TDOA based ADS-B validation using a Particle Filter and Statistical Hypothesis testing

Tom Landzaat
Royal NLR
Amsterdam, The Netherlands
tom.landzaat@nlr.nl

Hans Driessen
TU-Delft, EEMCS/ME/MS3
Delft, The Netherlands
j.n.driessen@tudelft.nl

Hans van Hintum
LVNL, S&I \CNSI \SUR
Amsterdam, The Netherlands
j.e.a.vanhintum@lvnl.nl

***Abstract*—ADS-B is a widely used protocol that transmits aircraft's position, velocity among other data. The protocol is not encrypted leading to the need of validation. A validation algorithm is proposed that makes use of Time Difference of Arrival localization to validate the position and velocity of ADS-B transmitting targets. Nowadays, Air navigation service providers (ANSP) commonly have at least one TDOA localization system in operation, allowing for cost effective implementation. Validation is achieved by using a Particle Filter and hypothesis tests. A novel method is used where the initial density is generated effectively based on the first set of TDOA measurements. Validation is possible when two or more ground stations receive the same ADS-B transmission, therefore the Particle Filter is designed to process such measurements. The algorithm is tested on data provided by Air Traffic Control The Netherlands' North sea surveillance system. Results show that the validation works and that the algorithm is able to detect spoofing. Based on spoofed ADS-B messages and true TDOA measurements, the real and fake target can be detected when the distance is roughly 750 to 1000 meters (depending on the situation and the various tuning parameters). In addition, validation based on two or more ground stations per measurements has the effect that the covered area is increased. Considering TDOA systems require four GSs for tracking applications.**

***Index Terms*—ADS-B, Validation, TDOA, Particle Filter, Hypothesis Testing, State Estimation, Spoofing Detection**

I. Introduction

Automatic Dependent Surveillance Broadcast (ADS-B) allows commercial aircraft to broadcast their own position, speed, altitude, and other information to ground stations and other nearby aircraft. This information is then used by air traffic control for situational awareness, and collision avoidance. ADS-B spoofing is possible due to the lack of authentication and encryption in the ADS-B protocol. This can result in incorrect decision-making and safety hazards. Ground station flooding, false alarm attack and virtual trajectory modification are some of the attack types as described in [1]. Forging a spoofed ADS-B is demonstrated in [2] showing the vulnerability of the system.

This paper is based on the Master Thesis of the first author as part of the Electrical Engineering Master at TU-Delft, executed in cooperation with Air Traffic Control The Netherlands (LVNL). Finalization and publication has been supported by his current employer the Royal NLR.

Encryption has been proposed to ensure the validity of ADS-B messages [3]–[5], but ADS-B is not intended and designed for encryption and therefore not a feasible solution.

Machine-Learning (ML) based solutions are also proposed [6]–[8]. A significant disadvantage of ML is that it is vulnerable to real ADS-B messages transmitted at a later time. Secondly, training data of spoofed messages are required and it is hard to obtain proper training data.

Third type of validation that is proposed in literature is validation based on measurements of the ADS-B transmission. This can be done by measuring the angle of arrival of the impinging signal [9], [10]. But also traditional Mode-S radar can be used for validation.

This paper proposes an algorithm that validates the position and velocity of ADS-B messages based on position and velocity estimates computed from a series of Time Difference of Arrival (TDOA) measurements. The motivation for TDOA is twofold. Firstly, validation requires at least two Ground Stations (GS) per received ADS-B message, compared to tracking that requires at least four GSs per measurements. This leads to an increase in coverage and substantial increase in available measurements for processing. Secondly, many Air Navigation Service Providers (ANSP) have operational TDOA systems, allowing for a cost effective implementation.

To estimate the position and velocity from the TDOA measurements the use of a track filter is proposed. In [11] and [12] two track filters have been presented. They both first compute target position from the GS measurements, and run a track filter using these position estimates. At least four TOA measurements are required to obtain a unique position estimate. In practice, however, a significant portion of TDOA measurements originate from only two or three GSs, meaning the measurements are ambiguous in location (the target is somewhere on a hyperboloid of two sheets or the intersection of two such hyperboloids). These measurements are neglected in approaches like [11] and [12].

Nevertheless, ambiguous measurements still provide enough information of the ADS-B target such that the position can be validated. Therefore a Particle Filter (PF) is proposed that is able to process measurements originating

from two GSs or more. Such a state estimator is sufficient when validating ADS-B messages. This approach allows for validation in a larger area, because the area covered with two GSs is always larger than the area covered by four GSs.

Section II introduces the state estimation problem and section III describes the implemented PF. The spoofing detection is treated as a binary hypothesis testing problem and the derivation and implementation details of the hypothesis test are described in section IV. In section V the entire algorithm is analysed based on real TDOA measurements and ADS-B messages provided by the North Sea Wide-Area Multilateration system operational at Air traffic Control the Netherlands (LVNL).

II. State Estimation based on TDOA measurements

In this section the problem of estimating object position and velocity from series of TDOA measurements is presented as a state estimation problem.

A. Bayesian State Estimation

Let $\mathbf{x}_k$ denote the state vector. The generic state evolution and the measurement model are given as

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{f}_k\left(\mathbf{x}_k, \mathbf{w}_k\right) \\ \mathbf{z}_k &= \mathbf{h}_k(\mathbf{x}_k, \mathbf{n}_k) \end{aligned} \tag{1}$$

where $\mathbf{f}_k\left(\mathbf{x}_k, \mathbf{w}_k\right)$, represents the object dynamics with $\mathbf{w}_k$ the process noise, and $\mathbf{h}_k(\mathbf{x}_k, \mathbf{n}_k)$ represents the measurement function, where $\mathbf{n}_k$ is the measurement noise.

The state evolution and measurement equation define the transition density $p(\mathbf{x}_{k+1}/\mathbf{x}_k)$ and the likelihood $p(\mathbf{z}_k/\mathbf{x}_k)$ respectively.

The posterior density allows a recursive expression referred to as Bayesian recursion given by

$$\begin{aligned} p(\mathbf{x}_{k+1} \mid \mathbf{Z}_k) &= \int p(\mathbf{x}_{k+1} \mid \mathbf{x}_k) p(\mathbf{x}_k \mid \mathbf{Z}_k) d\mathbf{x}_k \\ p(\mathbf{x}_k \mid \mathbf{Z}_k) &= \frac{p(\mathbf{z}_k \mid \mathbf{x}_k) p(\mathbf{x}_k \mid \mathbf{Z}_{k-1})}{p(\mathbf{z}_k \mid \mathbf{Z}_{k-1})} \end{aligned} \tag{2}$$

The state estimation problem is now defined as obtaining an approximation to the posterior density $p(\mathbf{x}_k/\mathbf{Z}_k)$, where $\mathbf{Z}_k$ represents the collection of all measurements received until (and including) time t_k.

B. Object dynamics

In the proposed filter solution a nearly constant velocity model is used. This model is sufficient for many ANSPs due to the fact that almost all commercial airliners fly at an almost constant velocity. Also during landing and take-off the constant velocity is found to be sufficient. Let the state vector be defined as

$$\mathbf{x}_k^T = [\mathbf{l}_k^T \mathbf{v}_k^T] \tag{3}$$

with $\mathbf{l}_k$ and $\mathbf{v}_k$ the 3D location and velocity of the target, respectively. The target dynamics then becomes the linear Gaussian model defined by

$$\mathbf{x}_{k+1} = \mathbf{F}\mathbf{x}_k + \mathbf{w}_k \tag{4}$$

with

$$\mathbf{F} = \begin{bmatrix} \mathbf{I}_3 & T_k\mathbf{I}_3 \\ \mathbf{O}_3 & \mathbf{I}_3 \end{bmatrix} \tag{5}$$

where $\mathbf{I}_3$ is the 3D identity matrix and $T_k = t_{k+1} - t_k$. The covariance of the process noise is defined as

$$\mathbf{W}_k = \sigma_w^2 \begin{bmatrix} \frac{T_k^3}{3}\mathbf{I}_3 & \frac{T_k^2}{2}\mathbf{I}_3 \\ \frac{T_k^2}{2}\mathbf{I}_3 & T_k\mathbf{I}_3 \end{bmatrix}. \tag{6}$$

C. TDOA measurements

The TDOA measurements are constructed from TOA measurements originating from the same transmission received by N_k GSs. Obviously the TOA's depend on the distance between the target location $\mathbf{l}_k$ and the GS positions $\mathbf{s}_j, j = 1, \ldots, N_k$. In what follows, we assume that the GS position $\mathbf{s_1}$ is defined as the GS that receives the ADS-B message first, j refers to one of the other GSs that delivers a TOA measurement. Each TDOA measurement equation is assumed being generated according to

$$z_k^j = h_k^j(\mathbf{l}_k) + n_k^j \text{ for } \quad j = 1, \ldots, (N_k - 1) \tag{7}$$

with n_k^j the measurement noise, and the nonlinear measurement function

$$h_k^j(\mathbf{l}_k) = \frac{||\mathbf{s}_{j+1} - \mathbf{l}_k|| - ||\mathbf{s}_1 - \mathbf{l}_k||}{c} \tag{8}$$

with c the speed of light.

Besides nonlinear, the model underlying each TDOA measurement is ambiguous, since it defines a paraboloid of two sheets containing infinitely many locations leading to the same measurement. It is well-known that TDOA measurements from four (or more) GSs at different locations and heights lead to a unique location. However in our approach it is desired to work with less than four GS TOA measurements per scan.

The measurement vector $\mathbf{z}_k$ is constructed as a collection of TDOA measurements generated via Eq. (7)

$$\mathbf{z}_k = \mathbf{h}_k(\mathbf{l}_k) + \mathbf{n}_k, \tag{9}$$

where the number of these measurements varies from time to time depending on factors like the exact positions of the GSs and their distances to the target.

Assuming the noise of the TOA measurements is zero mean and uncorrelated between the GSs, the covariance $\mathbf{Q}$ of $\mathbf{n}_k$ is given as

$$\mathbf{Q} = \mathbf{C}\mathbf{\Sigma}\mathbf{C}^T \tag{10}$$

with

$$\mathbf{C} = \begin{bmatrix} -1 & 1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \tag{11}$$

and where $\mathbf{\Sigma}$ is a diagonal matrix with the variances of the individual TOA measurements as the corresponding diagonal elements.

The pdf of the measurements conditioned on the target state is then given as follows

$$p(\mathbf{z}_k \mid \mathbf{x}_k) = \frac{1}{\sqrt{|2\pi\mathbf{Q}|}} \exp\left(-\frac{1}{2}||\mathbf{z}_k - \mathbf{h}_k(\mathbf{l}_k))||^2_{\mathbf{Q}}\right) \quad (12)$$

with notation $||\mathbf{a}||^2_{\mathbf{B}} = \mathbf{a}^T\mathbf{B}^{-1}\mathbf{a}$.

III. Particle Filter Description

Since our aim is to develop a filter that can work with TDOA measurements from less than four GSs, a particle filter solution is advocated. The proposed PF is essentially a Sequential Importance Resampling (SIR) filter, except for the filter initialization.

A. Particle Filter Initialization

A generic initialization of the filter would be to generate particles in a large 3D volume independent of the knowledge of the GS positions that received the TOA measurements and the TOA measurements themselves, and proceed with a SIR filter update. In this particular application, such a generic initialization would be extremely inefficient. Instead the initialization is based on the following considerations.

At first, every TDOA measurement commonly represents a potential target location on a hyperboloid of two sheets. In our application, the individual TOAs associated with the GSs are known, such that one of these sheets is not valid. Secondly, the height of the targets that are to be dealt with are positive and lie in a relatively small interval. Thirdly, the points on a hyperboloid allow an easy sampling; one coordinate of each point on a hyperboloid can be written as an explicit function of the other two. These three considerations together makes it possible on the basis of one TDOA measurement to generate an equally weighted set of particles that can serve as the initial particle cloud. This procedure can be repeated in case more TDOA measurements are available in the first scan.

B. Particle Filter Flow Chart

The flow chart of the SIR filter is given as Algorithm 1

Algorithm 1 SIR-Particle Filter Algortihm

Input: $\mathbf{z}_k$
Output: $\{\mathbf{x}^i_k, \omega^i_k\}, i = 1, \ldots, N_s$

1: Generate an initial set of particles, see III-A
2: Set $\omega^i_0 = 1/N_s$ for $i = 1, ..., N_s$
3: **for** k = 1,...,K **do**
4: Compute $\omega^i_k = p(\mathbf{z}_k|\mathbf{l}^i_k)$ for $i = 1, \ldots, N_s$
5: Resample using multinomial resampling
6: Normalize $\omega^i_k = \frac{\omega^i_k}{\sum \omega^i_k}$
7: Sample $x^i_k \sim p(\mathbf{x}_k|\mathbf{x}^i_{k-1})$ for $i = 1, \ldots, N_s$

IV. Hypothesis Testing

In this section, a hypothesis test is defined using the information in the ADS-B message, its measurement equation, and the posterior pdf on the target state based on TDOA measurements, as obtained via the SIR-PF. This hypothesis test can be used to determine the ADS-B message as spoofed or not spoofed. To achieve this the likelihood ratio test (LRT) is used and the null and alternative hypotheses and their likelihoods are defined.

However before outlining the details of the hypothesis testing, since the ADS-B measurements are longitude, lattitude, height and speed, the state is transformed to Cartesian coordinates (comprising 3D location and velocity).

$$\mathbf{z}^{ADSB}_g = \mathbf{g}(\mathbf{z}^{ADSB}_c) \quad (13)$$

Where c denotes Cartesian coordinate system, and g Geodetic coordinates. This transformation uses an approximation to transform the associated covariance, resulting in the ADS-B covariance R_k.

In the remainder of this section, ADS-B measurements are considered to be in Cartesian coordinates.

A. Hypothesis Definition

$\mathcal{H}_0$: No spoofing
$\mathcal{H}_1$: Spoofing

The probability of detecting spoofing is defined as

$$p(\text{choose } \mathcal{H}_1|\mathcal{H}_1) = P_d \quad (14a)$$

and the associated probability of miss detection as

$$p(\text{choose } \mathcal{H}_0|\mathcal{H}_1) = P_m = 1 - P_d \quad (14b)$$

The probability of false detection of spoofing is defined as

$$p(\text{choose } \mathcal{H}_1|\mathcal{H}_0) = P_{fa} \quad (14c)$$

and the probability of a correct acceptance of the ADS-B measurement as

$$p(\text{choose } \mathcal{H}_0|\mathcal{H}_0) = P_a = 1 - P_{fa} \quad (14d)$$

The likelihood ratio of the ADS-B message being spoofed or not is defined as the ratio of the likelihoods of the ADS-B message conditioned on the received TDOA measurements under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively

$$L(\mathbf{z}^{ADSB}_k) = \frac{p\left(\mathbf{z}^{ADSB}_k|\mathbf{Z}_k, \mathcal{H}_0\right)}{p\left(\mathbf{z}^{ADSB}_k|\mathbf{Z}_k, \mathcal{H}_1\right)} \underset{H_1}{\overset{H_0}{\gtrless}} \tau \quad (15)$$

where $\mathbf{Z}_k$ represents all TDOA measurements received so far.

1) Null Hypothesis: The likelihood under the null hypothesis, i.e. no spoofing, is given by;

$$p\left(\mathbf{z}^{ADSB}_k|\mathbf{Z}_k, \mathcal{H}_0\right) = \int p(\mathbf{z}^{ADSB}_k|\mathbf{x}_k, \mathcal{H}_0)p(\mathbf{x}_k|\mathbf{Z}_k)d\mathbf{x}_k \quad (16)$$

The first term under the integral is the likelihood on a non-spoofed ADS-B measurement. With the above modeling assumptions the likelihood is given by

$$p\left(\mathbf{z}_k^{ADSB}|\mathbf{x}_k,\mathcal{H}_0\right)=\frac{1}{\sqrt{|2\pi R_k|}}\exp\left(-\frac{1}{2}||\mathbf{z}_k^{ADSB}-\mathbf{x}_k||^2_{\mathbf{R}_k}\right) \tag{17}$$

The second term under the integral is the posterior density on the target state given all TDOA measurements. This is, as explained before, in general a non-Gaussian density, which is represented with the particle cloud computed from the particle filter. This implies that the integral can be approximated with

$$p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_0\right)\approx\ldots$$
$$\ldots\frac{1}{N_s}\sum_{i=1}^{Ns}\frac{1}{\sqrt{|2\pi R_k|}}\exp\left(-\frac{1}{2}||\mathbf{z}_k^{ADSB}-\mathbf{x}_k^i||^2_{\mathbf{R}_k}\right) \tag{18}$$

2) Spoofing Hypothesis: Under the spoofing hypothesis $p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_1\right)$ represents the likelihood of a spoofed target message. It is assumed that this likelihood does not depend on the TDOA measurements. Secondly, the only information about a spoofed target message is that it will be within the area where one of the ground stations can receive the message, therefore this is represented with a uniform pdf over a relatively large volume V

$$p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_1\right)=\frac{1}{V} \tag{19}$$

B. Likelihood Ratio Test

Combining the likelihoods $p(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_0)$ and $p(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_1)$, the Likelihood Ratio can be approximated as

$$L(\mathbf{z}_k^{ADSB})\approx\ldots$$
$$\ldots\frac{1}{N_s}\sum_{i=1}^{Ns}\frac{V}{\sqrt{|2\pi R_k|}}\exp\left(-\frac{1}{2}||\mathbf{z}_k^{ADSB}-\mathbf{x}_k^i||^2_{\mathbf{R}_k}\right)\underset{H_1}{\overset{H_0}{\gtrless}}\tau \tag{20}$$

For each ADS-B message the LRT is computed and compared against the threshold τ. Three methods of determining τ are considered namely, the Minimum Bayes Risk (MBR), Neyman-Pearson (NP) and Minmax (MM). The MBR relies on knowledge of the prior probability on spoofing and the definition of costs that are associated with the decision errors, NP only requires a pre-specified probability of false alarm, while MM only relies on the definition of costs associated with the decision errors.

1) Minimum Bayes Risk: Applying the setting of the threshold according to the MBR, two ingredients are required. At first prior probabilities associated with the hypotheses are assumed to be known as π_0 and π_1, respectively. The prior probabilities can be set by the user depending on their perception of the probability that spoofing can occur. Secondly, costs associated with the decision error are defined as C_{10} and C_{01}, representing the cost of a false alarm and a miss, respectively. The costs can be set by the user reflecting the relative costs associated with the decision errors.

Having specified these parameters, the MBR aims at minimizing the Bayesian (average) risk

$$\mathcal{R}(\tau)=C_{10}\pi_1P_m(\tau)+C_{01}\pi_0P_{fa}(\tau) \tag{21}$$

where the minimum risk is obtained by setting the threshold according

$$\tau_{MBR}=\frac{C_{01}}{C_{10}}\frac{\pi_1}{\pi_0} \tag{22}$$

This is a very elegant and computationally tractable result. It is commonly less easy to compute the attained minumum risk, but usually that is of less interest to the user. This test is usually preferred over alternatives, provided appropriate prior probabilities and costs can be selected.

2) Neyman-Pearson: In the NP procedure, the threshold is set such that the test maximizes the probability of detection P_d for a desired probability of false alarm P_{fa}. Commonly, like in this case, after selection of the P_{fa}, there are no degrees-of-freedom for maximizing the P_d. Therefore, it remains to specify the threshold in terms of the P_{fa}, which is given by the following integral expression.

$$P_{fa}(\tau_{NP})=\int_{L(\mathbf{z}_k^{ADSB})>\tau_{NP}}p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_0\right)d\mathbf{z}_k^{ADSB} \tag{23}$$

with $p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_0\right)$ as defined in Eq. (16).

An explicit analytic expression for this integral is generally impossible to obtain. In this particular case, the assumption of a Gaussian distribution is being used. The first pdf in Eq. (16), $p\left(\mathbf{z}_k^{ADSB}|\mathbf{x}_k,\mathcal{H}_0\right)$, is Gaussian, due to the measurement modeling assumptions. The second pdf in the same equation, $p(\mathbf{x}_k|\mathbf{Z}_k)$, is available as a particle cloud as computed by the SIR particle filter, Here, this density is approximated by a Gaussian with matching first and second order statistics

$$p(\mathbf{x}_k|\mathbf{Z}_k)\approx\mathcal{N}(\mathbf{x}_{k/k},\mathbf{P}_{k/k}) \tag{24}$$

with $\mathbf{x}_{k/k}$ and $\mathbf{P}_{k/k}$, the mean and the covariance of the particle cloud $\{\mathbf{x}_k^i\}, i=1,\ldots,N_s$, respectively.

Using this approximation, the conditional pdf on the ADS-B message can be approximated with

$$p\left(\mathbf{z}_k^{ADSB}|\mathbf{Z}_k,\mathcal{H}_0\right)\approx\mathcal{N}(\mathbf{x}_{k/k},\mathbf{S}_k) \tag{25}$$

with $\mathbf{S}_k=\mathbf{P}_{k/k}+\mathbf{R}_k$.

For the four dimensional ADS-B message (longitude, lattitude, height, and speed), assuming the Gaussian approximation, the probability of false alarm can be computed as [13]

$$P_{fa}(\tau_{NP})=\left(1+\frac{G(\tau_{NP})}{2}\right)\exp\left(-\frac{G(\tau_{NP})}{2}\right) \tag{26}$$

with the gate $G(\tau_{NP})$ defined as function of the NP threshold τ_{NP} according to

$$G(\tau_{NP})=-2\ln\left(\frac{\tau_{NP}}{V}\sqrt{2\pi|\mathbf{S}_k|}\right) \tag{27}$$

Using these expressions, a relationship between false alarm probability and the detection threshold has been obtained,

which can be inverted, using one of the available mathematics toolboxes. This formula is quite involved and is left out of the paper.

3) Minmax: An alternative to the NP-test is the Minmax test, which is based on assuming no knowledge of the prior probability π_0, and $\pi_1 = 1 - \pi_0$. Under the Minmax approach the maximum Bayes Risk is minimized

$$\tau_{MM} = \arg\min_{\tau} \left(\max_{0 \leq \pi_0 \leq 1} \mathcal{R}(\pi_0, \tau) \right) \tag{28}$$

The conditional risks are defined as,

$$R_0(\tau) = C_{10} P_m \tag{29a}$$

$$R_1(\tau) = C_{01} P_{fa} \tag{29b}$$

These two are combined to obtain the total Bayes Risk,

$$\mathcal{R}(\pi_0, \tau) = \pi_0 R_0(\tau) + (1 - \pi_0) R_1(\tau) \tag{30}$$

It has been shown in [14] that when the two conditional risks are equal, the maximum Bayes Risk is minimized. The threshold can thus be obtained by Eq. (31)

$$R_0(\tau) = R_1(\tau) \tag{31}$$

$R_0(\tau)$ can be found in Eq. (26), and P_m by [13]

$$P_m = \frac{1}{V} \frac{\pi^2}{2} \sqrt{|S_k|} G(\tau_{MM})^2 \tag{32}$$

V. Results

A. Detection Performance

The validation algorithm is tested on a wide-area multilateration system in operation by the LVNL designed by ERA. Three flights are inspected in the analysis, Flight A is a north-bound flight from Schiphol Airport at FL300, B similar and containing large amounts of measurements (see figure 2)where the number of ground stations is below four, and flight C a helicopter operating at FL25.

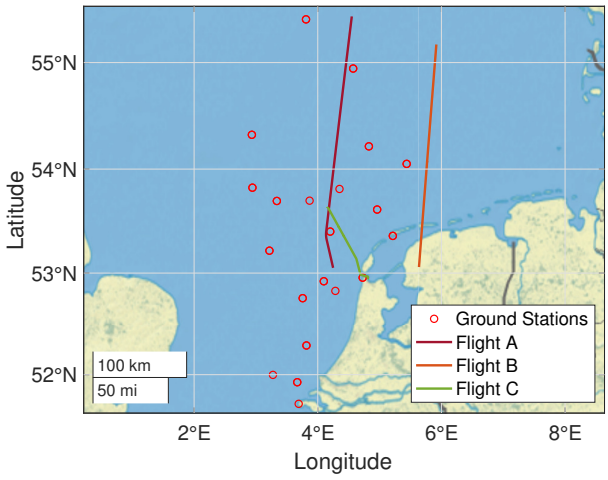

Fig. 1. Overview of ground stations and flights

Table I shows the percentage of received ADS-B messages that are validated by the MBR, NP and MM respectively. Detailed investigation shows that in flight C the PF is unable to correctly estimate the height of the target due to very bad vertical dilution of precision, this is a known TDOA issue. Velocity and horizontal position are estimated correctly by the PF. Furthermore, The algorithm performs good and as expected in nominal operations.

	MBR	NP	MM
Flight A	100%	100%	100%
Flight B	100%	100%	100%
Flight C	96.0375%	95.2738%	100%

TABLE I
PERCENTAGE OF MESSAGES VALIDATED

Figure 2 shows the distribution of number of ground stations that receive each ADS-B message for flight B. This histogram illustrates the amount of measurements that can be used for validation. Measurements from two or three GSs are generally ignored by conventional TDOA systems.

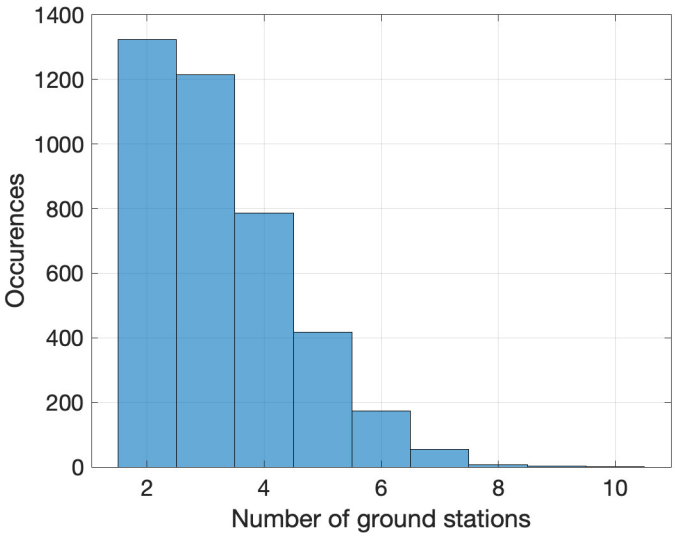

Fig. 2. Histogram showing the distribution of GSs receiving each ADS-B message for flight B

Figures 3 and 4 illustrate a scenario where the use of all measurements leads to an increased coverage. At low altitudes the ADS-B messages are received by few GSs, thus in such scenarios the coverage is increased. Figure 4 suggest a bias in the PF. But it must be noted that the operational system at LVNL is calibrated and the PF is not, leading to a difference in performance. The increased covered area is largely dependent on the area which is covered by two or three GSs. In this scenario at take-off the increase is marginal, and at final approach, the increased coverage is about 400 meter. For en-route traffic this area is expected to increase due to the wider spread of GSs at higher altitudes.

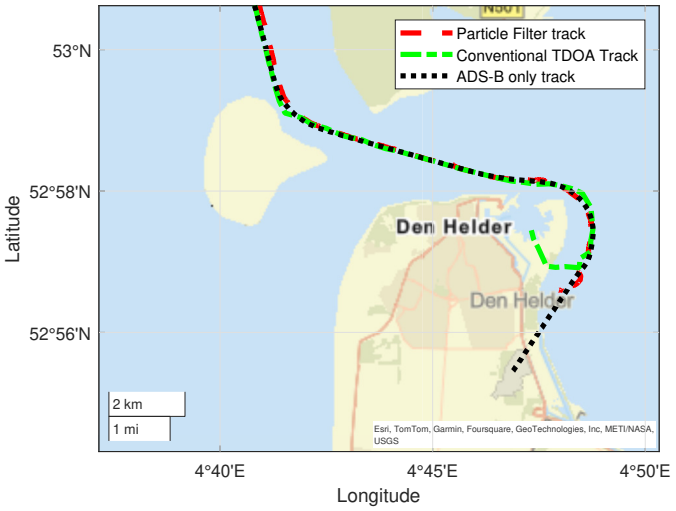

Fig. 3. Track of start of flight B

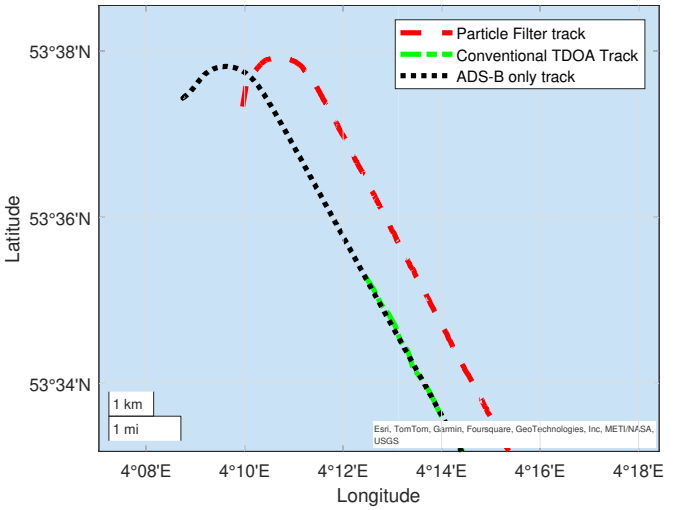

Fig. 4. Track of end of flight B

B. Spoofing Detection Performance

In this section two different dynamic spoofing scenarios are investigated based on flights B and C. The scenario is such that an airborne target alters its ADS-B location from beginning to the end of the flight, with an offset in the horizontal plane or vertical plane. The spoofed trajectory is a parallel track with respect to the real airborne target.

1) Flight B: The real transmitted ADS-B messages are offset with the indicated error in the figures 5 and 6. Results show that the NP detector is the most sensitive to detecting the offset in the real ADS-B messages with respect to the true location of the target. Figure 6 illustrates that all three detectors have better performance in detecting vertical spoofing when compared to horizontal spoofing. Likely the result of the associated ADS-B and PF uncertainty in each dimension.

A pattern can be seen in the data where initially the target is accepted as a true ADS-B message, but as the filter closes in on the true location, and the uncertainty decreases, all three hypothesis test eventually decide the message is spoofed.

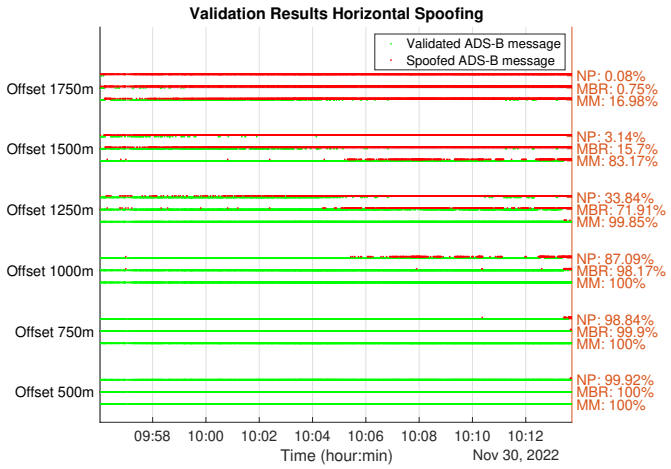

Fig. 5. Flight B: Spoofing detection results for horizontal spoofing. Right hand side shows the percentage of messages validated for each hypothesis test. Left hand size shows the offset compared to the true ADS-B track

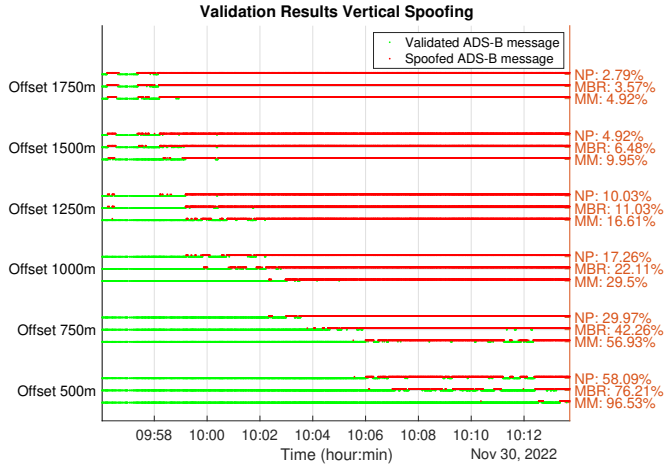

Fig. 6. Flight B: Spoofing detection results for vertical spoofing. Right hand side shows the percentage of messages validated for each hypothesis test. Left hand size shows the offset compared to the true ADS-B track

2) Flight C: Validation results show some irregularities in performance in figure 7 and 8. The cause of the rejection of messages is the bad estimation of the correct height and not the offset of the spoofed messages. This again is the result of a very high vertical dilution of precision.

C. Tuning Parameters

Table II shows the tuning variables in the PF that are used in generating the results.

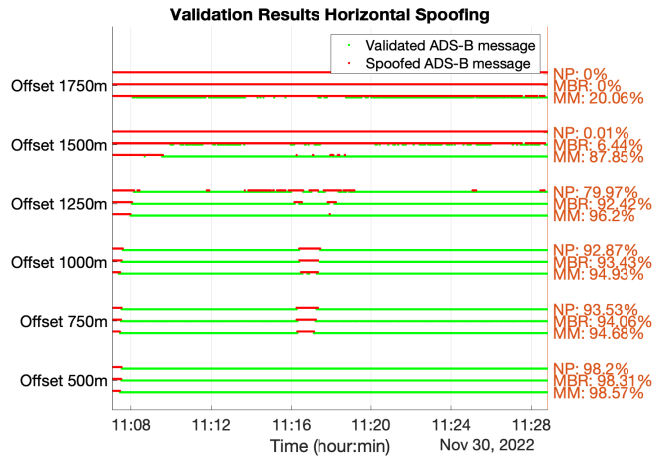

Fig. 7. Flight C: Spoofing detection results for horizontal spoofing. Right hand side shows the percentage of messages validated for each hypothesis test. Left hand size shows the offset compared to the true ADS-B track

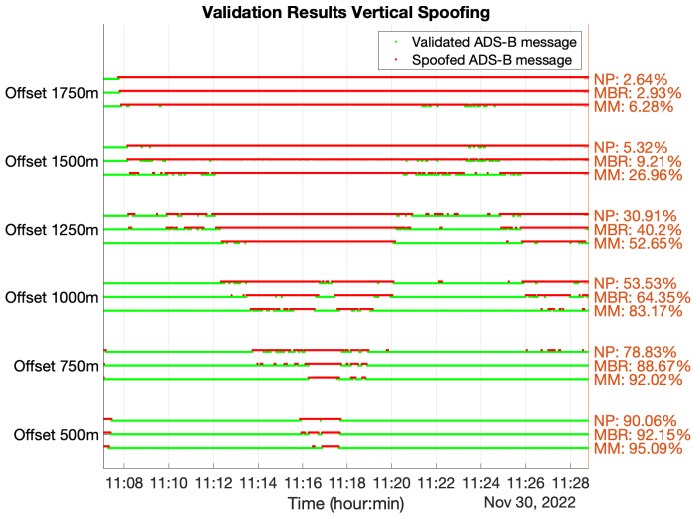

Fig. 8. Flight C: Spoofing detection results for vertical spoofing. Right hand side shows the percentage of messages validated for each hypothesis test. Left hand size shows the offset compared to the true ADS-B track

VI. Conclusion

Ambiguous TDOA measurements are used for ADS-B validation. This method can validate the ADS-B messages before a traditional TDOA system can even track the target. Validation can thus be done before the location of the target is determined independently. The ADS-B location message (if validated) can then already be used by ATC and the coverage of the TDOA / ADS-B system is increased from the area where four GSs receive a message, to the area there two GSs receive a message.

A likelihood ratio test is used to determine if the ADS-B message is spoofed. Determining a threshold value can be somewhat trivial, therefore, three different tests are explored to find which one is best suited. Results have shown that each test is capable of correct ADS-B validation. The Neyman-Pearson has the highest threshold generally, followed by the MBR and the Minmax. It must be noted that these obtained thresholds are completely tuning dependent. Each test in general is able to detect spoofed position messages from a range 750m to 1000m onwards. Again, here is must be noted that these results depend on the quality of the provided measurements. The test that is best suited completely depends on operator preference, availability of suited prior probabilities and reasonable costs that can associated with the possible decision errors.

Process noise Tuning			
location variance	$\sigma_x^2 = 7^2$	$\sigma_y^2 = 7^2$	$\sigma_z^2 = 4^2$
velocity variance	$\sigma_{vx}^2 = 1^2$	$\sigma_{vy}^2 = 1^2$	$\sigma_{vz}^2 = 0.5^2$
$p(\mathbf{x}_k, \mathcal{H}_1)$ **Tuning**			
location	$V_x = 220e^3$	$V_y = 523e^3$	$V_z = 21e^3$
velocity	$V_v = 225e^3$		
Hypothesis Test Tuning	**MBR**	**MM**	**NP**
π_0	0.75		
π_1	0.25		
C_{00}	0	0	
C_{01}	1	1	
C_{10}	1	1	
C_{11}	0	0	
P_{fa}			10^{-6}
PF	N_s	measurement std.	
	$5e^4$	$\sigma_v = 10^{-7}$	
ADS-B	Velocity var.		
	$\sigma_a^2 = 4^2$		

TABLE II
Tuning variables

References

[1] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication," Tech. Rep.

[2] W.-P. Air Force Base, "Exploiting the automatic dependent surveillance-broadcast system via false target injection," Tech. Rep.

[3] S. Amin, T. Clark, R. Offutt, and K. Serenko, "Design of a cyber security framework for ads-b based surveillance systems," in *2014 Systems and Information Engineering Design Symposium (SIEDS)*, 2014, pp. 304–309. DOI: 10.1109/SIEDS.2014.6829910.

[4] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can Cryptography Secure Next Generation Air Traffic Surveillance?" Tech. Rep.

[5] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ads-b security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3322–3334, 2019. DOI: 10.1109/JIOT.2018.2882633.

[6] S. Khan, J. Thorn, A. Wahlgren, and A. Gurtov, "Intrusion Detection in Automatic Dependent Surveillance-Broadcast (ADS-B) with Machine Learning," in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 2021-October, Institute of Electrical and Electronics Engineers Inc., 2021, ISBN: 9781665434201. DOI: 10.1109/DASC52595.2021.9594431.

[7] X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Detecting ADS-B Spoofing Attacks using Deep Neural Networks," Apr. 2019. [Online]. Available: http://arxiv.org/abs/1904.09969.

[8] J. Wang, Y. Zou, and J. Ding, "ADS-B spoofing attack detection method based on LSTM," *Eurasip Journal on Wireless Communications and Networking*, vol. 2020, no. 1, Dec. 2020, ISSN: 16871499. DOI: 10.1186/s13638-020-01756-8.

[9] W. Huygen, J. Sun, and J. Hoekstra, "ADS-B Signal Verification Using a Coherent Receiver," MDPI AG, Dec. 2021, p. 4. DOI: 10.3390/engproc2021013004.

[10] C. Reck, M. S. Reuther, A. Jasch, and L. P. Schmidt, "Verification of ADS-B positioning by direction of arrival estimation," *International Journal of Microwave and Wireless Technologies*, vol. 4, no. 2, pp. 181–186, Apr. 2012, ISSN: 17590787. DOI: 10.1017/S1759078712000086.

[11] M. Khalaf-Allah, "Particle filtering for three-dimensional tdoa-based positioning using four anchor nodes," *Sensors*, vol. 20, no. 16, 2020, ISSN: 1424-8220. DOI: 10.3390/s20164516. [Online]. Available: https://www.mdpi.com/1424-8220/20/16/4516.

[12] N. Xia and M. A. Weitnauer, "Tdoa-based mobile localization using particle filter with multiple motion and channel models," *IEEE Access*, vol. 7, pp. 21 057–21 066, 2019. DOI: 10.1109/ACCESS.2019.2897936.

[13] S. S. Blackman, *Multiple-Target Tracking with Radar Applications*. 610 Washington Street Dedham, MA 02026: Arteck House, Inc, 1986.

[14] H. V. Poor, *An Introduction to Signal Detection and Estimation (2nd Ed.)* Berlin, Heidelberg: Springer-Verlag, 1994, ISBN: 0387941738.