BIASING EMITTER LOCATION ESTIMATES VIA FALSE LOCATION INJECTION

Lauren M. Huie[*†] *and Mark L. Fowler*[†]

[*]Air Force Research Laboratory, [†] State University of New York at Binghamton

ABSTRACT

We consider the problem of a rogue introducing bias into a network estimating location under the time difference of arrival (TDOA) method. In particular we consider how a rogue by injecting only a single false sensor position can drive the network's location estimate a specified distance away from the true value. The least squares (LS) residuals is minimized to find the false location to inject given the rogue's desired distance offset. In order to illustrate the success of our method, we consider the statistical tools that the locating network might employ to handle our false information injection including least squares and in the presence of outliers robust least median squares (LMS). We show that our method can successfully bias the location estimate of an estimating network when both LS and LMS methods are used.

***Index Terms*—** Emitter location, TDOA, non-linear least squares, information injection

1. INTRODUCTION

Sensor networks communicate using a shared wireless medium, and thus it is possible for a rogue sensor to infiltrate the network. Although methods exist for securing sensor networks (i.e., encryption), such unauthorized access can still occur [1]. Thus, it is important to understand how a rogue can degrade estimation accuracy as well as how a sensor network can mitigate its effect.

One sensor network estimation task of particular interest is estimating the location of an emitter. We consider the problem of a rogue introducing bias into a locating network using time difference of arrival (TDOA). We assume a rogue sensor can inject a false report of its state (e.g. sensor position and velocity) into an estimating network. In particular, this work seeks the false sensor location which drives the emitter location estimate a specified distance away from its true value.

The problem of decreasing the accuracy of localization networks has been previously considered in [2, 3, 4]. In [2], a bias is introduced into triangulation through a simple corruption model where the adversary arbitrarily alters a percentage of measurements such that they vote for some other location. In order to obtain a consensus, many measurements are required. Alternatively in [3, 4] a single false location injection is used to decrease estimation accuracy by minimizing the Fisher Information Matrix (FIM). Here and in [3, 4] we assume that a single rogue sensor deceitfully pairs with one valid sensor thereby corrupting a single sensor pair. The other $M-1$ pairs each contain two valid sensors. While [4] shows that it is possible to maximally degrade estimation accuracy via a single injection, as will be shown in Section 3.1, minimizing the FIM does not necessarily introduce a bias.

This work solves a different problem, where in order to drive the emitter location estimate away from its true value we minimize the LS cost of the TDOA residuals to determine the false sensor location to be injected. The main contributions of this work are: (1) a method by which a rogue can introduce a significant bias into the location estimate of an estimating network under TDOA, and (2) the bias achieved by the rogue can be intuitively controlled through a distance parameter. Through numerical results we show that our method is able to introduce significant bias even in the presence of robust estimation techniques.

Section 2 discusses estimation under TDOA. Section 3 presents a new method of finding the false rogue position that introduces significant bias. Section 4 evaluates the success of the rogue using mean squared error (MSE) for both the nonlinear LS and more robust least median squares (LMS).

2. BACKGROUND

A collection of N sensors is used to estimate the location of a stationary emitter located at $\mathbf{x}_e$. In a two-dimensional scenario at least two pairs of sensors are needed under the time difference of arrival (TDOA) method to obtain a location estimate. The sensors are paired apriori into $M = \frac{N}{2}$ pairs and no two pairs share a common sensor. Each pair of sensors defines a hyperbola where the foci are the sensor locations [5]. The actual TDOA of the m^{th} sensor pair is

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

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

Each sensor pair makes their TDOA estimate, $\hat{\tau}_m$, by cross correlating their measured signal data. All estimated

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

TDOAs are sent to a single node for location processing which is assumed here to not be the rogue sensor. The measurements are corrupted by additive estimation errors

$$\hat{\tau}_m = \tau_m(\mathbf{x}_e) + n_m \quad m = 1, \ldots, M, \tag{2}$$

where n_m is the m^{th} pair's random TDOA measurement error. The TDOA measurements are obtained using the maximum likelihood (ML) estimator. From the asymptotic properties of the ML estimator [6], the distribution of n_m is taken as zero-mean Gaussian with variance σ_m^2 for $m = 1, ..., M$.

Using the TDOA measurements, the location estimate can be found by minimizing the least squares (LS) cost of the TDOA residuals given by

$$\hat{\mathbf{x}}_e = \arg\min_{\tilde{\mathbf{x}}_e} \sum_{m=1}^{M} \left(\hat{\tau}_m - \tau_m(\tilde{\mathbf{x}}_e)\right)^2 \tag{3}$$

where $\tilde{\mathbf{x}}_e$ is the variable of all possible emitter locations. Due to the non-linear dependency on $\tilde{\mathbf{x}}_e$, the Gauss-Newton method [6] can be used to iteratively find the LS solution. Since non-linear LS is typically used to estimate location [5], it is important to understand how the non-linear LS estimate can be influenced by a rogue's false injection.

3. IMPACT OF THE ROGUE SENSOR

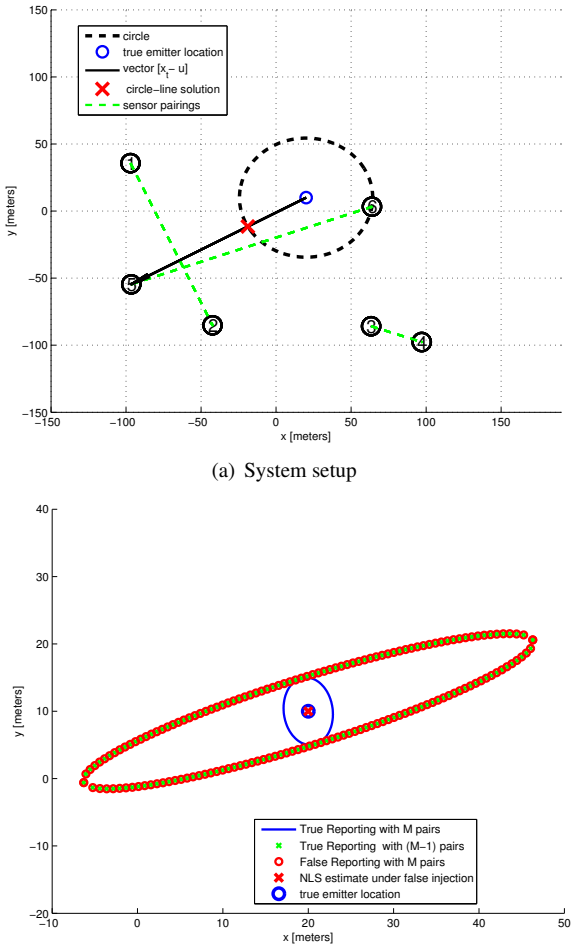
In [4] we considered a rogue that seeks to maximally degrade accuracy by choosing its false state to minimize the Fisher Information Matrix (FIM). In this section we first show that the rogue's choice of false state in [4] degrades the location to exactly the same location estimate that would be achieved if only the $M-1$ non-corrupt sensor pairs are used. Thus, we show the strategy in [4] only degrades accuracy by increasing the variance and does not introduce any bias into the location estimate as shown in Figure 1. We precisely determine the impact of the solution in [4] on the non-linear LS estimate and introduce a new method capable of introducing significant bias into the estimate.

3.1. Interpretation of the FIM Minimizing Solution

In [3, 4] a single rogue sensor is used to inject a false state into the network to minimize the FIM. The closed form solution in [4] is given by

$$\frac{\mathbf{x}_f^* - \mathbf{x}_e}{||\mathbf{x}_f^* - \mathbf{x}_e||} = \frac{\mathbf{x}_t - \mathbf{x}_e}{||\mathbf{x}_t - \mathbf{x}_e||} \tag{4}$$

where $\mathbf{x}_f^*$ is the false state and $\mathbf{x}_t$ is the true sensor in the corrupt pair. The result in (4) states that the false position lies along the vector from the emitter through the true sensor. If a locating network is assumed to be able to detect and reject erroneous TDOA measurements then care should be taken when choosing a position on the line (4). To avoid



(a) System setup

(b) Performance comparison of M and $(M-1)$ pairs

Fig. 1. Impact of the rogue using the solution in [4].

detection, the sensor position that does not change the TDOA value of the corrupted pair should be selected. This position is at the same distance from the emitter as the actual position of the sensor.

We now provide further insight into the impact of the choice of false state. Namely, the solution in [4] is equivalent to only using the non-corrupt pairs to perform the emitter location. This can be seen by examining the non-linear LS estimate update [6] given by

$$\hat{\boldsymbol{\theta}}_{k+1} = \boldsymbol{\theta}_k + \left(\mathbf{H}_{\boldsymbol{\theta}_k}^T \mathbf{H}_{\boldsymbol{\theta}_k}\right)^{-1} \mathbf{H}_{\boldsymbol{\theta}_k}^T \mathbf{r}, \tag{5}$$

where $\hat{\boldsymbol{\theta}}$ is the unknown parameter (emitter location), the Jacobian, $\mathbf{H}_{\boldsymbol{\theta}_k}$ is the derivative of TDOA w.r.t. the emitter's location given that the k^{th} estimate is correct, and $\mathbf{r}$ is the residual TDOA given the k^{th} estimate. For M sensor pairs, the Jacobian is (dropping the subscript) $\mathbf{H} = \left[\mathbf{h}_1^T; \ldots; \mathbf{h}_{M-1}^T; \mathbf{h}_M^T\right]$ where $\mathbf{h}_m$ is the derivative of TDOA of the m^{th} pair w.r.t. the emitter's location and $\mathbf{h}_m^T$ is the m^{th} row of $\mathbf{H}$. The product $\mathbf{H}^T\mathbf{H}$ can be written as the sum of each pair's con-

tribution, $\mathbf{H}^T\mathbf{H} = \mathbf{h}_1\mathbf{h}_1^T + \mathbf{h}_2\mathbf{h}_2^T + \cdots + \mathbf{h}_M\mathbf{h}_M^T$, where we assume that the last pair M contains the corrupt rogue sensor and from [4], $\mathbf{h}_M^T = \bar{\mathbf{0}}_{1\times 2}$. The Jacobian becomes $\mathbf{H} = \left[\mathbf{h}_1^T; \ldots; \mathbf{h}_{M-1}^T; \bar{\mathbf{0}}_{1\times 2}\right]$ and the product $\mathbf{H}^T\mathbf{H}$ becomes

$$\mathbf{H}^T\mathbf{H} = \underbrace{\mathbf{h}_1\mathbf{h}_1^T + \mathbf{h}_2\mathbf{h}_2^T + \cdots + \mathbf{h}_{M-1}\mathbf{h}_{M-1}^T}_{\text{due to non-corrupt pairs}} + \bar{\mathbf{0}}_{2\times 2} \qquad (6)$$

indicating that the non-linear LS estimate is computed using only the non-corrupt pairs' Jacobian submatrices. Thus, the solution in [4] can increase the variance no more than to the level that would occur if only the M–1 non-corrupt pairs are used for location processing as shown in Figure 1. In many cases this prohibits the rogue from significantly degrading the performance, i.e., for cases where the performance with the remaining M–1 pairs is sufficiently good. It also leaves some random aspect to the degradation achieved - even though the variance is larger, a particular estimate may be quite accurate. Next we explore a new approach, which does not have this limitation and allows for the rogue to introduce significant bias into the location estimate.

3.2. Biasing the Location Estimate

The goal of the rogue is to drive the non-linear LS estimate of emitter location to be r distance units away from its true value by injecting a single false position. That is, the rogue seeks to move the non-linear LS estimate to the position

$$\hat{\mathbf{x}}_{e,r}(\theta) = \mathbf{x}_e + r\left[cos(\theta) \quad sin(\theta)\right],^T \qquad (7)$$

where r is the desired offset and θ is any value in $[0,\ 2\pi]$ to be selected by the rogue as shown by the dashed circle in Figure 2. Since the rogue allows the location estimate to be at any value of θ, it must also be considered in the optimization.

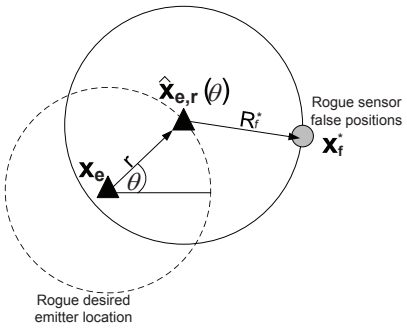


Fig. 2. Rogue desired emitter location estimate

To find the false position, the LS cost of the TDOA residuals is minimized given the rogue's desired condition in (7). The problem can be formulated as

$$\arg\min_{\mathbf{x}_f,\theta} \sum_{m=1}^{M-1} \left(\bar{\tau}_m(\hat{\mathbf{x}}_{e,r}(\theta)) - \tau_m\right)^2 + \left(\bar{\tau}_M\left(\hat{\mathbf{x}}_{e,r}(\theta), \mathbf{x}_f\right) - \tau_M\right)^2 \qquad (8)$$

where $\bar{\tau}_m(\theta)$ and $\bar{\tau}_M(\theta,\ \mathbf{x}_f)$ are the TDOA values for the possible values of $\mathbf{x}_f$ and θ, and τ_m is the true value of TDOA of the m^{th} pair in (1). For simplicity of notation we drop the functional dependence of the TDOAs on $\hat{\mathbf{x}}_{e,r}(\theta)$ to θ noting that all parameters in (7) except θ are known.

The problem in (8) is non-linear and due to the rank deficiency of the Jacobian matrix the Gauss-Newton method cannot be used. The Jacobian is given by

$$\mathbf{H} = \begin{bmatrix} \frac{\partial\bar{\tau}_1(\theta)}{\partial\theta} & \frac{\partial\bar{\tau}_1(\theta)}{\partial\mathbf{x}_f} \\ \vdots & \vdots \\ \frac{\partial\bar{\tau}_M(\theta,\mathbf{x}_f)}{\partial\theta} & \frac{\partial\bar{\tau}_M(\theta,\mathbf{x}_f)}{\partial\mathbf{x}_f} \end{bmatrix} \qquad (9)$$

where $\frac{\partial\bar{\tau}_m(\theta)}{\partial\mathbf{x}_f} = \bar{\mathbf{0}}_{1\times 2}\ \ \forall m \neq M$. The Jacobian is $M\times 3$ and is clearly rank degenerate. To remedy this problem a change of variables can be used where $R_f = ||\hat{\mathbf{x}}_{e,r}(\theta) - \mathbf{x}_f||$. The LS cost in (8) can be re-written as

$$\arg\min_{R_f,\theta} \sum_{m=1}^{M-1} \left(\bar{\tau}_m(\theta) - \tau_m\right)^2 + \left(\bar{\tau}_M(\theta,\ R_f) - \tau_M\right)^2 \qquad (10)$$

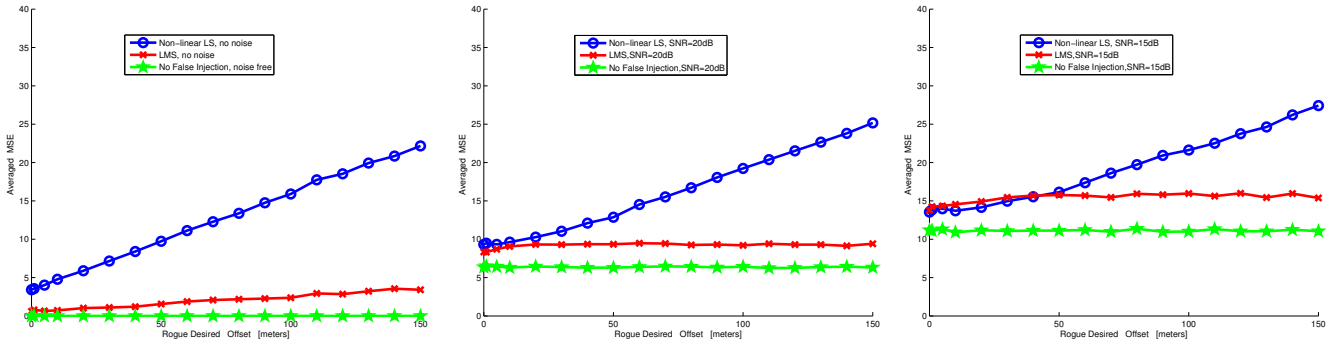
where $\bar{\tau}_M(\theta,\ R_f) = \frac{1}{c}\left[||\hat{\mathbf{x}}_{e,r}(\theta) - \mathbf{x}_t|| - R_f\right]$. By minimizing the LS cost the rogue can reduce its detectability. If the rogue's false state significantly increases the LS sum beyond expected then its presence can be detected. As such, the rogue seeks to ensure this sum of squares is minimized while still driving the estimate away from its true value. The set of false positions which minimize the LS cost (10) is described by a circle with center $\hat{\mathbf{x}}_{e\,r}(\theta)\,|_{\theta=\theta^*}$ and radius R_f^* as shown in Figure 2. As a result, any point on this circle reported to the locating network's non-linear LS algorithm is a solution for the rogue's false position.

The solution of (10) is found by evaluating over a fine grid, although it is expected that this could be solved using other methods such as gradient-based methods, or using particle swarm optimization techniques.

4. EVALUATING THE FALSE INJECTION

We assume that the rogue selects the false sensor location to inject as in Section 3 and then reports the location to the estimating network. Our method is evaluated for an estimating network that uses both traditional non-linear LS and robust LS techniques to obtain its final location estimates $\hat{\mathbf{x}}_{e,\text{LS}}$ and $\hat{\mathbf{x}}_{e,\text{LMS}}$. Recall, the LS estimate is given by $\hat{\mathbf{x}}_e = \arg\min_{\tilde{\mathbf{x}}_e} \sum_{m=1}^{M}\left(\hat{\tau}_m - \tau_m(\tilde{\mathbf{x}}_e)\right)^2$, and can be solved iteratively using Gauss Newton.

It is well known that LS estimation is susceptible to outliers. A natural consideration is the use of robust statistical techniques [7] to remove the sensitivity to outliers. To this end, it is important to also evaluate the impact of our approach when robust statistical methods are used. Specifically, we evaluate our method against least median squares (LMS).



(a) Noise free (b) SNR=20dB (c) SNR=15dB

Fig. 3. Mean squared error performance for non-linear LS and LMS.

The performance of LMS has been shown in [8]. Although no closed form exists for LMS, [9] provides an efficient method. There are two main steps, (1) clustering the measurements into subsets to obtain a set of weights, and (2) reweighting the measurements and solving for the final estimate using weighted LS.

Given X total measurements, K subsets are randomly chosen, each with n samples. For each subset j an estimate $\hat{\boldsymbol{\theta}}_j$ is found and the squared residuals r_{ij}^2 for each estimate is determined across all X measurements . The cluster with the smallest median of the squared residuals is used to determine the weights for each measurement,

$$w_i = \begin{cases} 1 & |\frac{r_i}{s_o}| \leq \gamma \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

where $s_o = 1.48826\left(1 + \frac{5}{X-P}\right)\sqrt{\text{med}_i r_i^2\left(\hat{\boldsymbol{\theta}}\right)}$, P is the dimension of the unknown parameter, and γ is a threshold chosen as in [9]. Given these weights, weighted LS is then used to find the final location estimate.

The effectiveness of our approach in biasing the location estimate is evaluated as a function of MSE and the rogue desired offset. We consider 2000 sensor-emitter geometries randomly generated in a 1000m$\times$1000m field for ten sensor pairs.

Figure 3 shows the MSE of the estimate in the presence of false injection under non-linear LS and LMS for varying SNR. The baseline MSE without injection is shown for comparison. We observe that our method is able to successfully bias the location estimate across varying distances and SNR for both LS and LMS. For higher SNR, LMS gives a smaller error than compared with LS as expected. For lower SNR and small distance offsets LS gives a smaller error, while for larger distances LMS gives a smaller error which is to be expected [2]. For LS, increasing the distance offset increases the MSE while for LMS the MSE still increases but levels out quickly with larger distances.

5. CONCLUSION

In this work, we consider the problem of a rogue sensor that seeks to drive the emitter location estimate away from its true value. In order to more seriously degrade performance, the LS cost is minimized given the condition of the rogue's desired offset. Our method introduces significant bias into the estimate for a network employing non-linear LS and even when robust estimation methods such as LMS are used.

6. 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] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," *Proc. of the 4 th Int. Symp. on Information Processing in Sensor Networks (IPSN)*, pp. 91–98, 2005.

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

[4] L.M. Huie and M.L. Fowler, "A Closed Form for False Location Injection under Time Difference of Arrival," *in 44th Asilomar Conf. on Signals, Systems and Computers*, Nov 2010.

[5] D.J. Torrieri, "Statistical Theory of Passive Location Systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-20, no. 2, pp. 183–198, 1984.

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

[7] S.A. Kassam and H.V. Poor, "Robust techniques for signal processing: A survey," *Proceedings of the IEEE*, vol. 73, no. 3, pp. 433–481, 2005.

[8] P.J. Rousseeuw, "Least median of squares regression," *Journal of the American statistical association*, vol. 79, no. 388, pp. 871–880, 1984.

[9] P.J. Rousseeuw and A.M. Leroy, *Robust regression and outlier detection*, John Wiley & Sons Inc, 1987.