A Closed Form for False Location Injection under Time Difference of Arrival

Lauren M. Huie*† lauren.huie@rl.af.mil
Mark L. Fowler† mfowler@binghamton.edu
*Air Force Research Laboratory, Rome, NY 13441
† Department of Electrical Engineering, State University of New York at Binghamton, Binghamton, NY 13902

***Abstract*—We consider a sensor network, which in the presence of a rogue sensor, is tasked with estimating emitter location under the time difference of arrival (TDOA) method. The rogue seeks to maximally degrade estimation accuracy by injecting a single false report of sensor position. Our closed form solution gives a set of false positions that minimize the network's Fisher Information Matrix (FIM). We find that the rogue sensor should report a false position along the vector pointing from the emitter to its valid paired sensor. Further, a method for finding the false location that not only minimizes the FIM but is also robust to the location network's ability to detect and reject erroneous TDOA measurements is developed.**

***Index Terms*—Emitter Location, Time Difference of Arrival (TDOA), Fisher Information, False Data, Information Injection**

I. Introduction

One sensor network estimation task of particular interest is estimating the location of an emitter. Since sensor networks communicate using a shared wireless medium it is possible for a rogue sensor to infiltrate the network and thus influence estimation accuracy. This work considers the problem of a rogue sensor injecting a single false position into a network tasked with estimating the location of an emitter. Although methods exist for securing sensor networks i.e. encryption, such unauthorized access can still occur [1].

A common method for locating an emitter is the time and frequency difference of arrival (TDOA/FDOA) method [2], [3], where the estimation accuracy is assessed using the Fisher Information Matrix (FIM) [4]. A number of applications using TDOA/FDOA and the FIM have been considered such as sensor pairings [5], fault tolerant vehicle guidance [6], and bit allocation [7]. Recently, the problem of a rogue sensor infiltrating an emitter location network has also been investigated in [8]. However, due to the complexity of the FIM under TDOA/FDOA, previous approaches [5]–[8] have relied on numerical methods which lack an analytic solution.

In this work we focus on the TDOA method as a natural starting point towards the development of an analytic solution for the rogue sensor problem. Under the TDOA method, sensors are typically paired and each pair generates its own TDOA estimate. These estimates are then combined to form an estimate of the emitter's location. In this scenario, we assume that a rogue sensor corrupts a single pair of sensors by pairing with a valid sensor. Further, we assume that the rogue knows the location of the emitter and the positions of the other valid sensors in the network. This is reasonable as this information is generally shared within a network for use in location processing.

*This work is supported in part by AFOSR LRIR 09RI02COR.

The main contributions of this work are:

1) A closed form solution for the problem of a rogue injecting a single false location into a network tasked with estimating an emitter's location under TDOA.

2) A method for finding the false sensor position that not only minimizes the FIM but is also robust to the location network's ability to detect and reject erroneous TDOA measurements.

This is significant because previous work lacks an analytic solution for the rogue problem.

II. Background

In order to assess location accuracy, the Fisher Information Matrix (FIM) [4] is used as the distortion criteria. Let $\hat{\mathbf{s}} = \mathbf{s}(\boldsymbol{\theta}) + \mathbf{n}$ represent the received noisy vector comprised of a deterministic signal vector $\mathbf{s}(\boldsymbol{\theta})$ parameterized by vector $\boldsymbol{\theta}$ and corrupted by Gaussian noise $\mathbf{n}$, with covariance matrix $\mathbf{C}$. The FIM is given by

$$\mathbf{J}(\boldsymbol{\theta}) = \frac{\partial \mathbf{s}^T(\boldsymbol{\theta})}{\partial(\boldsymbol{\theta})}\mathbf{C}^{-1}\frac{\partial \mathbf{s}(\boldsymbol{\theta})}{\partial(\boldsymbol{\theta})} \tag{1}$$

where $\frac{\partial \mathbf{s}(\boldsymbol{\theta})}{\partial(\boldsymbol{\theta})} \triangleq \mathbf{H}$ is the Jacobian matrix, $\boldsymbol{\theta}$ is the emitter's location, and $\mathbf{s}(\boldsymbol{\theta})$ is a vector of the true TDOAs at the receivers.

A collection of N sensors is used to locate a stationary emitter, $\mathbf{u}$. A two-dimensional scenario is considered where at least two pairs of sensors are needed under TDOA. The sensors are paired apriori into $M = \frac{N}{2}$ pairs and no pair shares a common sensor. The actual TDOA of the m^{th} sensor pair is

$$\tau_m = \frac{1}{c}\left(||\mathbf{x}_i - \mathbf{u}|| - ||\mathbf{x}_j - \mathbf{u}||\right) \tag{2}$$

where $\mathbf{x}_i$, $\mathbf{x}_j$ are the locations of sensors i and j, and c is the speed of light.

Each sensor pair makes their TDOA estimate, $\hat{\tau}_m$ from cross correlating their measured signal data [2]. All estimated TDOAs are sent to a single node for location processing. The measurements are corrupted by additive estimation errors

$$\hat{\tau}_m = \tau_m + n_m \quad m = 1, \ldots, M \tag{3}$$

where n_m is the m^{th} pair's random TDOA measurement error. The TDOA measurements are obtained using the maximum likelihood (ML) estimator [2]. From the asymptotic properties of the ML estimator [4], the distribution of n_m is taken as zero-mean Gaussian with variance σ_m^2 for $m = 1, ..., M$.

Under TDOA, the Jacobian is the derivative of the TDOA with respect to the emitter's location and is given by

$$\mathbf{H} = \begin{bmatrix} \frac{\partial}{\partial \mathbf{u}} (\tau_1) \\ \vdots \\ \frac{\partial}{\partial \mathbf{u}} (\tau_M) \end{bmatrix} \tag{4}$$

where the derivative of the m^{th} pair's TDOA is

$$\frac{\partial (\tau_m)}{\partial \mathbf{u}} = -\frac{1}{c} \left[\frac{\mathbf{x}_i - \mathbf{u}}{||\mathbf{x}_i - \mathbf{u}||} - \frac{\mathbf{x}_j - \mathbf{u}}{||\mathbf{x}_j - \mathbf{u}||} \right]. \tag{5}$$

An error ellipse interpretation of the FIM can be used which shows how the location error is oriented in the x-y plane [9]. The eigenvectors of the FIM dictate the major and minor axes of the error ellipse and the reciprocal square roots of the eigenvalues dictate the lengths of the axes. Figure 1 shows the error ellipse and is used as an illustrative case throughout the paper.

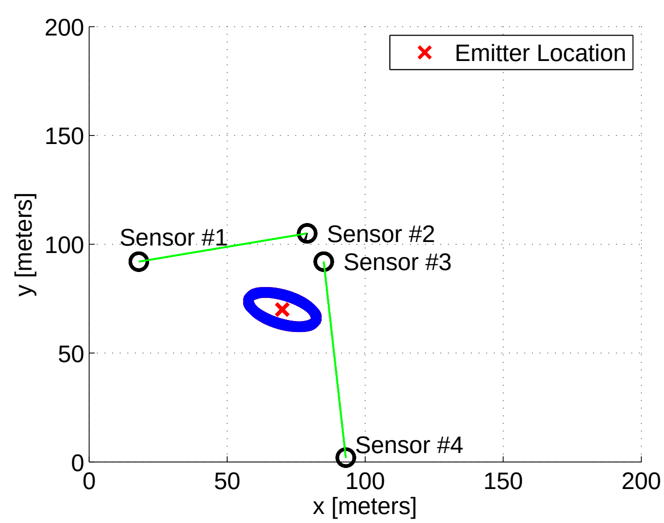


Fig. 1. System setup for a two pair network. Sensors 1 & 2 and 3 & 4 are paired as shown in green. The error ellipse using the TDOA method is shown in blue for $\sigma_{\text{TDOA}} = 17.4$ ns.

III. False Location Injection

The presence of a rogue sensor is considered, whose goal is to degrade the estimation accuracy of a network estimating emitter location as described in Section II. The rogue sensor has the ability to inject a single false report of a sensor's state, which in this paper is the sensor's location. The single false sensor position, $\mathbf{x}_f$ is sought that minimizes the locating network's FIM and is given by

$$\arg \min_{\mathbf{x}_f} \ \det \left(\mathbf{H}^T \mathbf{C}^{-1} \mathbf{H} \right) \tag{6}$$

where $\mathbf{H}$ is a function of the false location, $\mathbf{x}_f$ as in (4)-(5). The FIM is positive semidefinite [4]. We assume a means for injecting a false position exists. The rogue pairs with another valid sensor thereby corrupting a single sensor pair in the network. It is assumed that the first pair is corrupted by the rogue and is composed of the rogue sensor reporting a false position, $\mathbf{x}_f$ and a valid sensor reporting its true position, $\mathbf{x}_t$.

The FIM can be expressed as the linear combination of each pair's contribution to the FIM,

$$\begin{aligned} \mathbf{H}^T \mathbf{C}^{-1} \mathbf{H} &= \begin{bmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \end{bmatrix} \begin{bmatrix} \frac{1}{\sigma_1^2} & 0 \\ 0 & \frac{1}{\sigma_2^2} \end{bmatrix} \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} & (7) \\ &= \frac{1}{\sigma_1^2} \mathbf{h}_1 \mathbf{h}_1^T + \frac{1}{\sigma_2^2} \mathbf{h}_2 \mathbf{h}_2^T & (8) \end{aligned}$$

where $\mathbf{h}_1^T = [h_{11} \quad h_{12}]$ and $\mathbf{h}_2^T = [h_{21} \quad h_{22}]$ are the derivatives of TDOA w.r.t emitter location of the corrupt and non-corrupt pairs, respectively. Each submatrix $\mathbf{h}_m \mathbf{h}_m^T$ is pair m's contribution to the Fisher Information Matrix. The variance of TDOA for the corrupt and non-corrupt pairs are given by σ_1^2 and σ_2^2, respectively.

For convenience, we let $\mathbf{A} = \frac{1}{\sigma_2^2} \mathbf{h}_2 \mathbf{h}_2^T$ since the non-corrupt pair is not a function of the false position. Further, by introducing a new variable, $\mathbf{Y} = \mathbf{h}_1 \mathbf{h}_1^T$, gives

$$\mathbf{H}^T \mathbf{C}^{-1} \mathbf{H} = \frac{1}{\sigma_1^2} \mathbf{Y} + \mathbf{A} \tag{9}$$

where $\mathbf{Y}$ is the outer product of the derivative of the corrupt pair's TDOA. Although (9) is shown for two sensor pairs, the above holds for additional non-corrupt pairs, where $\mathbf{A}$ reflects the contribution of the additional pairs.

From the construction of $\mathbf{Y}$, the diagonal entries of $\mathbf{Y}$ are ≥ 0 and is at most rank one. The problem (6) seeks to minimize the determinant of the FIM. The matrix $\mathbf{A}$ is rank one, which implies the sum in (9) is at least rank one. Since the Rank($\mathbf{Y} + \mathbf{A}$) $\leq$ Rank($\mathbf{Y}$) + Rank($\mathbf{A}$), there are two possibilities for $\mathbf{Y}$. If $\mathbf{Y}$ has rank one, the only way the rank($\mathbf{Y} + \mathbf{A}$) is one is if the row and column spaces of $\mathbf{Y}$ and $\mathbf{A}$ are dependent. If these two matrices are dependent, then this implies that both sensor pairs give the same contribution to the FIM. This can happen if the unit vectors pointing from the emitter to the sensors in both pairs are equal, i.e. the sensors lie along the same vector. Since the rogue can only move one sensor position in $\mathbf{h}_1$, this is not a viable geometry as it would require the location network to have positioned a sensor from each pair along the same line from the emitter, resulting in a poor geometry for location. Otherwise given any arbitrary geometry it may not be possible to ensure there is a solution such that the matrix $\mathbf{Y}$ is rank one and the Rank($\mathbf{Y}+\mathbf{A}$) is also rank one. However, if $\mathbf{Y}$ has rank zero, this restriction is not imposed. Thus, $\mathbf{Y}$ is constrained to be rank zero which requires $\mathbf{Y} \geq \mathbf{0}$.

Since the $\log(\cdot)$ is monotonically increasing in its argument, substituting (9) gives

$$\begin{aligned} \arg\min_{\mathbf{Y}} \quad & \log\left(\det\left(\frac{1}{\sigma_1^2}\mathbf{Y}+\mathbf{A}\right)\right) & (10)\\ \text{s.t.} \quad & \mathbf{Y} \geq \mathbf{0} & (11) \end{aligned}$$

which is a concave minimization problem where σ_1^2 and $\mathbf{A}$ are known constants.

The objective function is linearized using the Taylor Series Expansion about $\mathbf{Y}_k$,

$$\log\left(\det\left(\tfrac{1}{\sigma_1^2}\mathbf{Y}+\mathbf{A}\right)\right) \approx \log\left(\det\left(\tfrac{1}{\sigma_1^2}\mathbf{Y}_k+\mathbf{A}\right)\right)+\mathrm{tr}\{\mathbf{B}_k \cdot [\mathbf{Y}-\mathbf{Y}_k]\} \quad (12)$$

where $\mathbf{B}_k = \left(\frac{1}{\sigma_1^2}\left(\frac{1}{\sigma_1^2}\mathbf{Y}_k+\mathbf{A}\right)^{-1}\right)$. The constants in (12) can be ignored since they do not affect the minimization. We have a sequence of semidefinite programs (SDP)s

$$\mathbf{Y}_{(k+1)} = \arg\min_{\mathbf{Y}} \ \mathrm{tr}\{\mathbf{B}_k\mathbf{Y}\} \quad (13)$$

which are each convex [10]. A similar linearization procedure is used for the rank minimization problem [11], where $\mathbf{Y}_0 = \mathbf{I}$. Due to the non-negative constraint, (13) converges in one step using [12] to the optimal value $\mathbf{Y}^* = \mathbf{0}$. Thus, we need only solve

$$\begin{aligned} \arg\min_{\mathbf{Y}} \quad & \mathrm{tr}\{\mathbf{B}_k\mathbf{Y}\} & (14)\\ \text{s.t.} \quad & \mathbf{Y} \geq \mathbf{0} & (15) \end{aligned}$$

which is a semidefinite program in variable $\mathbf{Y}$.

Since $\mathbf{Y}^* = \mathbf{0}$ it follows that the derivative of the TDOA, $\mathbf{h}_1^* = \mathbf{0}$ as in (5). Since $\mathbf{h}_1$ is not a one-to-one function of $\mathbf{x}_f$, multiples values of $\mathbf{x}_f^*$ exist which yield the same value of $\mathbf{Y}^*$. Nonetheless, we obtain a closed form solution for the false location,

$$\frac{\mathbf{x}_f^*-\mathbf{u}}{||\mathbf{x}_f^*-\mathbf{u}||} = \frac{\mathbf{x}_t-\mathbf{u}}{||\mathbf{x}_t-\mathbf{u}||}. \quad (16)$$

The solution in (16) dictates the unit vector pointing from the emitter $\mathbf{u}$, to the valid true sensor $\mathbf{x}_t$, should equal the unit vector pointing from the emitter to the rogue corrupted sensor $\mathbf{x}_f$. Therefore, any position along the vector through $\mathbf{x}_t$ maximally degrades estimation accuracy. Figure 2 shows a numerical example, where sensor 1 is injected with a false position. The positions which minimize the det(FIM) are marked with an "$\mathbf{x}$".

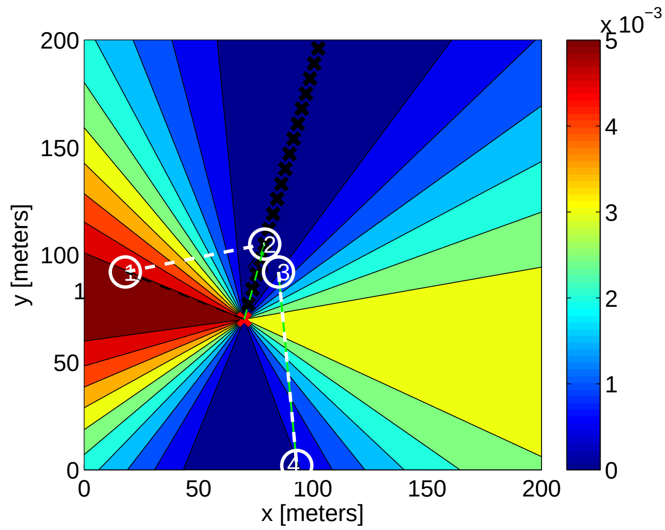


Fig. 2. Evaluation of the determinant of the FIM for the geometry in Figure 1 at a 0.2 meters interval over a 200m x 200m grid. Sensor 1 is injected with a false position. The solution set of false locations are marked with an "$\mathbf{x}$".

IV. Detecting and Rejecting Erroneous TDOA Measurements

Thus far it is assumed that the locating network is unaware of the rogue sensor. Next, we consider the scenario where the locating network is aware of the rogue and of the rogue's ability to corrupt one of its TDOA measurements.

We consider the case where the location network has the ability to validate each senor pair's measurement by comparing the measured TDOA with the expected TDOA. Upon detection of an inconsistent TDOA measurement, the erroneous measurement is ignored by the network. We assume that the locating network has more than the minimum number of pairs needed for location. If not, rejection of one of the erroneous TDOA measurements would leave only one usable TDOA measurement to perform emitter location, as a minimum of two TDOAs are required. In order to ensure that the rogue's injection is not rendered useless, the TDOA measurement from the corrupted pair must not be discarded.

A. Ensuring Valid TDOA Measurements

It is in the rogue's interest to choose a false location that results in a TDOA measurement that is equal to the expected TDOA. We observe that any position at the same distance from the emitter as the sensor's true location does not change the value of TDOA. Figure 3 shows a numerical example where any position along the dashed circle gives the same value of TDOA as if the sensor was reporting its true position.

While the rogue wants to ensure its injection is not detected, its objective is still to maximally degrade estimation accuracy. Since the FIM is composed of the TDOA derivatives, sensor positions with the same TDOA value can have different values of Fisher Information. Using the solution in (16), we choose the location along the vector at the same distance from the

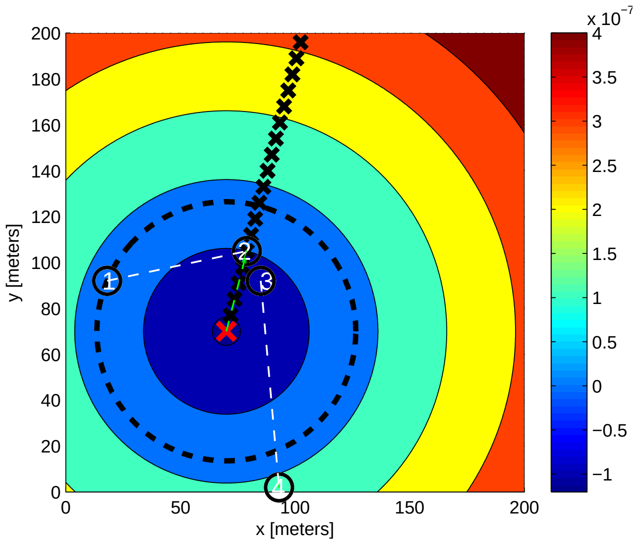
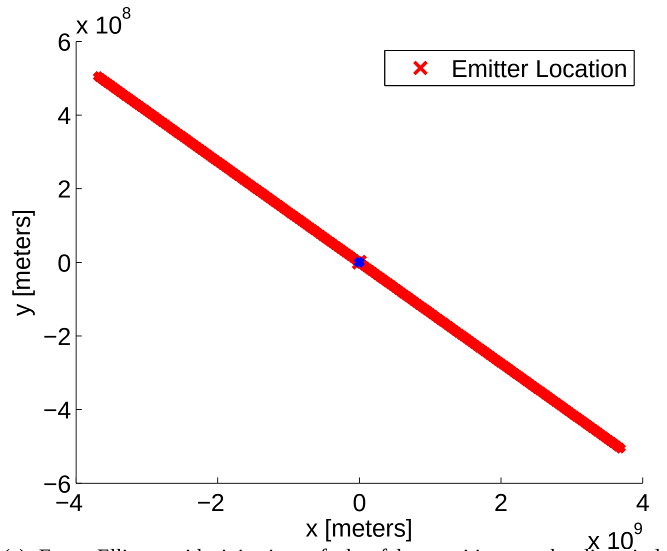
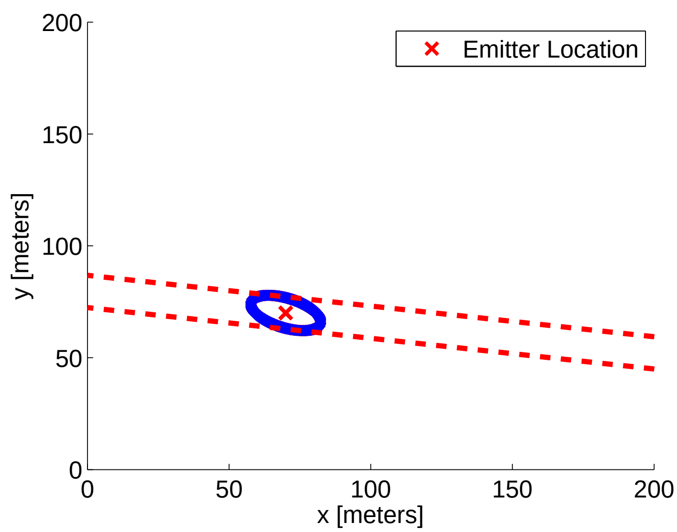


Fig. 3. Evaluation of the TDOA for grid locations. The dashed circle corresponds to the locations that do not change the TDOA. The false positions which satisfy (16) are marked with an "x".



(a) Error Ellipse with injection of the false position at the line-circle intersection in Figure 3



(b) A zoomed-in view of 4(a). Error ellipses with (dashed red) and without (solid blue) a false location

Fig. 4.

emitter as the sensor's true location. Figure 3 shows the set of locations that do not change the TDOA by the dashed circle and the locations that minimize the FIM determined from (16) are marked with an "x". The intersection of the circle and line is the position that not only minimizes the FIM but also gives a TDOA as if the sensor was reporting its true position.

The error ellipse interpretation of the FIM is revisited. The error ellipses with and without injection of a false position are compared. Using the false location solution in (16), the corresponding error ellipse is plotted in red in Figure 4. The error ellipse without the rogue sensor is plotted in blue. It is observed that the accuracy has been degraded such that the network cannot locate the emitter.

V. Conclusion

This work investigates the problem of a rogue sensor able to inject a single false sensor position into a network tasked with estimating an emitter's location under the time difference of arrival method. We find a closed form solution which states that the false senor locations that minimize the Fisher Information Matrix lie along the vector pointing from the emitter through the valid sensor in the rogue corrupted pair. Using this result, we present a method for finding the false sensor locations that not only minimize the FIM but also ensures that the resulting TDOA measurement is utilized by the locating network.

References

[1] H. Chan and A. Perrig, "Security and privacy in sensor networks," *IEEE Computer Society*, vol. 36, no. 10, pp. 103–105, 2003.

[2] S. Stein, "Differential delay/Doppler ML estimation with unknown signals," *IEEE Transactions on Signal Processing*, vol. 41, no. 8, pp. 2717–2719, 1993.

[3] P. Chestnut, "Emitter location accuracy using TDOA and differential Doppler," *IEEE Transactions on Aerospace Electronic Systems*, vol. AES-18, pp. 214–218, 1982.

[4] S. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice Hall, 1993.

[5] X. Hu and M. Fowler, "Sensor Selection for Multiple Sensor Emitter Location Systems," *IEEE Aerospace Conference*, pp. 1–10, 2008.

[6] N. Wu, Y. Guo, K. Huang, M. Ruschmann, and M. Fowler, "Fault-tolerant tasking and guidance of an airborne location sensor network," *International Journal of Control Automation and Systems*, vol. 6, no. 3, pp. 351–363, 2008.

[7] M. Chen and M. Fowler, "Data Compression for Multiple Parameter Estimation with Application to TDOA/FDOA Emitter Location," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 46, no. 1, pp. 308–322, 2010.

[8] L. Huie and M. Fowler, "Emitter Location in the Presence of Information Injection," *in the Proceedings of Conference on Information Science and Systems, CISS*, March 2010.

[9] M. Fowler, “Analysis of single-platform passive emitter location with terrain data,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 37, no. 2, pp. 495–507, 2001.

[10] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[11] M. Fazel, H. Hindi, and S. Boyd, “Log-det heuristic for matrix rank minimization with applications to Hankel and Euclidean distance matrices,” in *Proceedings of the American Control Conference*, vol. 3, 2003, pp. 2156–2162.

[12] M. Grant, S. Boyd, and Y. Ye, “CVX: Matlab software for disciplined convex programming,” *avialable at http://www. stanford. edu/boyd/cvx*, vol. 1.