Design of Estimators with Integrity in the Presence of Error Model Uncertainty

Juan Blanch and Todd Walter

Stanford University

Abstract

We develop and evaluate a new type of estimator designed for applications with error model uncertainty – and more specifically where the error model uncertainty is defined following the Advanced RAIM framework). We first establish a theoretical lower limit on the achievable state estimation error bound and use this limit to bound the distance to optimality of the proposed estimator. For requirements on integrity and continuity on the order of 10^{-7}, and prior fault probabilities of 10^{-4} (values typical for ARAIM), we find that the error bounds obtained in this type of estimator are within 20% of the best possible achievable bounds for critical geometries.

1. INTRODUCTION

Fault detection and exclusion are key functions for positioning algorithms meant to provide high integrity error bounds or simply accurate positions in the presence of faulty measurements. It is well known that least square estimators are not optimal when the error model includes the possibility of faults affecting the measurements, as it is the case in RAIM for un-augmented GNSS, or radionavigation signals in cluttered environments. A least square estimator (or even a linear estimator) that includes an unbounded fault will result in an unbounded position error. To limit the growth of the position error, the effect of that measurement must be mitigated. This is the objective of fault detection and exclusion (FDE) algorithms. As indicated by their name, most available FDE algorithms are structured so that detection and exclusion are two distinct steps, after which a linear unbiased estimator (most often a least squares filter) is used (Lee et al, (1996), Blanch et al, (2010), Joerger et al, (2016), Blanch et al, (2017)). This approach works very well in many applications and is the basis for the standard approaches in RAIM and Advanced RAIM. It is however not guaranteed to be the best approach. The purpose of this paper is to develop estimators that are not constrained by this structure and to evaluate their potential benefits.

In our previous work (Blanch et al, (2021)), we described an estimator and its associated protection level that merges the fault detection and fault exclusion functions. A key contribution was the derivation of a protection level (PL) with an analytical proof of both integrity and continuity (or probability of alert) for the proposed estimator, which is non-linear. The estimator was applied to GNSS data collected on the ground with artificial faults and evaluated using a service volume model. Preliminary results suggested that this approach may improve upon the classical paradigm of FDE in at least three ways: it provides a better worst-case performance (in terms of protection level -50% reduction in typical ARAIM scenarios), it has a simpler logic, and the position solution tends to be smoother over time. The purpose of this work is to continue the development and evaluation of this new class of estimators as described below.

One of the methods to evaluate an estimator is by comparing the achieved PLs to those of an optimal estimator, or if not known, to a lower bound on the achievable PLs. We will therefore start by casting the search of the estimator as an optimization problem. This problem appears to be a very complex mini-max problem, for which there are no obvious solutions. (It is precisely this fact that has resulted in a very rich RAIM literature: if there was one known optimal solution, there would be no need to approach the problem from different angles.) We will use this formulation to develop lower bounds on the achievable performance of the optimal estimator. These lower bounds are a function of the geometry of the problem, the nominal error model, and the fault error models. These lower bounds on the PLs will allow us to evaluate the performance of our proposed estimators.

In the second section, we will simplify and generalize the approach we developed in Blanch et al, (2021). The key to the proposed approach was that rather than focus on a point estimate, we focus on estimating a region in space. It is relatively straightforward to design a region that contains the true position with high probability by using the principles of solution separation fault detection algorithms (Brenner, (1995), Blanch et al, (2010)). The difficult part is to design it such that it does not grow without limits when a fault is present. In Blanch et al, (2021), we showed that this can be done by carefully defining the region shape as a function of the measurement residuals in the case of a linear measurement equation and a Gaussian error model.

In the last section we evaluate the PL obtained in the second section against the lower bound established in the first section (which is a lower bound on the best PL that could be achieved by any estimator) for a set of representative integrity and continuity requirements.

2. MEASUREMENT MODEL

We consider the linear measurement model:

$$y = Gx + \varepsilon \tag{1}$$

where

y is the vector of measurements

x is the state to be estimated

ε is the measurement error

We note that this model can encompass scenarios where *y*, *x*, and *ε* refer to measurements, states, and measurement errors over time. (Equation (1) would be the batch formulation.)

Error model

In this work, we are looking for techniques that have a guarantee of performance, both for continuity and integrity. This necessarily means that we need to place limits on the uncertainty of the error model. A fully uncertain error model would allow state estimation errors that are both unbounded and undetectable.

One way to describe the uncertainty is by constraining the state error models to a set of hypotheses H_i that form a partition of the set of possible measurement errors and states. Each hypothesis may correspond to a different error characterization, and even the addition of new states. In addition, we assume that the error model follows one of hypotheses H_i with known probability p_i:

In the case of RAIM and ARAIM, a hypothesis corresponds to the addition of a new state:

$$\varepsilon = \eta + A_i b_i$$

where A_i is a known matrix, b_i is a vector of unknown biases with arbitrary entries, and η is Gaussian bounded, which means we may treat it as:

$$\eta \sim N\left(0, W^{-1}\right)$$

The case $A_i = 0$ is the fault free hypothesis H_0. Each of the other hypotheses corresponds to a range of error models spanning all the possible values of the added fault bias b_i.

3. LOWER BOUNDS ON ACHIEVABLE ESTIMATOR PERFORMANCE

Our goal in this section is to develop a lower bound on the achievable PL. After defining the objectives and constraints of the optimization problem, we will cast the search of the estimator as an optimization problem. Then, after deriving a key decomposition of the estimator, we will establish that any PL that meets the requirements is above a certain limit.

3.1 Probability of loss of integrity

The probability of loss of integrity can be expressed as the probability that two events happen:

- the position estimate exists, that is, *f(y)* is defined
- the position error exceeds a known limit *L*. In this paper, we will focus on the error in one coordinate (we will note *e* the corresponding vector).

The first condition means that we need to specify a region Ω in the space of measurements where the function *f* is defined. (As an example, in the case of RAIM for fault detection, Ω is the set of measurement vectors that result in the test statistic to be below the detection threshold.) We will label ε our not-to-exceed probability of loss of integrity. The integrity requirement can be expressed as:

$$P\left(\left|f(y)-e^T x\right|>L, y\in\Omega\right)\le\varepsilon \tag{2}$$

3.2 Probability of Alert

The probability of alert is the probability that no state estimate is deemed safe. With the definitions above, it is simply the probability that *f(y)* does not exist, or equivalently, that the vector of measurements *y* does not belong to the region Ω. If we label α our upper limit on the probability of alert, the constraint can be expressed as:

$$P\left(y\notin\Omega\right)\le\alpha \tag{3}$$

3.3 Estimator search

We can now formulate the search of the estimator *f* and the region Ω as the following minimization problem:

$$\begin{aligned}&\text{minimize } L\\ \text{subject to } &\begin{array}{l}P\left(\left|f(y)-e^T x\right|>L, y\in\Omega\right)\le\varepsilon\\ P\left(y\notin\Omega\right)\le\alpha\end{array}\end{aligned} \tag{4}$$

Even for simple threat spaces (for one fault hypothesis), the search of the optimal estimator *f* is an open problem.

3.4 Estimator decomposition

We start by stating a general property of the estimator *f*, where the only assumption we make that its estimate must be independent of the reference frame. Any such estimator *f* will have the following decomposition:

$$f\left(y\right)=s_{LS}{}^{T}y+f\left(Py\right) \tag{5}$$

where:

$$s_{LS}=WG\left(G^{T}WG\right)^{-1}e$$

$$P=W-WG\left(G^{T}WG\right)^{-1}G^{T}W$$

Equation (5) states that the estimator *f* is the sum of the least squares estimate and a function of the measurement residuals. We will be using the fact that the first term and the second term are uncorrelated (this is a well-known property of the least-squares error and its residuals). In the rest of this section, we provide a proof for (5).

Let us perform a change of variables as follows:

$$x'=x+\Delta x \tag{6}$$

In the new frame, the measurement equation is:

$$y'=Gx'+\varepsilon=G\left(x+\Delta x\right)+\varepsilon=y+G\Delta x \tag{7}$$

Because we have only changed the frame, we must have:

$$f\left(y'\right)=f\left(y\right)+e^{T}\Delta x \tag{8}$$

This equation expresses that the estimate in the new frame must be equal to the estimate in the old frame translated by Δx. Combining Equations (7) and (8), we obtain:

$$f\left(y+G\Delta x\right)=f\left(y\right)+e^{T}\Delta x \tag{9}$$

In other words, if we displace the state by Δx and everything else stays the same, we expect the estimate to be displaced by the same amount. Let us consider the following decomposition of the errors:

$$y=W^{-1}Py+G\hat{x}_{LS} \tag{10}$$

where $\hat{x}_{LS}=\left(G^{T}WG\right)^{-1}G^{T}Wy$. Combining Equation (9) and (10) we obtain Equation (5).

3.5 Lower bound on the achievable protection level: formulation

We will start by formulating the result of this section. Any solution *(f, L)* to the problem (4) is such that:

$$\frac{1}{2}\max_{i,j}\left(Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_i}\right)+Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_j}\right)\right)\sigma_{ss,0,ij}\leq L \tag{11}$$

Where

$\sigma_{ss,0.ij}$ is the standard deviation of the solution separation between the all-in-view least squares solution and the least squares solution that is fault tolerant to the fault hypothesis *i* and *j* [6]. (This is the least squares solution that adds *b_i* a and *b_j* as fault states)

Q is the tail cdf of a normal distribution, that is $Q(x) = \int_{x}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}t^2} dt$

The maximum is taken across all pairs (*i,j*) of fault hypotheses

It is significant, (and perhaps counterintuitive) that the lower achievable PL is related to the fault tolerant filter to the combination of two faults rather than the fault tolerant filter to one fault only. There is also a second lower bound that is a more direct consequence of (5):

$$Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_0}\right)\sigma_0 \le L \qquad (12)$$

3.6 Lower bound on the achievable protection level: proof

The proof for the inequality (11) is based on the design of fault hypotheses that meet certain criteria. We start by combining Equations (2) and (3) to obtain:

$$P\left(\left|f(y)-x_q\right|>L\right) \le \varepsilon+\alpha \qquad (13)$$

Writing the formula of total probability and expressing the fact that each of the terms must be bounded by the sum, we get:

$$P\left(\left|f(y)-x_q\right|>L \mid H_i\right) \le \frac{\varepsilon+\alpha}{p_i} \qquad (14)$$

(recall that p_i is the prior probability of hypothesis H_i)

We now re-write (14) by using Equation (5) and the measurement Equation (1), the estimation error under H_i is given by (note that we have dropped the subscript 'LS' to lighten notations):

$$f(y)-e^T x = s^T\varepsilon + s^T A_i b_i + f\left(W^{-1}Py\right) \qquad (15)$$

The first term is distributed as $N\left(0, e^T\left(G^T W G\right)^{-1} e\right)$ and independent of the remaining ones. For this reason, Equation (14) implies:

$$P\left(\left|s^T A_i b_i + f\left(W^{-1}Py\right)\right| > L \mid H_i\right) \le \eta_i \qquad (16)$$

with $\eta_i = 2\frac{\varepsilon+\alpha}{p_i}$

At this point, we are dealing with points in the parity space, so it is convenient to perform the usual change of variables:

$$z = UW^{-1}Py$$

so that $z \sim N\left(R_i b_i, I_{n-p}\right)$ where *p* is the length of *x* and $R_i = UW^{-1}PA_i$.

Let us now consider the regions Ω$_i$ defined by:

$$\Omega_i = \left\{ z \mid \left| s^T A_i b_i + f\left(z\right) \right| \le L \right\} \tag{17}$$

According to Equation (16) we have

$$P\left(z \in \Omega_i \mid H_i\right) \ge 1 - \eta_i \tag{18}$$

In the following steps we will place constraints on *b$_i$* and *b$_j$* so that $\Omega_i \cap \Omega_j \ne \varnothing$. The idea here is to get the two regions close enough to each other so that they need to overlap. To achieve this, we first solve the problem:

$$\min P\left(z \in \Omega_i \mid H_j\right)$$

$$P\left(z \in \Omega_i \mid H_i\right) = 1 - \eta_j \tag{19}$$

The solution to this is given by the Neyman-Pearson lemma. There exists a constant *c* such that:

$$\Omega_i = \left\{ z \mid \frac{p\left(z \mid H_i\right)}{p\left(z \mid H_j\right)} > c \right\} \tag{20}$$

Using the expression for the distribution of *z* conditioned on *H$_i$* or *H$_j$* and after some algebra, we deduce that there exists *K* such that:

$$\Omega_i = \left\{ z \mid z^T \frac{R_j b_j - R_i b_i}{\left| R_i b_i - R_j b_j \right|} \le K \right\} \tag{21}$$

This means that the region Ω$_i$ is defined by its projection over the unit vector $\frac{R_j b_j - R_i b_i}{\left| R_i b_i - R_j b_j \right|}$. The constraint in (19) gives us the equation:

$$P\left(z \in \Omega_i \mid H_i\right) = 1 - \eta_i = 1 - Q\left(K - \left(R_i b_i\right)^T \frac{R_i b_i - R_j b_j}{\left| R_i b_i - R_j b_j \right|} \right) \tag{22}$$

Similarly, we have:

$$P\left(z \in \Omega_i \mid H_j\right) = 1 - Q\left(K - \left(R_j b_j\right)^T \frac{R_i b_i - R_j b_j}{\left| R_i b_i - R_j b_j \right|} \right) \tag{23}$$

We now set this probability such that $P\left(z \in \Omega_i \mid H_j\right) > \eta_j$. We get the second equation:

$$\left(R_j b_j\right)^T \frac{R_j b_j - R_i b_i}{\left| R_i b_i - R_j b_j \right|} - K \le Q^{-1}\left(\eta_j\right) \tag{24}$$

Combining (22) and (24), we get the constraint on *b*b_i and b_j

$$\left|R_i b_i - R_j b_j\right| \le Q^{-1}\left(\eta_i\right) + Q^{-1}\left(\eta_j\right) \tag{25}$$

To recapitulate, we have found a constraint on b_i and b_j such that $P\left(z \in \Omega_i \mid H_j\right) > \eta_j$ no matter the shape of Ω_i and Ω_j. Since $P\left(z \in \Omega_j \mid H_j\right) = 1 - \eta_j$ it follows that we must also have $\Omega_i \cap \Omega_j \neq \varnothing$. Let us now choose a point *z* in $\Omega_i \cap \Omega_j$. For such a point we have (by definition) $\left|s^T A_i b_i + f(z)\right| \le L$ and $\left|s^T A_j b_j + f(z)\right| \le L$. This means that we must have

$$\left|s^T A_i b_i - s^T A_j b_j\right| \le 2L \tag{26}$$

This inequality is true if the constraint (25) is met. To find the largest lower limit on *L*, we solve the optimization problem:

$$\max\left|s^T\left(A_i b_j - A_j b_j\right)\right|$$

$$\text{Subject to } \left|R_i b_i - R_j b_j\right| \le Q^{-1}\left(\eta_i\right) + Q^{-1}\left(\eta_j\right) \tag{27}$$

We are now very close to our goal. Let us rewrite (27) with

$$A = \begin{bmatrix} A_i & 0 \\ 0 & A_j \end{bmatrix}, b = \begin{bmatrix} b_i \\ b_j \end{bmatrix}, K = Q^{-1}\left(\eta_i\right) + Q^{-1}\left(\eta_j\right)$$

We get

$$\max\left|s^T A b\right|$$

$$\text{Subject to } b^T A^T P A b \le K^2$$

This is a straightforward optimization problem (for example, it can be solved directly with a Lagrange multiplier for the constraint). The solution is given by

$$\max\left|s^T A b\right| = K\sqrt{s^T A\left(A^T P A\right)^{-1} A^T s} \tag{28}$$

It turns out that the term in under the square root is the standard deviation of the solution separation between the all-in-view least squares estimator s and the least squares estimator fault tolerant to A, s_A (Blanch et al, (2010), Joerger et al, (2016)), that is:

$$\max\left|s^T A b\right| = K\sqrt{\left(s - s_A\right)^T W^{-1}\left(s - s_A\right)} \tag{29}$$

(The Appendix includes a derivation that makes the link between these two expressions more apparent.) This concludes the proof of (11).

The proof for (12) is more straightforward. For any *z* we have:

$$P\left(\left|s_{LS}^T \varepsilon\right| > L \mid z, H_0\right) \le P\left(\left|s^T + f(z)\right| > L \mid z, H_0\right) \tag{30}$$

If we now integrate over z, we get:

$$P\left(\left|s_{LS}^T \varepsilon\right| > L \mid H_0\right) \le P\left(\left|s^T + f(z)\right| > L \mid H_0\right) \le \eta_0 \tag{31}$$

This inequality results directly in the lower bound (12).

4. ESTIMATOR DESIGN

In the previous section, we have established a lower bound on the achievable performance of an estimator meeting the integrity and continuity constraints expressed by (4) under the error model described above. In this section, we describe an estimator that meets those constraints and that appears to achieve a performance relatively close to the bound established above (Equation (11), at least for typical requirements (the values of *α* and *ε*).

The principles of the design of the estimator are the same as the ones described in Blanch et al, (2021). The main idea consists in focusing on the design of a function that defines a *region in the state space* instead of a point estimate. That is, we will define a function $y \mapsto \Gamma(y)$

The region $\Gamma(y)$ must:

- exist or not exceed a certain size with probability 1 - *α* (that is the continuity requirement)
- contain the true value of the state with probability 1 - *ε*

Compared to [6], we both simplify the approach and generalize it. Because of the new formulation, the Protection Levels are slightly reduced.

4.1 Fault tolerant position solutions

As in [6] and as suggested by the expression on the lower bound on the PL, a key element in the design of the estimator is the set of fault tolerant estimators $\hat{x}^{(i)}(y)$ corresponding to each of the fault modes *H*ᵢ, and also those tolerant to any two fault hypothesis *i* and *j*, which we will denote as $\hat{x}^{(ij)}(y)$. In most applications, these fault tolerant estimators will be least squares estimators, but they don't need to be. The only thing we need is that the probability of the estimation error exceeding a limit be calculable. For example, for a least-squares estimator (and the assumed error model) we know that:

$$P\left(x \notin \left[\hat{x}^{(i)} - K\sigma_i, \hat{x}^{(i)} + K\sigma_i\right] \mid H_i\right) = P\left(\left|x - \hat{x}^{(i)}\right| > K\sigma_i \mid H_i\right) = 2Q(K) \tag{32}$$

where σ_i is the standard deviation of the position error associated to the estimator $\hat{x}^{(i)}(y)$ (whose expression is known and given in Blanch et al, (2010)) (to simplify the notations, *x* now denotes one single coordinate).

4.2 Building blocks for region Γ

For each pairwise combination of fault modes *i* and *j* (this includes single hypotheses as well since *i* = 0 corresponds to the fault free hypothesis), we define the regions:

$$D_{ij}(L) = \left\{x' \mid \left|\hat{x}^{(ij)} - x'\right| \le L\right\} \tag{33}$$

(We add the prime symbol to stress the fact x in the definition above does not refer to the true value of the state). Because of (32), we have:

$$P\left(x \notin D_{ij}(L) \mid H_i\right) = 2Q\left(\frac{L}{\sigma_{ij}}\right) \tag{34}$$

4.3 Combining the blocks

For a given fault hypothesis *Hi*, any of the regions $D_{ij}\left(L\right)$ would be a good candidate as a building block for our region Γ. However, this would lead to an unbounded size in case of a fault (see [6]). Instead, for each *i*, we are going to consider the intersection of $D_{ij}\left(L\right)$ over the indices *j*:

$$\Delta_i = \bigcap_j D_{ij}\left(L\right) \tag{35}$$

Using the fact that $P\left(x \notin A \cap B\right) \leq P\left(x \notin A\right) + P\left(x \notin B\right)$, we get:

$$P\left(x \notin \Delta_i \mid H_i\right) \leq \sum_j P\left(x \notin D_{ij}\left(L\right)\right) \tag{36}$$

To be fault tolerant to any of the fault hypotheses, we define *Γ* as the union of the Δ_i. That is:

$$\Gamma = \bigcup_i \Delta_i \tag{37}$$

The probability of loss of integrity is bounded as follows:

$$P\left(x \notin \Gamma\right) = \sum_i p_i \cdot P\left(x \notin \Delta_i \mid H_i\right) \leq \sum_i p_i \cdot \sum_j P\left(x \notin D_{ij}\left(L\right)\right) \tag{38}$$

This is a key bounding result because it allows to compute the probability of loss of integrity. In the case of our Gaussian model (Equation (34)), we have:

$$P\left(x \notin \Gamma\right) = \sum_i p_i \cdot P\left(x \notin \Delta_i \mid H_i\right) \leq 2\sum_i \sum_j p_i \cdot Q\left(\frac{L}{\sigma_{ij}}\right) \tag{39}$$

4.4 Size of region Γ

Let us now examine the size of *Γ*. Let us choose two points *a* and *b* in *Γ*. There must be two indices *i* and *j* such that $a \in \Delta_i$ and $b \in \Delta_j$. By the definition (35), we have $\Delta_i \subset D_{ij}\left(L\right)$ and $\Delta_j \subset D_{ij}\left(L\right)$, therefore $a \in D_{ij}\left(L\right)$ and $b \in D_{ij}\left(L\right)$. According to (33), this means that $\left|a-b\right| \leq 2L$, and that the size of *Γ* is less than 2L. It is very important to note that the size of *Γ*, is bounded under all the hypotheses. If we therefore choose our estimate to be the midpoint of *Γ* , then *L* will correspond to the protection level.

4.5 Probability of Alert

With this approach, the probability of alert coincides with the probability that the region *Γ* is empty. Under hypothesis *Hi*, the probability that *Γ* is empty is bounded by the probability that the point $\hat{x}^{(i)}$ is not included. This probability is bounded as follows ([6]):

$$P\left(\hat{x}^{(i)} \notin \Delta_i \mid H_i\right) \leq 2\sum_j Q\left(\frac{L}{\sigma_{ss,i,ij}}\right) \tag{40}$$

where $\sigma_{ss,ij,i}$ is the standard deviation of the solution separation $\hat{x}^{(i)} - \hat{x}^{(ij)}$ (as given, for example, in Blanch et al, (2010)). The total probability of alert is bounded using the same decomposition as for the integrity (Equation(38)). We get:

$$P\left(\Gamma(y)=\varnothing\right)\leq 2\sum_i p_i\sum_j Q\left(\frac{L}{\sigma_{ss,ij,i}}\right) \tag{41}$$

In the general case, we have the upper bound:

$$P\left(\Gamma(y)=\varnothing\right)\leq 2\sum_i p_i\sum_j P\left(\hat{x}^{(i)}\notin D_{ij}\left(L\right)\right) \tag{42}$$

4.6 Protection Level Equations

Using Equation (39) and (41), sufficient conditions for the protection Level *L* are given by:

$$\begin{gathered} 2\sum_i\sum_j p_i\cdot Q\left(\frac{L}{\sigma_{ij}}\right)\leq\varepsilon \\ 2\sum_i p_i\sum_j Q\left(\frac{L}{\sigma_{ss,ij,i}}\right)\leq\alpha \end{gathered} \tag{43}$$

These equations slightly improve the *PL* as compared to Blanch et al, (2021) when considering the Gaussian error model. However, the biggest change is that these two equations can be generalized to other error models using the expressions (38) for the integrity and (42) for the continuity.

4.7 Summary of method to compute the protection level L and the estimate $\hat{x}$

1. Compute subset solutions and sub-subset solutions $\hat{x}^{(i)},\hat{x}^{(ij)}$ and their associated standard deviations (as well as solution separation deviations)
2. Determine *L* as the maximum of the solutions to Equations (43): this is the protection level
3. Determine *Γ* using Equation (37)
4. Find the center of Γ this is the estimator $f\left(y\right)$

4.8 List of exclusion candidates and list of fault modes

As pointed out in Blanch et al, (2021), the above equations are well adapted to the situation where the list of exclusion candidates coincides with the list of fault hypothesis. There are however scenarios where the list of exclusion candidates is a subset of the fault hypotheses that need to be monitored. This is typically the case when the probability of alert requirements is less stringent than the integrity risk requirement. In this paragraph, we generalize the approach to include this case in a more efficient way than in [6].

To do that, we first add a few more degrees of freedom to our construction of *Γ*. We define *J* as the set of indices corresponding to the subsets that are in the list of exclusion candidates [9]. We define

$$\Delta_i=\bigcap_j D_{ij}\left(L_{ij}\right)\text{ for } i\in J$$

$$\Delta_i=\bigcap_{j\in J} D_{ij}\left(L_{ij}\right)\text{ for } i\notin J$$

Using the same arguments as before, we have:

$$P\left(x \notin \Gamma\right) = \sum_i p_i \cdot P\left(x \notin \Delta_i \mid H_i\right) \leq 2\sum_{i \in J}\sum_j p_i \cdot Q\left(\frac{L_{ij}}{\sigma_{ij}}\right) + 2\sum_{i \notin J}\sum_{j \in J} p_i \cdot Q\left(\frac{L_{ij}}{\sigma_{ij}}\right) \tag{44}$$

We now examine the size of *Γ*. As before, if two points *a* and *b* are in *Γ*, there must be two indices *i* and *j* such that $a \in \Delta_i$ and $b \in \Delta_j$. If *i* or *j* are in *J*, then we have as before $\left|a-b\right| \leq L_{ij} + L_{ji}$. However, if neither are in *J*, we only have that for any *k* in *J*:

$$\left|a-b\right| \leq L_{ik} + L_{jk} + \left|\hat{x}^{(ik)} - \hat{x}^{(k)}\right| + \left|\hat{x}^{(jk)} - \hat{x}^{(k)}\right| \tag{45}$$

This inequality will enable the bounding of the size of $\Delta_i \cup \Delta_j$ under hypothesis H_k. Following an approach similar to the ones we user in Blanch et al, (2021), the requirement on the protection level L can be written as

$$2\sum_{i \in J} p_i \sum_j Q\left(\frac{L_{ij}}{\sigma_{ij}}\right) + 2\sum_{i \notin J} p_i \sum_{j \in J} Q\left(\frac{L_{ij} - T_{i,ij}}{\sigma_{ij}}\right) \leq \alpha$$

$$2\sum_{i \in J} p_i \sum_j Q\left(\frac{L_{ij}}{\sigma_{ss,i,ij}}\right) + 2\sum_{i \notin J} p_i \sum_{j \in J} Q\left(\frac{L_{ij} - T_{i,ij}}{\sigma_{ss,i,ij}}\right) + 2\sum_{i \notin J}\sum_{j \in J} Q\left(\frac{T_{i,ij}}{\sigma_{ss,i,ij}}\right) + \sum_{i \notin J} p_i \tag{46}$$

We note that to solve these equations, we must also determine the thresholds $T_{i,ij}$. For the details on a practical approach to determine them we refer the reader to [6].

5. EVALUATION OF THE ESTIMATOR

The benefits of a preliminary version of the proposed estimator compared to a standard approach have been demonstrated in [6] both with real GNSS data and in availability simulations. Our goal here is to evaluate the proposed estimator against the lower bound established in the first section. Let us first look at the order of magnitude of a solution to the equation that sets the PL (Equation (43)). It is very often the case (especially with critical geometries with respect to availability) that is dominated by one term. With this assumption, we can write that

$$L \simeq \max_{i,j} Q^{-1}\left(\frac{\varepsilon}{2p_i}\right)\sigma_{ij} \tag{47}$$

Based on Equation (11), we can define a simpler lower bound on the achievable PL

$$L_{low} = \max_{i,j} Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_i}\right)\sigma_{ss,0.ij} = \max_{i,j} Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_i}\right)\sqrt{\sigma_{ij}^2 - \sigma_0^2} \tag{48}$$

(The second equation is a consequence of the relationship $\sigma_{ij}^2 = \sigma_0^2 + \sigma_{ss,0,ij}^2$ (Blanch et al, (2010)).) It is also often the case that, for critical geometries, $\sigma_{ss,0,ij} \simeq \sigma_{ij}$ (because the second term dominates). With these approximations, we have:

$$\frac{L}{L_{low}} \simeq \frac{Q^{-1}\left(\frac{\varepsilon}{2p_i}\right)}{Q^{-1}\left(2\frac{\varepsilon+\alpha}{p_i}\right)}$$

Let is now look at typical values $\varepsilon = 10^{-7}$, $\alpha = 10^{-7}$, $p_i = 2\times10^{-4}$ (projected Galileo prior probability of constellation wide fault (ARAIM SARPS draft, (2021)). With these values the PL for the proposed estimator is within 20% of the lower bound on the achievable PL. The margin is further reduced if we add the effect of the dilution of both integrity and continuity due to temporal exposure (Milner et al, (2020)). As a point of comparison, the standard approach provides PLs that are 90% larger than the lower bound (we deduce this from the fact that the PLs are almost twice as large as the ones obtained using the proposed estimator).

Figure 1 shows the trace of the PL in one coordinate obtained with the proposed estimator, the corresponding lower bound, and the baseline H-ARAIM algorithm for an H-ARAIM scenario with the settings described in Blanch et al, (2021). We can observe the effect predicted above for the PL values: the lower bound is relatively tight (especially compared to the performance of the baseline algorithm).

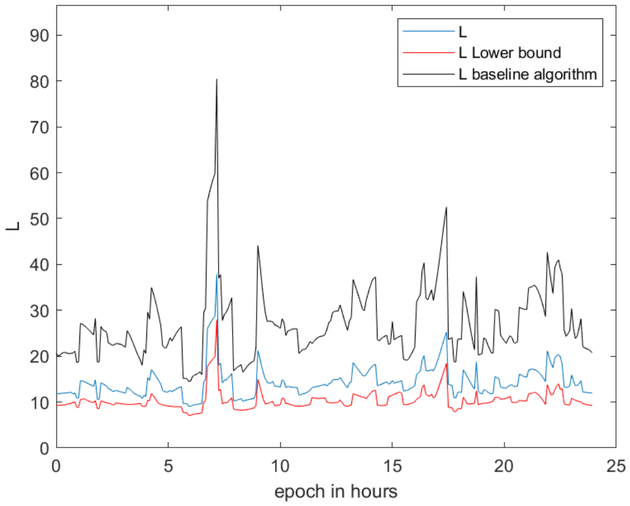

Figure 1 *Trace of the error bound L, the corresponding lower bound L_{low}, and the L computed in a standard FDE algorithm*

6. SUMMARY

In this work, we generalize and evaluate the design of a new type of estimator designed for applications with error model uncertainty. The approach is designed with the Advanced RAIM framework for the error model, but it can be used in more general settings. To evaluate the approach, we first establish a theoretical lower limit on the achievable state estimation error bound for any estimator. We then use this lower limit to bound the distance to optimality of the proposed estimator. For requirements on integrity and continuity on the order of 10^{-7}, and prior fault probabilities of 10^{-4} (values typical for ARAIM), we find that the error bounds obtained in this type of estimator are within 20% of the best possible achievable bounds for critical geometries.

ACKNOWLEDGEMENTS

We gratefully acknowledge the support of the FAA Satellite Navigation Team for funding this work under Memorandum of Agreement #: 693KA8-19-N-00015.

REFERENCES

Fifth Draft of ARAIM SARPs: Baseline Development Standard, ICAO Working Paper, Eighth meeting of the Joint Working Groups, November 2021.

Blanch, J., Walter, T., and Enge, P. (2010). RAIM with optimal integrity and continuity allocations under multiple failures. *IEEE Transactions on Aerospace and Electronic Systems*, *46*(3), 1235–1247. https://doi.org/10.1109/TAES.2010.5545186

Blanch J., Walter, T., and Enge, P.," Protection Levels after Fault Exclusion for Advanced RAIM," *NAVIGATION, Journal of The Institute of Navigation*, Vol. 64, No. 4, Winter 2017, pp. 505-513.

Blanch, J., Walter, T., Enge, P., "Theoretical Results on the Optimal Detection Statistics for Autonomous Integrity Monitoring", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 64, No. 1, Spring 2017, pp. 123-137.

Blanch, J., Walter, T. "A Fault Detection and Exclusion Estimator for Integrity Monitoring", *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, September 2021, pp. 1672-1686. https://doi.org/10.33012/2021.17954

Brenner, M. "Integrated GPS/Inertial Fault Detection Availability," in Proc. of the ION GPS-95, Palm Springs, 1995.

Joerger M., Pervan B. Fault detection and exclusion using solution separation and chi-squared ARAIM. IEEE Trans. Aerosp. Electron. Syst. 2016;52:726–742. doi: 10.1109/TAES.2015.140589.

Lee, Y., Van Dyke, K., DeCleene, B., Studenny, J., Beckmann, M., "SUMMARY OF RTCA SC-159 GPS INTEGRITY WORKING GROUP ACTIVITIES", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 43, No. 3, Fall 1996, pp. 307-362.

Milner, Carl, Pervan, Boris, Blanch, Juan, Joerger, Mathieu, "Evaluating Integrity and Continuity Over Time in Advanced RAIM," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, Oregon, April 2020, pp. 502-514.

https://gps.stanford.edu/resources/tools/maast

APPENDIX

To see how the solution separation comes in the problem (27), we first remark that

$$s^T Ab = \left(s - s_A\right)^T Ab \text{ for any } b \tag{49}$$

This because the estimator *s_A* is fault tolerant to *Ab*. In addition, because both and *s* and s_A are unbiased estimates of the state *x*, we have (without loss of generality, we will assume that W is the identity to lighten the notations)

$$\left(s - s_A\right)^T = \left(s - s_A\right)^T P \tag{50}$$

Re-writing (27), we get:

$$\begin{gathered} \max\left|\left(s - s_A\right)^T PAb\right| \\ \text{Subject to } \left|PAb\right| \leq K^2 \end{gathered} \tag{51}$$

Applying Cauchy-Schwarz to the vectors PAb and $s - s_A$, we get the upper bound on the objective function:

$$\left|\left(s-s_A\right)^T PAb\right| \le \left|s-s_A\right|\left|PAb\right| = K\left|s-s_A\right| \tag{52}$$

So we see how the solution separation appears. Now, because $s-s_A = sA\left(A^T PA\right)^{-1} A^T P$ (this can be obtained using the matrix inversion lemma Blanch et al. (2017b), it is in the span of PA, which means that equality is achieved for a certain *b*.