Distinguishing Aerial Intruders from Trajectory Data: A Model-Based Hypothesis-Testing Approach

David Petrizze, Kasra Koorehdavoudi, Mengran Xue, and Sandip Roy

Abstract—Motivated by security needs in unmanned aerial system (UAS) operations, an algorithm for identifying airspace intruders (e.g., birds vs. drones) is developed. The algorithm is structured to use sensed intruder velocity data from Internet-of-Things platforms together with limited knowledge of physical models. The identification problem is posed as a statistical hypothesis testing or detection problem, wherein inertial feedback-controlled objects subject to stochastic actuation must be distinguished by speed data. The maximum a posteriori probability detector is obtained, and then is simplified to an explicit computation based on two points in the sample autocorrelation of the data. The simplified form allows computationally-friendly implementation of the algorithm, and simplified learning from archived data. Also, the total probability of error of the detector is computed and characterized. Simulations based on synthesized data are presented to illustrate and supplement the formal analyses.

I. INTRODUCTION

Unmanned aerial systems (UAS) support diverse applications ranging from emergency response to package delivery and infrastructure monitoring [1]. The growing use of UASs (drones) is bringing forth significant concerns with regard to security and privacy, as evidenced by numerous high-profile disruption events [2]. One particular concern is that the airspace of secure facilities, such as airports, prisons, ports, or power plants, may be violated by drones, which may engage in destructive acts or extract sensitive information [3]. To address this concern, a range of technologies for detecting, classifying, and counteracting drone intrusions—known collectively as CounterUAS technologies—have been proposed. Although some of these technologies show promise, they have not been adopted in operational systems at a wide-scale. Key barriers to adoption include: 1) the difficulty of developing technologies that differentiate drones from other harmless intruders (e.g., birds) with high sensitivity and specificity; and 2) the high cost associated with deployment and persistent operation of many CounterUAS technologies.

New sensors deployed on Internet-of-Things (IoT) platforms hold great promise for enabling practical CounterUAS solutions. In particular, new sensing systems—such as small meta-materials-based radar systems—can permit relatively high-frequency sensing of UAS trajectories at a reasonable cost, although typically at lower resolutions than traditional systems. Meanwhile, IoT devices can allow distributed operation of these sensing technologies in the field at a reasonable cost. However, use of these IoT solutions for CounterUAS requires development and computationally-efficient algorithms for detection and identification of threats.

Our goal here is to explore algorithm development and deployment for IoT-based CounterUAS solutions, focusing particularly on the problem of distinguishing airspace or aerial intruders (e.g., birds vs. drones, or drones of different types) using trajectory data. The intuition underlying our algorithms is that many intruders, including both drones and birds, are inertial objects which seek to follow piecewise-constant velocity trajectories using feedback in the presence of ambient stochastic disturbances (e.g., wind). However, they differ in mass, and also in the strengths of the applied feedback (e.g., drones typically have more tightly regulated velocities than birds). In consequence, the ambient velocity responses of airspace intruders to the ambient disturbances are varied, which intrinsically allows differentiation.

Based on this intuition, we pose the problem of distinguishing airspace intruders of different types as a hypothesis testing or detection problem [4], where the data generated under each hypothesis is governed by a feedback-controlled dynamical model with different parameters. We then use the standard machinery for hypothesis testing to formally construct an optimal algorithm for differentiation. The main contribution of the study is to then use the special structure of the hypothesis testing problem to gain insight into the optimal detector, and permit computationally-attractive learning and deployment of the detector. Specifically, we demonstrate that the optimal detector reduces to a test on two points on the autocorrelation of the velocity; this form allows for scalable and easily deployable solutions on IoT platforms. Additionally, we show that the special problem structure allows for the computation of detection error probabilities, which serve as confidence levels on detection outcomes, and give insight into the data horizon needed for accurate differentiation of intruders.

From a methodological standpoint, the paper develops a way to distinguish feedback-controlled devices operating in noisy environments from sampled ambient time-series data. Specifically, our work shows how measured data can be
used in tandem with limited physical model knowledge to enable improved detection, computationally-friendly detector implementation, and error analysis of the detector.

The paper is organized as follows. The airspace intruder detector problem is presented in Section II. The optimal detector is developed in Section III, and then simplified to an explicit form in Section IV. The detection error is characterized in Section V. Finally, simulation examples are presented in Section VI. Note that two minor typos are present in the conference publication [5]; (18) and Table I have since been corrected.

II. MODELING AND PROBLEM FORMULATION

We pose the problem of distinguishing airspace intruders as a statistical hypothesis testing or detection problem, wherein trajectory data together with simplified model knowledge is used for detection.

Broadly, aerial intruders can be viewed as traversing a sequence of distinct flight segments while moving through the airspace (see Fig. 1). During each flight segment, the intruder can be modeled as seeking to follow a constant-velocity trajectory toward a waypoint, via application of a feedback control. Once the waypoint is reached, the intruder then continues along a different flight segment, with a different velocity (speed, direction) goal.

For this study, we assume that a sensing system (e.g., radar) obtains samples of the velocity profile, over a portion of the flight. Many recently developed low-cost sensing technologies, such as new lightweight radars and imaging technologies, are able to obtain relatively high frequency but low resolution data of this sort. In general, the measured profile will include data from one or more constant-velocity flight segments of the aerial intruder. Here, we consider the circumstance that data from only a single flight segment is available. Specifically, we consider using the deviation of the intruder’s speed from the mean speed in its direction of flight, which approximates the deviation from the reference or goal speed, to distinguish the intruder.

While a detector could be built by only considering measured speed data, incorporation of some model knowledge about intruder flight should allow for improved detection, and also perhaps allow more computationally friendly detector learning and use. With this in mind, a simplified mathematical model for the deviation of the intruder’s speed from the reference speed is considered. To permit an easier development, let us assume that there are two types of intruders indicated by the variable $I$, say $I = 1$ (e.g. bird) and $I = 2$ (e.g. drone). The intruder’s speed deviation from the reference is denoted as $x(t)$, and is modeled as arising from a feedback-controlled inertial object which is subject to a zero-mean white Gaussian disturbance. Specifically, the deviation is modeled as:

$$m_I \dot{x} = -k_I x + w,$$

where $I$ indicates the type of intruder, $m_I$ is the intruder’s mass, $k_I$ is a lumped feedback term which indicates the strength of the regulatory effort imposed by the intruder’s velocity control systems, and $w$ is a force disturbance (e.g. environmental force) which is modeled as a zero-mean white noise signal with intensity $q$ (i.e. the noise autocorrelation is $R_{ww}(t) = q\delta(t)$). This model is illustrated in Fig. 2.

A sensor (e.g. a radar system) is assumed to make measurements of an intruder’s velocity profile at sample times, from which the velocity deviation at these times can be computed. Thus, we assume that the measurement signal

$$y[k] = x(kT)$$

is available at times $k = 0, \ldots, k_f - 1$, where $T$ is the sampling interval, $k = 0$ corresponds to the first available velocity measurement, and $k_f$ measurements are available in total.

Our goal is to develop a method for distinguishing the type of an intruder, using the measurement signal $y[k]$. We formulate the problem of distinguishing the intruder type as maximum a posteriori probability (MAP) detection or hypothesis testing problem, wherein the most likely intruder...
type given the observation sequence is selected as the intruder type. Mathematically, the MAP detector $\hat{I}$ is given by:

$$\hat{I} = \arg\max_{i=1,2} \Pr(I = i | y[0], \ldots, y[k_f - 1]).$$  \hspace{1cm} (3)

We note that computation of the MAP detector requires prior probabilities of the intruder types, $\Pr(I = 1) = p$ and $\Pr(I = 2) = 1 - \Pr(I = 1) = 1 - p$. Alternately, absent priors, a varying threshold can be used to distinguish between the intruder types to tune sensitivity vs specificity; see [4]. We also seek to compute probability of error metrics for the detector, which are valuable both for providing real-time confidence intervals, and for overall performance evaluation of the detector.

Finally, it is noted that the model for an intruder’s speed deviation is a gross over-simplification, in that it does not capture any multi-time-constant dynamics of the intruder, nonlinearities such as wind drag, and structure in the spectrum of the disturbance. We deliberately use an over-simplified model because of the difficulty inherent to building and parameterizing detailed models of intruder dynamics. Thus, our approach is to use a condensed model of the physics – which captures the salient constraints on the physical dynamics resulting from inertia and regulation – together with data to get simple and hopefully robust rubrics for such a detector. Our analysis will show that the abstracted model yields a very simple sufficient statistic for detection, i.e. for field implementation of the technology for two reasons.

On the other hand, because CounterUAS technologies would be subject to delays and errors. Given these concerns, there is a significant motivation to pursue a simplified, explicit computation of the MAP detector.

**III. DETECTOR**

A formal expression for the MAP detector for distinguishing airspace intruders is developed in the following theorem, using the standard methodology for hypothesis testing. To present the result, we use the notation $y$ for the vector of observations used for detection, i.e. $y = (y[0], y[1], \ldots, y[k_f - 1])^T$.

**Theorem 1:** The MAP detector for the intruder-identification problem is given by:

$$\hat{I}(y) = \begin{cases} 1 & \text{for } y^T Q y \leq z \\ 2 & \text{otherwise} \end{cases}.$$  \hspace{1cm} (4)

Here, $Q$ is given by:

$$Q = \Sigma_1^{-1} - \Sigma_2^{-1},$$  \hspace{1cm} (5)

where $\Sigma_I$ is the covariance matrix governing the velocity observations of intruder type $I$. The $i,j$-th element of $\Sigma_I$ is:

$$(\Sigma_I)_{ij} = \frac{q}{2k_f m_I} e^{-\frac{k_f}{m_I} |T| i-j|} = \alpha_I |\rho_I|^{i-j},$$  \hspace{1cm} (6)

where $T$ is the sampling period, $q$ is the wind noise magnitude, $m_I$ is the intruder’s effective mass, $k_f$ is the intruder’s effective feedback gain, and $\rho_I = e^{-\frac{k_f}{m_I} |T|}$. Finally, the detector threshold $z$ is given by:

$$z = \ln \left( \frac{\Pr (I = 1)^2 |\Sigma_2|}{\Pr (I = 2)^2 |\Sigma_1|} \right).$$  \hspace{1cm} (7)

Proof: The observation sequence under each hypothesis is a zero mean Gaussian process, with different autocorrelation functions. The form of the hypothesis test derives readily from the joint Gaussian distribution of the observations under each hypothesis (see e.g. [4]). The covariance matrices can then be obtained from the statistical analysis of a first-order system driven by white noise.

Specifically, to derive the form of the MAP detector, the joint probability density function for the measurement sequence under each hypothesis (intruder type) is compared. Based on the Gaussian density function, the MAP detector specifies $\hat{I} = 1$ if the following expression holds:

$$\Pr (I = 1) e^{-\frac{1}{2} y^T \Sigma_1^{-1} y} > \Pr (I = 2) e^{-\frac{1}{2} y^T \Sigma_2^{-1} y},$$  \hspace{1cm} (8)

and specifies $\hat{I} = 2$ otherwise. This expression readily simplifies to give (4), (5), and (7).

The entries in the covariance matrix $\Sigma_{ij}$ follow from the statistical analysis of the dynamical model of the intruder (1). To characterize the covariance, we first note that the transfer function from the white noise drive to the velocity signal is given by:

$$X(s) = \frac{1}{W(s)} = \frac{1}{m_I s + k_f}.$$  \hspace{1cm} (9)

From the transfer function, it readily follows that the auto-correlation of the (stationary) velocity response is given by:

$$R_{vv}(\tau) = \frac{q}{2k_f m_I} e^{-\frac{k_f}{m_I} |\tau|}.$$  \hspace{1cm} (10)

Considering samples as specified by (2), it follows that the covariance matrix $\Sigma_I$ is given by [4].

**IV. SIMPLIFIED COMPUTATION OF THE DETECTOR**

The expression for the detector given in Theorem 1 allows for an algorithmic computation of the MAP hypothesis. However, the computation on its face is rather intensive, requiring inversion and computation of determinants for two dense covariance matrices whose dimensions grow with the number of samples. Further, the determinant and inverse calculations are prone to numerical instability unless a very high precision algorithm is used. Thus, these inversion and determinant computations may be computationally unattractive when they must be performed using low-cost hardware (e.g., a microcontroller). On the other hand, because CounterUAS technologies would typically be used in outdoor spaces with harsh environments, persistent transmission of data to a central server is also unappealing from an energy-use standpoint, and also may be subject to delays and errors. Given these concerns, there is a significant motivation to pursue a simplified, explicit computation of the MAP detector.

In addition to these computational challenges, the expression for the MAP detector in Theorem 1 also does not give intuition into how the measured data is processed for detection – the detector uses an apparently arbitrary quadratic form of the data. This lack of insight is also problematic for field implementation of the technology for two reasons.
First, the expression does not identify whether a small set of sufficient statistics can be used for detection; if such a set of sufficient statistics could be determined, this would simplify detector computation and also possibly allow for simplified learning of the detector if the model was unknown. By the same token, insight into the detector form may allow for more robust detection algorithms when model parameters are partially unknown or subject to error.

With these motivations, the interesting structure of $\Sigma_I$ is particularly appealing from a simplification standpoint. The following theorem demonstrates that the matrix inverse and determinant can be computed exactly, thus yielding a simple, explicit expression for the MAP detector.

**Theorem 2:** The MAP detector for the intruder-identification problem is given by:

$$I(y) = \begin{cases} 1, & a k_f R_{yy}(0) + b k_f R_{yy}(1) + c (\bar{y}_0^2 + \bar{y}_{k_f-1}^2) \leq z, \\ 2, & \text{otherwise} \end{cases}$$

where $R_{yy}(k)$ denotes the sample autocorrelation of the elements of $y$. The constants $a$, $b$, and $c$ are given as follows:

$$a = \frac{1 + \rho_1^2}{\alpha_1 (1 - \rho_1^2)} - \frac{1 + \rho_2^2}{\alpha_2 (1 - \rho_2^2)},$$

$$b = \frac{2 \rho_2}{\alpha_2 (1 - \rho_2^2)} - \frac{2 \rho_1}{\alpha_1 (1 - \rho_1^2)},$$

$$c = \frac{\rho_2^2}{\alpha_2 (1 - \rho_2^2)} - \frac{\rho_1^2}{\alpha_1 (1 - \rho_1^2)}.$$  

Similarly, $z$ is given by:

$$z = 2 \ln \left( \frac{\Pr(I = 1)}{\Pr(I = 2)} \right)$$

$$+ k_f \ln \frac{\alpha_2}{\alpha_1} + (k_f - 1) \ln \frac{1 - \rho_2^2}{1 - \rho_1^2}.$$  

**Proof:** $\Sigma_I$ is readily identified as a Kac-Murdock-Szego matrix $[6]$, with the following analytical inverse:

$$\Sigma_I^{-1} = \frac{1}{\alpha_I (1 - \rho_I^2)} \begin{bmatrix} 1 & -\rho_I & \ldots & 0 & 0 \\ -\rho_I & 1 + \rho_I^2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 + \rho_I^2 & -\rho_I \\ 0 & 0 & \ldots & -\rho_I & 1 \end{bmatrix}.$$  

and a determinant given by:

$$|\Sigma_I| = \alpha_I^{k_f} (1 - \rho_I^2)^{k_f-1}.$$  

From here, (11), (12), (13), and (14) follow by evaluating the detector expression: $y \in \Sigma_I^{-1} \Sigma_I^{-1} y$, and simplifying the result. The expression for $z$ in (15) follows in the same way.

The explicit expression for the detector clarifies the sufficient statistic needed for detection, and gives intuition into how aerial intruders can be distinguished. Specifically, the detector requires only two points in the sample autocorrelation: 1) the sample variance of the measurement signal $y$, and 2) the covariance between subsequent samples in the measurement signal (i.e., measurements with one time step delay between them), provided that the intruder’s persistent trajectory is measured over a sufficiently long horizon. (The detector also includes an "edge effect" which reflects measurement limits at the initiation and end of measurement, but these terms become negligible as $k_f$ increases.) Meanwhile, the threshold for detection, $z$, is determined by the masses and control gains of the intruders, together with the sampling interval and the *a priori* probabilities of each intruder type.

Noting that the detector threshold can be modified to trade off sensitivity and specificity, detection essentially depends only on calculation of the variance and a single-shift covariance of the data. The simple detector form reflects the fact that intruders are modeled as an inertial mass with a proportional feedback. Provided that intruders can be roughly modeled in this way, i.e. they have a dominant response time constant, then this simple detector may be expected to allow for effective differentiation from ambient data.

Importantly, a detector of this form can be learned without knowledge of system parameters and given inaccuracies in the model form, using training data. In particular, noting that the detector is based on a linear combination of two points in the autocorrelation, a detector can be built by computing these two points in archived measurements of the two intruder types. These statistics can then be presented on a scatter plot to identify the detection rule. Thus, an entirely data-theoretic implementation of the detector is possible, even though the approach takes advantage of the dynamical model structure or constraints of aerial intruders (i.e., inertia, presence of feedback).

**V. Detector Error**

We next seek to characterize the performance of the MAP detector, as measured by its probability of error. The error-probability calculation provides a means for giving confidence intervals around the detection goal, which indicates the fidelity of the estimate to users of the detector. The presentation of confidence intervals is important for field implementation of the technology, because manual intervention to resolve threats is often costly, and hence operations would benefit from an indication of detector fidelity prior to intervention. An analysis of the detector’s performance also gives insight into the amount of data required for differentiation of aerial intruders, and hence allows understanding of whether detection from ambient data is practical or not. Intuitively, the gap between the two covariance matrices $\Sigma_1$ and $\Sigma_2$, as well as the number of velocity samples $k_f$, should determine the probability of correctly distinguishing the intruder.

Per standard hypothesis-testing methodologies, two types of error probabilities may be of interest. First, the total *a priori* probability of error of the detector, i.e. $\Pr(I(y) \neq I)$, is of interest as an overall fidelity metric for the detector. We denote this total error probability by $\Pr(E_T)$, where $E_T$ is
the event that a misdetection occurs ($\tilde{I}(y) \neq I$). The total error probability is an indication of the effectiveness of the detector over repeated trials, and is a function of only the system’s parameters.

Second, the probability of mis-detection given a sequence of measurements, i.e. $Pr(I(y) \neq I | y)$, is of interest as a real-time confidence interval for a deployed detector. This conditional error probability can readily be computed in terms of the prior probabilities and the Gaussian observation-sequence probabilities, via an application of Baye’s rule.

### A. A Priori Detector Error

The total error probability does not allow for a closed-form expression. However, using analyses of quadratic forms of Gaussian random variables, a convenient form for numerical computation of the error can be derived. In addition, by then exploiting the specific system structure for our detection problem, the factors influencing the detection probability also can be characterized, and some structural insight can be gained into the detector performance. The expression that allows for numerical computation of the total error probability is presented in the following theorem.

**Theorem 3:** The total probability of error for the detector can be computed as:

$$Pr(E_T) = \frac{Pr(I = 2) F_Z (Q, \Sigma_2, z)}{Pr(I = 1)[1 - F_Z (Q, \Sigma_1, z)]},$$

(18)

where $Q$, $\Sigma_1$, and $\Sigma_2$, and $z$ are defined in the presentation of the detector (Theorems 1 and 2). The term $F_Z(Q, \Sigma, z)$, a numerically-computed inverse Fourier transform, is given by:

$$F_Z(Q, \Sigma, z) = \frac{1}{2} - \sum_{i=0}^{N} \frac{\text{Im} \left[ \phi \left( \Delta \left( i + \frac{1}{2} \right) \right) e^{-j \Delta \left( i + \frac{1}{2} \right)} \right]}{\pi \left( i + \frac{1}{2} \right)},$$

(19)

where $j$ is the imaginary constant, and $\phi(\omega)$ is defined as:

$$\phi(\omega) = \prod_{k=1}^{k_f} (1 - 2j \omega \lambda_k)^{-\frac{1}{2}}.$$  

(20)

Here, $\lambda_k$ is the $k$th eigenvalue of the matrix product $Q \Sigma$.

**Proof:** Assume that $y$ contains $k_f$ velocity samples with zero mean, and that $Q$, $z$, $\Sigma_1$, and $\Sigma_2$ characterize a detector as defined by Section III. Intuitively, the probability that the detector concludes falsely is given by:

$$Pr(E_1) = Pr(y^T Q y \leq z \cap I = 2),$$

and

$$Pr(E_2) = Pr(y^T Q y > z \cap I = 1).$$

Here, $Pr(E_1)$ and $Pr(E_2)$ denote the probability of the detector misidentifying intruder types 1 and 2, respectively. Clearly, $Pr(E_T) = Pr(E_1) + Pr(E_2)$, and through simple manipulation, we can write $Pr(E_T)$ in terms of $Pr(y^T Q y \leq z | I = ...)$.

$$Pr(E_T) = \frac{Pr(I = 2) Pr(y^T Q y \leq z | I = 2) + Pr(I = 1)[1 - Pr(y^T Q y \leq z | I = 1)]}{Pr(I = 1)[1 - Pr(y^T Q y \leq z | I = 1)]}$$

We can interpret the above conditional probability expression in terms of the CDF of the random variable $Z$, where $Z = Y^T Q Y$, and the random vector $Y$ is Gaussian distributed with covariance $\Sigma_I$. This yields (18), and hence the notation $F_Z$.

From (17), $Z$ is observed to have a generalized chi-squared distribution, with a characteristic function defined by (20). The result follows from application of (8).

To ensure that (19) is accurate, the constants $N$ and $\Delta$ must be chosen appropriately to ensure that an accuracy threshold $E$ (where $0 < E < 1$) is met. The threshold indicates the maximum deviation between the true and computed error due to truncation (selection of $N$) and resolution (selection of $\Delta$) inaccuracies. To achieve this accuracy level, we claim that it is sufficient to assign

$$\Delta = \frac{2\pi t}{\ln(\theta) - \ln \left( \frac{E}{2} \right)},$$

(21)

and

$$N = \left[ \frac{1}{2\Delta |\lambda_{\min}|} \left( \frac{\pi E k_f}{4} \right)^{-\frac{2}{\Delta}} \right],$$

(22)

where $\theta$ is defined as:

$$\theta = \max \left\{ e^{zt} \prod_{k=1}^{k_f} (1 + 2t \lambda_k)^{-\frac{1}{2}}, e^{-zt} \prod_{k=1}^{k_f} (1 - 2t \lambda_k)^{-\frac{1}{2}} \right\}.$$  

(23)

Here, $t$ is chosen such that $0 < t < \frac{1}{2|\lambda_{\max}|}$; $\lambda_{\min}$ and $\lambda_{\max}$ represent the $\lambda_k$ with minimum and maximum magnitude, respectively.

To justify the bound on $N$, we notice that the sum’s truncation error, $E$, is given by:

$$E = \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \left| \phi \left( \left( k + \frac{1}{2} \right) \Delta \right) e^{-j \left( k + \frac{1}{2} \right) \Delta z} \right|.$$  

(24)

By the triangle inequality, we know that:

$$E \leq \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \left| \phi \left( \left( k + \frac{1}{2} \right) \Delta \right) e^{-j \left( k + \frac{1}{2} \right) \Delta z} \right|.$$  

(25)

Considering the maximum possible magnitude of the expression inside the absolute value, we similarly find:

$$E \leq \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \left| \phi \left( \left( k + \frac{1}{2} \right) \Delta \right) \right|.$$  

(26)

Substituting $\phi(u)$, we have:

$$E \leq \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \left| \prod_{i=1}^{k_f} (1 - 2j u \lambda_i)^{\frac{1}{2}} \right| \prod_{i=1}^{k_f} (1 - 2j u \lambda_i)^{\frac{1}{2}}.$$  

(27)

$$= \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \left| \prod_{i=1}^{k_f} (1 - 2j u \lambda_i) \right|^{\frac{1}{2}}.$$  

(28)

where $u = \left( k + \frac{1}{2} \right) \Delta$. Note that in our case, $Q$ is symmetric, and thus each $\lambda_i$ is real. By ignoring the real component, the
magnitude of the denominator in each term of the product will strictly decrease, meaning:

\[ E \leq \sum_{k=N+1}^{\infty} \frac{1}{\pi(k + \frac{1}{2})} \prod_{i=1}^{k_f} (2u |\lambda_i|)^{-\frac{1}{2}}. \]  

(29)

By reducing each \( \lambda_i \) to the \( \lambda_i \) with the smallest magnitude (\( \lambda_{\min} \)), the denominator will again decrease, so we find:

\[ E \leq \sum_{k=N+1}^{\infty} \frac{(2u |\lambda_{\min}|)^{-k_f}}{\pi(k + \frac{1}{2})}. \]  

(30)

Substituting for \( u \), we are left with:

\[ E \leq \frac{1}{\pi} (2\Delta |\lambda_{\min}|)^{-\frac{k_f}{2}} \sum_{k=N+1}^{\infty} \left( k + \frac{1}{2} \right)^{-\frac{k_f}{2} - 1}. \]  

(31)

We can yet again reduce the denominator in each term of the sum to find:

\[ E \leq \frac{1}{\pi} (2\Delta |\lambda_{\min}|)^{-\frac{k_f}{2}} \sum_{k=N+1}^{\infty} k^{-\left(\frac{k_f}{2} + 1\right)}, \]  

where the infinite sum is readily identified as a (convergent) p-series. We can bound this sum with the appropriate integral as follows:

\[ E \leq \frac{1}{\pi} (2\Delta |\lambda_{\min}|)^{-\frac{k_f}{2}} \int_{K}^{\infty} \tau^{-\left(\frac{k_f}{2} + 1\right)} d\tau \]  

(34)

\[ = \frac{1}{\pi} (2\Delta |\lambda_{\min}|)^{-\frac{k_f}{2}} \frac{2}{k_f} N^{-\frac{k_f}{2}} \]  

(35)

\[ = \frac{2}{k_f \pi} (2\Delta |\lambda_{\min}|)^{-\frac{k_f}{2}} \]  

(36)

Finally, we can solve for \( N \) in terms of a given upper bound on the error, \( E_{\text{upper}} \):

\[ N = \left[ \frac{1}{2\Delta |\lambda_{\min}|^2} \left( \frac{k_f \pi}{2} E_{\text{upper}} \right)^{-\frac{2}{k_f}} \right]. \]  

(37)

To justify the bound on \( \Delta \), we work from the following expression for the resolution inaccuracy which is developed in [3]:

\[ E = \max \left\{ \Pr \left( Z < z - \frac{2\Delta}{k} \right), \Pr \left( Z > z + \frac{2\Delta}{k} \right) \right\}. \]  

(38)

It turns out to be relatively straightforward to find \( \Delta > 0 \) so as bound this quantity, through the use of the Chernoff bounds.

We know that \( Z \)'s moment generating function, \( M_Z(t) \), is strictly positive and real valued for \( t \in (T_1, T_2) \), where the range \( (T_1, T_2) \) contains the origin. Hence, the Chernoff bounds for each tail probability are given by:

\[ \Pr \left( Z < z - \frac{2\Delta}{k} \right) \leq M_Z(s) e^{-s(z - \frac{2\Delta}{k})} \text{ for } T_1 < s < 0 \]  

(39)

\[ \Pr \left( Z > z + \frac{2\Delta}{k} \right) \leq M_Z(t) e^{-t(z + \frac{2\Delta}{k})} \text{ for } 0 < t < T_2. \]  

(40)

The quantity \( E \) will thus be bounded by the respective bounds for each tail as follows:

\[ E \leq \max \left\{ M_Z(s)e^{-s\left(z - \frac{2\Delta}{k}\right)}, M_Z(t)e^{-t\left(z + \frac{2\Delta}{k}\right)} \right\}. \]  

(41)

Substituting \( M_Z(t) \), we find:

\[ E \leq \max \left\{ e^{\frac{2\Delta}{k}} e^{-zs} \sum_{i=1}^{k_f} (1 - 2s\lambda_i)^{-\frac{1}{2}}, \right. \]

\[ \left. e^{-\frac{2\Delta}{k}} e^{-zt} \sum_{i=1}^{k_f} (1 - 2t\lambda_i)^{-\frac{1}{2}} \right\}. \]  

(42)

From here, let \( t = -s \), suitably chosen such that the condition on \( M_Z(t) \) is satisfied. (For example, let \( t = \frac{1}{4\lambda_{\max}} \), where \( \lambda_{\max} \) is the \( \lambda_i \) with the largest magnitude.) This substitution reduces our expression for \( E \) to the following:

\[ E \leq \theta e^{-\frac{2\Delta}{k}} := E_{\text{upper}}, \]  

(43)

where \( \theta \) is defined as:

\[ \theta = \max \left\{ e^{zs} \sum_{i=1}^{k_f} (1 + 2t\lambda_i)^{-\frac{1}{2}}, e^{-zt} \sum_{i=1}^{k_f} (1 - 2t\lambda_i)^{-\frac{1}{2}} \right\}. \]  

(44)

Once \( \theta \) has been computed, equation [43] can be used to compute \( \Delta \) in terms of an upper bound on error, \( E_{\text{upper}} \), as follows:

\[ \Delta = \frac{2mt}{\ln(\theta) - \ln(E_{\text{upper}})}. \]  

(45)

As demonstrated via simulation in section [VI] Theorem 3 provides an appealing method for computing the total probability of error of the airspace-intruder detector. Also of importance, the theorem characterizes the factors that influence the total error probability. Crucially, the theorem highlights that the detector error probability is dependent on the eigenvalues of the matrix products \( Q\Sigma_1 \) and \( Q\Sigma_2 \). However, we notice that \( Q\Sigma_1 = (\Sigma_1^{-1} - \Sigma_1^{-1})\Sigma_1 = I - Sigma_2^{-1}\Sigma_1 \), and similarly \( Q\Sigma_2 = I - \Sigma_1^{-1}\Sigma_2 \). With some effort, it can be seen that the rows of \( \Sigma_1^{-1}\Sigma_2 \) are related to the deconvolution of the impulse response of the type 2 intruder from that of the type 1 intruder. This matrix is close to the identity matrix if the two impulse responses are similar, which is the case if both the ratio and product of the control gain and mass are similar. In this case, \( Q\Sigma_1 \) and \( Q\Sigma_2 \) are nearly zero, and it follows immediately that the error probability is equal to the a priori. Meanwhile, if the impulse responses differ significantly (equivalently, their spectra are more distinct), the error probability decreases quickly with the number of samples \( k_f \).

### B. Detector Error Given Measurements

In addition to knowing the total probability of error, it is useful to know the probability of error given some measured velocity sequence \( y \). This probability, as well as an expression for the likelihood ratio for the alternate hypothesis, is stated in the following theorem:
Theorem 4: For a sequence of velocity deviation measurements in \( y \), the probability that the detector has concluded incorrectly is given by:

\[
\Pr \left( I \neq \hat{I} \mid Y = y \right) = \left( 1 + \frac{1}{r} \right)^{-1},
\]

(46)

where \( r \) is the probability ratio for the alternate hypothesis, defined by:

\[
r = e^{-\frac{1}{2}z - y^T Q y},
\]

(47)

Here, \( Q \) and \( z \) are defined in the specification of the detector (Theorem 1).

Proof: Assume \( y \) is given, having originated from the intruder model. Let \( Q \) and \( z \) be defined as in the presentation of the detector (Section III), and consider the likelihood ratio of hypothesis 1 to hypothesis 2. With some effort, it can be shown from the intruder distributions [5], that this ratio is given by:

\[
\frac{\Pr \left( I = 1 \right) \Pr \left( Y = y \mid I = 1 \right)}{\Pr \left( I = 2 \right) \Pr \left( Y = y \mid I = 2 \right)} = r_1 = e^{-\frac{1}{2} \left( y^T Q y - z \right)}.
\]

(48)

Here, we restrict \( y \) to that satisfying \( y^T Q y > z \), because \( r_1 \) is considered only when \( \hat{I} = 2 \) (i.e. hypothesis 2 is more likely). For the case where \( \hat{I} = 1 \), we find the opposite ratio, \( r_2 \), to be the following:

\[
r_2 = e^{-\frac{1}{2} \left( z - y^T Q y \right)},
\]

(49)

which is similarly valid only for \( y^T Q y \leq z \). Thus, we can write:

\[
r = e^{-\frac{1}{2} \left| y^T Q y - z \right|},
\]

(50)

where \( r \) is interpreted as the likelihood ratio of the opposite hypothesis, for all \( y \in \mathbb{R}^k \).

To determine the probability of error given \( y \), consider the case where \( I = 1 \) and \( \hat{I} = 2 \). We know from Bayes’ theorem that

\[
\Pr \left( I = 1 \mid Y = y \right) = \frac{\Pr \left( I = 1 \right) \Pr \left( Y = y \mid I = 1 \right)}{\Pr \left( Y = y \right)} = \frac{\Pr \left( I = 1 \right) \Pr \left( Y = y \mid I = 1 \right)}{\Pr \left( Y = y \mid I = 2 \right)} \Pr \left( Y = y \mid I = 2 \right).
\]

(51)

Through simple manipulation, it can be shown that

\[
\Pr \left( I = 1 \mid Y = y \right) = \left( 1 + \frac{\Pr \left( I = 2 \right) \Pr \left( Y = y \mid I = 2 \right)}{\Pr \left( I = 1 \right) \Pr \left( Y = y \mid I = 1 \right)} \right)^{-1} = \left( 1 + \frac{1}{r_2} \right)^{-1}.
\]

(52)

Similarly, for the case where \( I = 2 \) and \( \hat{I} = 1 \), we find:

\[
\Pr \left( I = 2 \mid Y = y \right) = \left( 1 + \frac{1}{r_1} \right)^{-1}.
\]

(53)

As in the formulation of \( r \), (52) and (53) are valid for the same complementary sets of \( y \), and hence the probability of detection error for all \( y \in \mathbb{R}^k \) can be written in terms of \( r \):

\[
\Pr \left( I \neq \hat{I} \mid Y = y \right) = \left( 1 + \frac{1}{r} \right)^{-1}.
\]

(54)

Table 1: Table of Simulation Parameters.

| Parameter | Value |
|-----------|-------|
| \( k_1 \) | 1     |
| \( k_2 \) | 3     |
| \( m_1 \) | 1     |
| \( m_2 \) | 1     |
| \( q \)  | 1     |
| \( k_f \) | 20    |
| \( T \)  | 0.5   |
| \( \Pr \left( I = 1 \right) \) | 0.5   |
| \( \Pr \left( I = 2 \right) \) | 0.5   |

VI. Examples

Simulations of the detector and error-probability calculation were undertaken for a case study, in which velocity measurement data of two intruder types (birds and drones) was synthesized according to [1]. The parameters for the simulations are shown in Table 1.

The MAP detector has been implemented on the synthesized bird-drone data. Several results are shown. First, the implementation of the detector is illustrated, through comparison of the data test (left side of Equation 4) with the threshold \( z \), for Monte-Carlo-generated trials of bird and drone data.

Fig. 3. The implementation of the MAP detector is illustrated. Specifically, the data test is compared with the detector threshold for trial bird and drone data, which have been synthesized according to the \( a \) priori probabilities and dynamic model. The detector effectively distinguishes the two types of intruders.

Second, real-time detection is illustrated, through application of the detector to streamed data over increasing horizons. In this example, the detector converges to the correct hypothesis after a horizon of \( k_f = 12 \). It is noted that an example requiring a longer horizon for convergence is included for illustrative purposes: in most cases, convergence was achieved within \( k_f = 7 \) samples.
Fig. 4. Application of the detector to streaming data is illustrated. The detector reaches correct hypothesis (intruder type) after $k_f = 12$ samples.

Fig. 5. After several thousand trials, measured error is shown to converge to the computed error.

Third, we compared the proportion of errors in repeated Monte Carlo trials to the expected total error as specified in Theorem 3, as a means to check the formal error calculation. The result after several thousand trials is shown in Figure 5: the total error probability as well as the error probability for each conclusion are shown. The error probability as computed from Monte Carlo simulations over a long horizon matches the exact computation.

Fourth, we illustrate the total probability of error as $k_1, m_1$ are held constant, and $k_2, m_2$ are varied, in order to get an idea for the feasibility of detection for a given intruder model pair. It can be seen that a (ratiometric) difference in $m$ improves detection fidelity more than that same difference in $k$. Additionally, it can be seen that when the time constant characterizing a drone ($m_2/k_2$) becomes significant relative to the sampling rate, it plays less of a role in detection than does a difference in the product of $k$ and $m$. This is intuitive, as aliasing will naturally play an integral role in the efficacy of the detector.

Fig. 6. Detection error according to the relative ratios and products of $k$ and $m_2$, is illustrated on a log scale.

Finally, we computed the detector’s error probability as a function of $k_f$, to get an preliminary idea of how the detector’s performance improves as the number of samples is increased. The plot shows an exponential decrease in the error probability with the horizon $k_f$, which suggests that a modest number of points can be used for reliable detection. In this sense, the detection approach appears to be promising for allowing robust differentiation of airspace intruders with different characteristics, such as drones and birds.

REFERENCES

[1] K. Valvanis and G. Vachtsevanos, Eds., Handbook of Unmanned Aerial Vehicles. Dordrecht: Springer Netherlands, 2015, vol. 1.
[2] T. Humphreys, “Statement on the security threat posed by unmanned aerial systems and possible countermeasures,” 2015.
[3] G. Herrera, J. Dechant, E. Green, and E. Klein, “Technology trends in small unmanned aircraft systems (suas) and counter-uas: A five year outlook,” no. IDA-P-8823, H-17-000624, 2017.
[4] A. Papoulis and S. Pillai, Probability, Random Variables, and Stochastic Processes. Tata McGraw-Hill Education, 2002.
[5] D. Petrizze, K. Koorehdavoudi, M. Xue, and S. Roy, “Distinguishing aerial intruders from trajectory data: A model-based hypothesis-testing approach.” American Control Conference, 2021.
[6] M. Kac, W. L. Murdock, and G. Szegö, “On the eigen-values of certain hermitian forms,” Journal of Rational Mechanics and Analysis, vol. 2, pp. 767–800, 1953. [Online]. Available: http://www.jstor.org/stable/24900353
[7] A. C. Rencher and G. B. Shaalje, Linear Models in Statistics. John Wiley & Sons, Ltd, 2007, ch. 5, pp. 117–119.
[8] R. B. Davies, “Numerical inversion of a characteristic function,” Biometrika, vol. 60, no. 2, pp. 415–417, 1973. [Online]. Available: http://www.jstor.org/stable/2334555