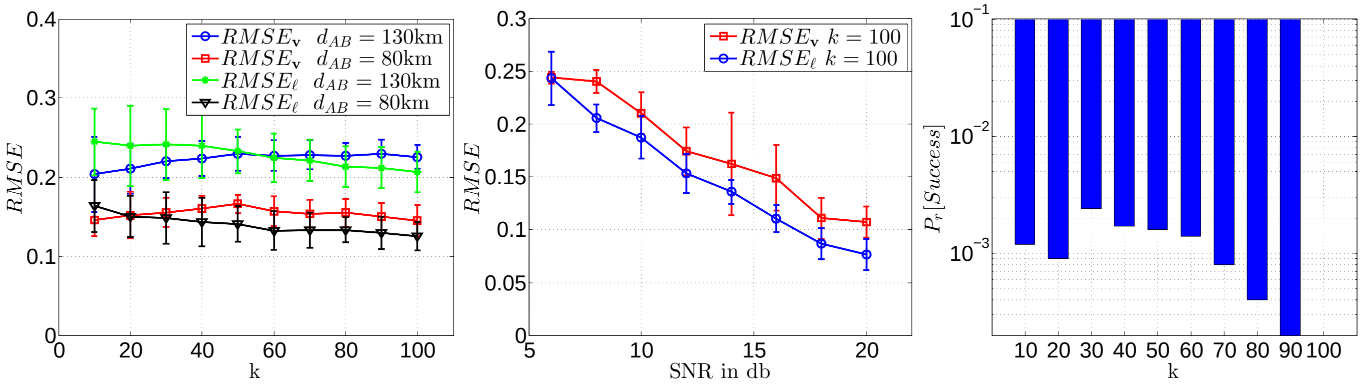


Figure 5. The Possible Spoofed Locations of G That Satisfy P

Simulation Setup: We performed our simulations in MATLAB R2014a. Unless otherwise noted, the prover and the verifier were assumed to fly at constant cruising speed of 900 km/h^{-1} and in opposite directions, while maintaining a constant altitude (as shown in Fig. 4). The symbol duration was set to $T_s = 10^{-6}$ sec based on the 1 Mbps transmission rate of ADS-B. We simulated a Rician channel $h(t)$ between the prover aircraft and the verifier aircraft. We set the K-factor of the Rician model to 50, which is appropriate for line-of-sight communications at high altitude and varied the maximum Doppler shift according to the velocities of the aircrafts. We used Jake's model to simulate the Doppler spectrum. The channel $h(t)$ was estimated by the verifier using the 8-symbol preamble of ADS-B frames ($N_s = 8$). Finally, we set the sampling period to $T = 5*10^{-8}$ sec (20 samples per symbol). For system (S) in (20), the selected parameters yield an underdefined system of 16 equations with 16 "oil" variables and 134 "vinegar" variables, which satisfies the required conditions for the security (S) [14].

Scenario 1: First, we considered a benign scenario in which aircraft B proves its true trajectory to aircraft A. We measured $RMSE_v$ and $RMSE_\ell$ as a function of the number of ADS-B frames k used for the verification in (15) and (18). Two initial distances were considered between the two aircrafts; $d_{AB} = 130$ km and $d_{AB} = 80$ km. Figure 6(a) shows $RMSE_v$ and $RMSE_\ell$, averaged



(a) (b) (c)

Figure 6. (a) ***RMSE*$_v$ as a Function of *k*, (b) *RMSE*$_\ell$ as a Function of *k*, (c) Probability of a Successful Emulation of a Trajectory Spoofing Attack**

over 100 repeated experiment executions. Confidence intervals of 95% are also shown. We observe that average $RMSE_v$ and $RMSE_\ell$ values remain relatively constant with k. However, the variance is reduced as k increases, leading to a more robust estimation of the aircraft location and velocity. We further measured $RMSE_v$ and $RMSE_\ell$ as a function of the SNR, when $k = 100$. Figure 6(b) shows a decreasing RMSE as the SNR improves. The RMSE plots allow us to select the thresholds γ_v and γ_ℓ used to verify the validity of a location/velocity claim at different SNR regimes, corresponding to verifications occurring at different distances between the prover and the verifier.

Scenario 2: In the second scenario, we considered a rogue ground station G spoofing a ghost aircraft B at aircraft A. To spoof B, we followed the steps of the security analysis presented in Section 5.3. We selected a straight line trajectory originating at $d_{AB} = 130$ km away from A, for an aircraft moving in the opposite direction of A at 900 km/h. Based on Fig. 6(a), we set $\gamma_v = 0.25$ and $\gamma_\ell = 0.3$. We used the trajectories of A and B, we computed the headings and relative radial velocities that need to be spoofed by G. We assumed full knowledge of the h_{GA} channel at G and formed the underdefined equation system (S) in (20). To solve (S), we used the in-built MATLAB solver *fsolve*, which employs the Levenberg–Marquardt curve-fitting algorithm [23] to perform an exhaustive search on the solution space. We used the set of targeted relative radial velocities as an input seed into the algorithm. We repeated this process 10,000 times and counted the number of times that G was capable of finding a solution to (S) that would meet both the γ_v and γ_ℓ thresholds. Figure 6(c) shows the ratio of the successful spoofing attempts (when both $RMSE_v$ and $RMSE_\ell$ are less than the corresponding thresholds) to the total number of attempts. We denote this ratio as $P_r[Success]$ and plot it as a function of the number of ADS-B frames used in the verification process. Our results show that G can spoof a ghost aircraft with low probability. Moreover, this probability decreases with the number of ADS-B frames used in the verification.

Related Work

Prior work on the ADS-B security has primarily focused on highlighting vulnerabilities to well-known attacks in wireless communications. Sampigethaya et al. have analyzed the security and privacy of ADS-B in the context of an “e-enabled” aircraft [10]. They defined an adversary model for the aviation domain and enumerated various RF communications related threats. These threats include eavesdropping, radio-frequency jamming, aircraft impersonation, active manipulation of data, and others. They have also proposed a list of system requirements for securing the ADS-B operation.

Strohmeier et al. surveyed ADS-B attacks that have been reported in recent literature [12]. Specifically, they discussed eavesdropping, jamming, message injection, message modification, and message deletion. Moreover, they presented state-of-the-art theoretical and practical efforts to counter the ADS-B threats. McCallie et al. also performed a survey on the vulnerabilities of ADS-B and related these vulnerabilities to air transportation operation and management risks [25]. They classified attacks to a taxonomy based on their nature to facilitate the application of possible solutions.

Costin and Francillon experimentally demonstrated the insecurity of ADS-B using solely the USRP platform and COTS radio transceivers [3]. By implementing a practical, low-cost and moderately sophisticated attacker, they demonstrated ADS-B message replay/injection attacks with relative ease. They also suggested solutions relying on the integration of lightweight cryptographic mechanisms.

While the threats on ADS-B are well-documented, few solutions exist that mitigate such threats. Sampigethaya and Poovendran proposed a group navigation method for verifying the message integrity of ADS-B IN messages. They presented a framework in which aircrafts are divided into groups according to average velocity, spatial dependency, and temporal restrictions derived from their trajectories. Each group is coordinated by a leader, who verifies position of other aircrafts by measuring time-difference-of-arrival of ADS-B messages. They further proposed a security simulation tool concept to visualize and asses the impact of ADS-B vulnerabilities.

Several researchers have proposed the integration of cryptographic mechanisms into the ADS-B standard [3], [7], [26]. Using well-known cryptographic techniques, ADS-B broadcasts can be authenticated, secured from message modification and replay, and impersonation attacks. However, such solutions require the costly redesign of the ADS-B standard and the worldwide deployment of a security infrastructure. The cost and security challenges associated with key management and inter-operability outweigh the potential benefits [13].

Krozel et al. [27] have proposed to use a suite of Kalman filters to reduce noise within measured ADS-B signals. Noise reduction is intended to identify wrong data and reduce the effect of data dropouts. Further, the authors have proposed integrity check mechanisms for ADS-B data using intent and geometric conformance. Intent conformance is the process by which the motion of an aircraft is compared with the broadcasted intent in vertical, horizontal, and speed dimensions. On the other hand, geometric conformance verifies that the aircraft state lies within the vertical and horizontal Required Navigation Performance (RNP) limits. For intent verification they have proposed a correlation function using the information included in ADS-B signals. The aircraft state variables are verified independently by separate uncoupled Kalman filters.

Conclusions and Future Work

We addressed the problem of the verifying the integrity of ADS-B navigation information without modifying the ADS-B standard. We proposed a PHY-layer verification method that exploits the Doppler spread phenomenon and the short coherence time of the channel between a prover aircraft and verifier aircraft to verify the velocity claims of the prover. The solution proposed in this work can be aplied independently of the ADS-B standard. We further related the velocity claims to location claims through simple kinematic equations. We analyzed the security of our verification scheme and showed that it is equivalent to solving underdefined quadratic equation systems which is known to be hard.

This work can be extended to study the security and accuracy of the proposed method in different adversarial scenarios. A natural extension considers the collusion of multiple ground stations which coordinate their falsified signals to spoof a ghost aircraft. Intuitively, the fundamental problem of the adversary is that he is unable to solve the set of underdefined quadratic equations for determining the signals that need to be transmitted from the multiple ground stations. A more advanced (and costly) adversary model can consider an airborne attacker that spoofs ADS-B signals. The set of candidate trajectories that can be emulated by an airborne attacker warrant further investigation. Finally, the present work considers a verification process that occurs at cruising altitude and at cruising speed. The verification of ADS-B signals during other flight phases, such as takeoff and landing, requires further investigation.

References

[1] I. A. T. Association *et al.*, *Airlines to welcome 3.6 billion passengers in 2016*, 2012.

[2] M. G. Whitaker, *Nextgen works for america: Chief nextgen officer update to congress*, Pursuant to Section 204 of the FAA Modernization and Reform Act of 2012 (P.L. 112-95), Federal Aviation Administration, 2014.

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

[4] W. Peng, Y. Li, H. Li, and B. Wen, "A novel high-sensitivity ADS-B receiver based on RF direct logarithmic detecting," in *Proc. of the International Conference on Computer Application and System Modeling*, 2012.

[5] G. Wright, "NAV CANADA implements ADS-B," in *Proc. of the Integrated Communications, Navigation and Surveillance Conference*, 2009, pp. 1–9.

[6] F. Kunzi and R. J. Hansman, *ADS-B benefits to general aviation and barriers to implementation*, http://hdl.handle.net/1721.1/63130, 2011.

[7] J. Baek, Y.-j. Byon, E. Hableel, and M. Al-Qutayri, "Making air traffic surveillance more reliable: A new authentication framework for automatic dependent surveillance-broadcast (ADS-B) based on online/offline identity-based signature," *Security and Communication Networks*, 2014.

[8] A. E. Smith, *Method and apparatus for improving ADS-B security*, US Patent 7,423,590, 2008.

[9] K. Sampigethaya and R. Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems," in *Proc. of the Communication Systems and Networks Conference*, 2011, pp. 1–6.

[10] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proc. of the IEEE*, vol. 99, no. 11, pp. 2040–2055, 2011.

[11] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Proc. of the Applied Cryptography and Network Security Conference*, 2013, pp. 253–271.

[12] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ADS-B: State of the art and beyond," *ArXiv preprint arXiv:1307.3664*, 2013.

[13] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?" *IEEE Security and Privacy Magazine*, 2014.

[14] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *Proc. of EUROCRYPT*, Springer, 1999, pp. 206–222.

[15] F. A. Administration, *Automatic dependent surveillance broadcast (ADS-B) out performance requirements to support air traffic control (ATC) service; final rule*, 75(103), 14 CFR Part 91 Federal Register, 2010.

[16] M. D. Austin and G. Stüber, "Velocity adaptive handoff algorithms for microcellular systems," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 3, pp. 549–561, 1994.

[17] M. J. Chu and W. E. Stark, "Effect of mobile velocity on communications in fading channels," *IEEE Transactions on Vehicular Technology*, vol. 49, no. 1, pp. 202–210, 2000.

[18] S. Hu, T. Eyceoz, A. Duel-Hallen, and H. Hallen, "Transmitter antenna diversity and adaptive signaling using long range prediction for fast fading ds/cdma mobile radio channels," in *Proc. of the Wireless Communications and Networking Conference*, 1999, pp. 824–828.

[19] J. M. Holtzman and A. Sampath, "Adaptive averaging methodology for handoffs in cellular systems," *Vehicular Technology*, vol. 44, no. 1, pp. 59–66, 1995.

[20] G. Park, D. Hong, and C. Kang, "Level crossing rate estimation with Doppler adaptive noise suppression technique in frequency domain," in *Proc. of the VTC Conference*, vol. 2, 2003, pp. 1192–1195.

[21] C. Tepedelenlioğlu and G. B. Giannakis, "On velocity estimation and correlation properties of narrowband mobile communication channels," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 4, pp. 1039–1052, 2001.

[22] W. Xiang, P. Richardson, and J. Guo, "Introduction and preliminary experimental results of wireless access for vehicular environments (WAVE) systems," in *Proc. of the Mobile and Ubiquitous Systems-Workshop*, 2006, pp. 1–8.

[23] D. W. Marquardt, "An algorithm for least-squares estimation of nonlinear parameters," *Journal of the Society for Industrial & Applied Mathematics*, vol. 11, no. 2, pp. 431–441, 1963.

[24] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined

systems of multivariate polynomial equations," in *Advances in Cryptology*, 2000, pp. 392–407.

[25] 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.

[26] R. Chen, C. Si, H. Yang, and X. Zhang, "ADS-B data authentication based on AH protocol," in *Proc. of the IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2013, pp. 21–24.

[27] J. Krozel, D. Andrisani, M. A. Ayoubi, T. Hoshizaki, and C. Schwalm, "Aircraft ADS-B data integrity check," in *Proc. of the AIAA Aviation, Technology, Integration, and Operations Conference*, 2004.

Acknowledgments

This research was supported in part by the NSF under grant CNS-1409172 and ARO grant W911NF-13-1-0302. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF.

Email Addresses

nghose@email.arizona.edu,llazos@ece.arizona.edu