2017 IEEE 56th Annual Conference on Decision and Control (CDC)
December 12-15, 2017, Melbourne, Australia

Minimum Variance Unbiased Estimation in the Presence of an Adversary

Kewei Chen, Vijay Gupta, and Yih-Fang Huang

Abstract— **Consider a setup in which a central estimator seeks to estimate an unknown deterministic parameter using measurements from multiple sensors. Some of the sensors may be adversarial in that their utility increases with the Euclidean distance between the estimate of the central estimator and their own local estimate. These sensors may misreport their measurements to the central estimator at a falsification cost. We formulate a Stackelberg game in which the central estimator acts as the leader and the adversarial sensors act as the follower. We present the optimal linear fusion scheme for the estimator and the optimal attack pattern for the adversarial sensors in the Nash equilibrium sense. Interestingly, the estimate at the central estimator may be better than if the measurements from the adversarial sensors were altogether ignored.**

I. INTRODUCTION

Smart personal devices equipped with a rich set of embedded sensors have led to the emergence of crowd sensing in a variety of applications such as environmental monitoring, traffic control, social networking, and so on. In this paradigm, a large number of sensors owned by different individuals generate measurements for an application and share these measurements with a central estimator. However, it may be costly for participants to serve as sensors. Not only may it consume resources such as power for measurement and transmission, there may also be a potential privacy hazard. Since the sensors do not belong to the central estimator, an important challenge for the central estimator is to design a mechanism to incentivize the sensors to generate and transmit measurements of sufficient quality.

A review of various incentive mechanisms that have been proposed for this purpose, including both monetary and non-monetary incentives, is provided in [1] and [2]. More specifically, systems based on micro-payments [3], reputations [4] [5] and auctions [6] [7] [8] have been discussed in the literature. One common assumption in early works in this direction was that sensors (more precisely, their owners) are truthful, in that they do not provide false measurements on purpose to 'game' the system and either gain more payment or degrade the estimate at the central estimator. Lately, strategic sensors, that can be untruthful in order to maximize their utilities, have also been considered. As an example, the work [9] studied selfish sensors who can transmit falsified information to increase their compensation.

Yet, sensors may also be adversarial in that their utility increases with the degradation in the quality of the estimate at the central estimator. This may be the case if the sensor benefits from particular actions that the central estimator may take due to its estimate being inaccurate, e.g., in a traffic estimation and control setting. Clearly, if all sensors are adversarial, the central estimator will not be able to obtain an estimate with bounded error (unless the falsification costs for the sensors are very high). We consider a setting in which only one sensor is adversarial and ask the question if it is possible to design a fusion scheme in which the central estimator can gain by including the (possibly erroneous) measurements from the adversarial sensor.

To this end, we formulate a Stackelberg game in which the central estimator acts as the leader and declares its fusion algorithm. The sensors act as the followers and choose their data to transmit. We solve the game by finding the subgame perfect Nash equilibrium (SPNE). We show that it is unique and always exists. In the SPNE, we show that the estimate at the central estimator can improve by including the information from the adversarial sensor as compared to simply discarding it. We also study the role of information availability at the adversarial sensor and show that the adversarial sensor can degrade the estimate at the central estimator more if she has access to the observations from the other sensors.

There are several streams of work that are relevant. The literature on CPS security in general, and security with malicious attackers in an estimation problem in particular, is now quite well developed (e.g., see [10], [11], [12], [13]). In this stream, our work is closest to those that model the problem as a game (e.g., [14] [15]); yet our formulation is quite different. As mentioned above, a different stream is the one inspired by crowdsensing and incentive design to obtain accurate data; however, these works do no consider adversarial sensors in general. Works on the Byzantine general problem consider adversarial sensors [16] [17], yet there does not seem to be a comprehensive game theoretic study of the problem. The work closest to ours seems to be [16], which studies estimation with an adversarial sensor that can arbitrarily change its reported data and designs an approach based on hypothesis testing to decide whether the data from the adversarial sensor should be used. Unlike [16], we set up a game theoretical model in which the adversarial sensor is assigned a utility function that guides its strategy. Although the utility function that we consider in this work is quite specific, the framework allows for more general utility functions in which the sensor wishes to degrade the estimate of the central estimator according to various metrics.

The rest of this paper is organized as follows. In Section II,

Kewei Chen, Vijay Gupta, and Yih-Fang Huang are with the Department of Electrical Engineering, University of Notre Dame, IN 46556, USA. (kchen6, vgupta2, huang)@nd.edu. The work was partially supported by NSF awards ECCS 1550016 and CNS 1739295 and the AFOSR award FA9550-15-1-0186.

the problem statement is presented and a Stackelberg game between the central estimator and the adversarial sensor is formulated. In Section III, we find the SPNE under two different scenarios and present the main results. Some further discussions are presented in Section IV. In Section V, we conclude the paper with some avenues for future work.

Notation: $\hat{\theta}$ denotes an estimate of the parameter θ. The Gaussian pdf is denoted by $\mathcal{N}(m, \sigma^2)$ where m is the mean and σ is the standard deviation. The expectation of a random variable X is denoted by $\mathbb{E}[X]$. The conditional expectation of a random variable X given another random variable Y is shown by $\mathbb{E}[X|Y]$. All variables are real-valued unless mentioned otherwise.

II. Problem Statement

We consider a centralized static estimation problem in which a central estimator uses observations from two sensors to estimate an unknown deterministic parameter $\theta \in \mathbb{R}$. Section III-D considers the case of $N > 2$ sensors. We consider the following model:

$$x_1 = \theta + v_1, \tag{1}$$

$$x_2 = \theta + v_2, \tag{2}$$

where x_1 and x_2 are observations of θ obtained by sensor 1 and sensor 2 separately; v_1 and v_2 are independent and identically distributed (i.i.d.) noises with $v_1, v_2 \sim \mathcal{N}(0, \sigma^2)$. Clearly, the minimum variance unbiased (MVU) estimate of θ using x_1 and x_2 would, in general, have lower error variance than the one obtained using either of the measurements alone.

The central estimator asks the two sensors to report their measurements. Denote by x_{r1} and x_{r2}, respectively, the measurements that sensor 1 and sensor 2 report to the central estimator. In general, $x_{ri} \neq x_i$. The central estimator is interested in calculating the minimum variance unbiased (MVU) estimate of θ. If $x_{ri} = x_i, i = 1, 2$, then this estimate is given by $\hat{\theta}_g = \dfrac{x_{r1} + x_{r2}}{2}$ with variance = $\dfrac{\sigma^2}{2}$, which is also the Cramer-Rao lower bound (CRLB) for the problem.

We now present the utility functions and strategy spaces of various decision makers.

- Sensor 1 is denoted as the loyal sensor. Its utility function is assumed to be $U_1 =$ constant and its strategy space is the choice of x_{r1}. Given that its utility function is independent of its strategy, we assume $x_{r1} = x_1$.
- Sensor 2 is the adversarial sensor. Its strategy space is to choose x_{r2}. We consider two separate scenarios:
  1) Scenario S_1: x_{r2} is a function of both x_1 and x_2.
  2) Scenario S_2: x_{r2} is a function of x_2 alone.

  The utility function for this sensor is given by
  $$U_a = (\hat{\theta}_g - \hat{\theta}_a)^2 - \beta(x_{r2} - x_2)^2, \tag{3}$$
  where $\hat{\theta}_g$ denotes the MVU estimate calculated by the central estimator using x_{r1} and x_{r2}, $\hat{\theta}_a$ is the MVU estimate of θ calculated by sensor 2 using the information she has access to, and $\beta > 0$ is a parameter that is used to calculate the falsification cost. For future use, we denote by $\epsilon = x_{r2} - x_2$ the amount of falsification introduced by sensor 2.
- The central estimator seeks to calculate the MVU estimate $\hat{\theta}_g$ of θ using x_{r1} and x_{r2}. We limit ourselves to the case when
  $$\hat{\theta}_g = w_1 x_{r1} + w_2 x_{r2}, \tag{4}$$
  where w_1 and w_2 are weights designed by the central estimator as its strategy. The utility function of the central estimator is denoted by $U_{estimator} = -\text{var}(\hat{\theta}_g)$.

We make the following assumptions:

(i) Constants such as β and σ^2, as well as the form of utility functions, are public knowledge.

(ii) The decision makers are risk neutral. Thus, sensor 2 seeks to maximize $\mathbb{E}[U_a]$ and the central estimator seeks to maximize $\mathbb{E}[U_{estimator}]$.

(iii) The timeline of the problem is as shown in Fig. 1.

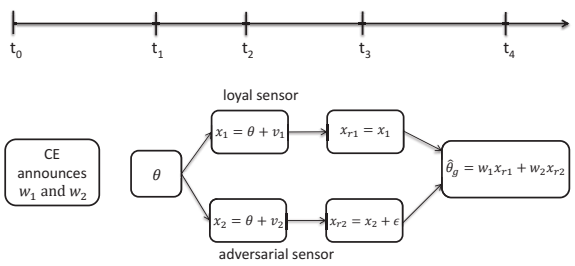

Fig. 1. Timeline of the Stackelberg game considered in the paper.

We are interested in a Stackelberg formulation of the problem in which the central estimator acts as the leader and the sensors act as the followers.

Remark 1: Note that the loyal sensor may not be a physically separate sensor. The role of this sensor can be played by the *a priori* information about θ as possessed by the central estimator.

Remark 2: As shown in the timeline in Fig. 1, w_1 and w_2 are announced at time t_0. The adversarial sensor chooses ϵ at time t_3 given this knowledge. The expectation on U_a in the utility function is over v_1 and v_2.

Remark 3: An upper bound on performance of the central estimator is obtained when $x_{r1} = x_1$ and $x_{r2} = x_2$. In this case, as discussed earlier, $\hat{\theta}_g = \dfrac{x_{r1} + x_{r2}}{2}$ and $\text{var}(\hat{\theta}_g) = \dfrac{\sigma^2}{2}$. A lower bound is obtained if the measurement from the adversarial sensor is discarded, i.e., if the central estimator sets $w_1 = 1$ and $w_2 = 0$. In this case, $\hat{\theta}_g = x_{r1} = x_1$ and $\text{var}(\hat{\theta}_g) = \sigma^2$.

The problem we consider is to identify the SPNE of this game and to identify the resulting utility functions. Subgame perfect Nash equilibrium (SPNE) is a generalization of the Nash equilibrium to a dynamic game. We refer the reader to [18] for a formal definition of SPNE.

III. Main Results

We proceed by backward induction to identify the SPNE of the game.

A. Scenario S_1: x_{r2} is a function of both x_1 and x_2.

For the case when the adversarial sensor has access to both x_1 and x_2, we have the following result.

Theorem 1: Consider the problem setting in Section II. If the adversarial sensor can choose x_{r2} as a function of both x_1 and x_2, the SPNE is given by the following strategies.

(i) The adversarial sensor chooses:

$$x_{r2} = x_2 + \epsilon = x_2 + \frac{w_2}{\beta - w_2^2}\left(w_1 x_1 + w_2 x_2 - \frac{x_1 + x_2}{2}\right). \tag{5}$$

(ii) The central estimator chooses:

$$\begin{cases} w_1 = w_2 = \dfrac{1}{2} & \text{when} \quad \beta \geq \dfrac{1}{4}, \\ w_1 = 1 - w_2; \quad w_2 = \dfrac{1}{2} - \dfrac{1}{2}\sqrt{1-4\beta} & \text{when} \quad \beta < \dfrac{1}{4}. \end{cases} \tag{6}$$

(iii) At SPNE, the estimate is unbiased and the variance is given by:

$$\text{min.var}(\hat{\theta}_g) = \begin{cases} \frac{\sigma^2}{2} & \text{when} \quad \beta \geq \dfrac{1}{4}, \\ \dfrac{A+B}{C}\sigma^2 & \text{when} \quad \beta < \dfrac{1}{4}, \end{cases} \tag{7}$$

where

$$\begin{aligned} A &= \left(\beta - \frac{1}{4} + \left(\frac{1}{2}\beta + \frac{1}{4}\right)\sqrt{1-4\beta}\right)^2, \\ B &= \left(\frac{1}{2} - \beta - \frac{1}{2}\sqrt{1-4\beta}\right)\left(\beta - \frac{1}{4} + \frac{1}{4}\sqrt{1-4\beta}\right)^2, \\ \text{and} \quad C &= \left(2\beta - \frac{1}{2} + \frac{1}{2}\sqrt{1-4\beta}\right)^2. \end{aligned} \tag{8}$$

Proof: Under Scenario S_1, $\hat{\theta}_a = \dfrac{x_1 + x_2}{2}$. Given w_1 and w_2, the utility function of adversarial sensor is

$$U_a = \left(w_1 x_1 + w_2\left(x_2 + \epsilon\right) - \frac{x_1 + x_2}{2}\right)^2 - \beta\epsilon^2. \tag{9}$$

Setting the derivative of U_a with respect to ϵ equal to 0 yields the best response of the adversarial sensor at time t_3 as

$$\begin{aligned} &\frac{\mathrm{d}U_a}{\mathrm{d}\epsilon} = 0 \\ \implies &\epsilon = \frac{w_2}{\beta - w_2^2}\left(w_1 x_1 + w_2 x_2 - \frac{x_1 + x_2}{2}\right). \end{aligned} \tag{10}$$

For the central estimator, first we note that if the weights are chose to satisfy the constraints $w_1 + w_2 = 1$ and $w_2^2 < \beta$, then, $\mathbb{E}[\epsilon] = 0$ and $\hat{\theta}_g$ is unbiased. This can be seen by noting that $\mathbb{E}[x_1] = \mathbb{E}[x_2] = \theta$ and

$$\begin{aligned} \mathbb{E}[\epsilon] &= \frac{w_2}{\beta - w_2^2}\left(\left(w_1 - \frac{1}{2}\right)\mathbb{E}[x_1] + \left(w_2 - \frac{1}{2}\right)\mathbb{E}[x_2]\right) \\ &= 0 \end{aligned} \tag{11}$$

when $w_1 + w_2 = 1$. Hence

$$\begin{aligned} \mathbb{E}[\hat{\theta}_g] &= \mathbb{E}[w_1 x_1 + w_2 x_{r2}] \\ &= \mathbb{E}[w_1 x_1 + w_2 x_2 + w_2 \epsilon] \\ &= (w_1 + w_2)\theta = \theta. \end{aligned} \tag{12}$$

Now, we have two possible cases.

- If $\beta \geq \dfrac{1}{4}$, the optimal strategy of the central estimator is $w_1 = w_2 = \dfrac{1}{2}$. This can be seen by noting that according to (10), $w_1 = w_2 = \dfrac{1}{2}$ yields $\epsilon = 0$. Further with this choice,
$$\hat{\theta}_g = \frac{x_1 + x_{r2}}{2} = \frac{x_1 + x_2}{2}, \tag{13}$$
which is an unbiased estimate that attains the CRLB.
- If $\beta < \dfrac{1}{4}$, the optimal strategy of the central estimator is given by $w_1 = \dfrac{1}{2} + \dfrac{1}{2}\sqrt{1-4\beta}, w_2 = \dfrac{1}{2} - \dfrac{1}{2}\sqrt{1-4\beta}$. This can be noted by observing that,
$$\begin{aligned} x_{r2} &= x_2 + \epsilon \\ &= x_2 + \frac{w_2}{\beta - w_2^2}(w_1 - \frac{1}{2})x_1 + \frac{w_2}{\beta - w_2^2}(w_2 - \frac{1}{2})x_2 \\ &= \frac{w_2(w_1 - \frac{1}{2})}{\beta - w_2^2}x_1 + \frac{\beta - \frac{1}{2}w_2}{\beta - w_2^2}x_2. \end{aligned} \tag{14}$$
Thus, the global estimate $\hat{\theta}_g$ is given by
$$\begin{aligned} \hat{\theta}_g &= w_1 x_1 + w_2 x_{r2} \\ &= \frac{\beta w_1 - \frac{1}{2}w_2^2}{\beta - w_2^2}x_1 + \frac{w_2(\beta - \frac{1}{2}w_2)}{\beta - w_2^2}x_2. \end{aligned} \tag{15}$$
Given that x_1 and x_2 are independent and $w_1 + w_2 = 1$, we can write
$$\begin{aligned} \text{var}(\hat{\theta}_g) &= \frac{(\beta w_1 - \frac{1}{2}w_2^2)^2 + w_2^2(\beta - \frac{1}{2}w_2)^2}{(\beta - w_2^2)^2} \\ &= \frac{(\beta(1-w_2) - \frac{1}{2}w_2^2)^2 + w_2^2(\beta - \frac{1}{2}w_2)^2}{(\beta - w_2^2)^2}. \end{aligned} \tag{16}$$
Note that $\text{var}(\hat{\theta}_g)$ is convex over w_2. Taking the derivative $\frac{\mathrm{d}\text{var}(\hat{\theta}_g)}{\mathrm{d}w_2} = 0$ yields a cubic equation with three real roots. We choose the root $w_2 = \dfrac{1}{2} - \dfrac{1}{2}\sqrt{1-4\beta}$ which satisfies $w_2^2 < \beta$. The weight w_1 is then given by $w_1 = 1 - w_2$. Replacing w_2 in (16) with $\dfrac{1}{2} - \dfrac{1}{2}\sqrt{1-4\beta}$ yields (7). Notice here that $w_2^2 < \beta$ and hence U_a is concave over ϵ and (10) yields the maximum of U_a.

■

Remark 4: When the adversarial sensor has access to x_1, her optimal falsification ϵ is an affine function of x_1 and x_2.

Remark 5: The subgame perfect Nash equilibrium is unique.

B. Scenario S_2: x_{r2} is a function of x_2 only

For the case when the adversarial sensor only has access to x_2, we have the following result.

Theorem 2: Consider the problem setting in Section II. If the adversarial sensor can choose x_{r2} as a function of x_2 only, the SPNE is given by the following strategies.

(i) The adversarial sensor chooses:

$$x_{r2} = x_2 + \epsilon = x_2 + \frac{w_2}{\beta - w_2^2}(w_1 + w_2 - 1)x_2. \tag{17}$$

(ii) The central estimator chooses:

$$\begin{cases} w_1 = w_2 = \frac{1}{2} & \text{when} \quad \beta \geq \frac{1}{4}, \\ w_1 = 1 - w_2; \quad w_2 = \sqrt{\beta} & \text{when} \quad \beta < \frac{1}{4}. \end{cases} \tag{18}$$

(iii) At SPNE, the estimate is unbiased and the variance is given by:

$$\text{inf.var}(\hat{\theta}_g) = \begin{cases} \frac{\sigma^2}{2} & \text{when} \quad \beta \geq \frac{1}{4}, \\ ((1-\sqrt{\beta})^2 + \beta)\sigma^2 & \text{when} \quad \beta < \frac{1}{4}. \end{cases} \tag{19}$$

Proof: When the adversarial sensor does not have access to x_1, $\hat{\theta}_a = x_2$. Given w_1 and w_2, the expected utility of the adversarial sensor can be written as

$$\begin{aligned} \mathbb{E}[U_a] =& \mathbb{E}[(w_1x_1 + w_2x_{r2} - x_2)^2 - \beta\epsilon^2] \\ =& \mathbb{E}[w_2^2\epsilon^2 + 2(w_1x_1 + w_2x_2 - x_2)w_2\epsilon \\ &+ (w_1x_1 + w_2x_2 - x_2)^2 - \beta\epsilon^2]. \end{aligned} \tag{20}$$

The expectation is over x_1. Since x_1 is unknown to the adversarial sensor, $\mathbb{E}[x_1|x_2] = \hat{\theta}_a = x_2$ is the maximum likelihood estimate for x_1. Hence,

$$\begin{aligned} \mathbb{E}[U_a] =& (w_2^2 - \beta)\epsilon^2 + 2(w_1\,\mathbb{E}[x_1] + w_2x_2 - x_2)w_2\epsilon \\ &+ \mathbb{E}[(w_1x_1 + w_2x_2 - x_2)^2] \\ =& (w_2^2 - \beta)\epsilon^2 + 2(w_1x_2 + w_2x_2 - x_2)w_2\epsilon \\ &+ \mathbb{E}[(w_1x_1 + w_2x_2 - x_2)^2]. \end{aligned} \tag{21}$$

Setting $\frac{\mathrm{d}\,\mathbb{E}[U_a]}{\mathrm{d}\epsilon} = 0$ yields the best response of the adversarial sensor at t_3.

$$\begin{aligned} &\frac{\mathrm{d}\,\mathbb{E}[U_a]}{\mathrm{d}\epsilon} = 0 \\ \implies & 2(w_2^2 - \beta)\epsilon + 2(w_1x_2 + w_2x_2 - x_2)w_2 = 0 \\ \implies & \epsilon = \frac{w_2}{\beta - w_2^2}(w_1 + w_2 - 1)x_2. \end{aligned} \tag{22}$$

For the central estimator, we again note that if $w_1 + w_2 = 1$ and $w_2^2 < \beta$, then, $\epsilon = 0$ and $\hat{\theta}_g$ is unbiased. Now we have two possible cases.

- If $\beta \geq \frac{1}{4}$, the optimal strategy of the central estimator is $w_1 = w_2 = \frac{1}{2}$. This can be seen by noting that according to (22), $w_1 = w_2 = \frac{1}{2}$ yields $\epsilon = 0$. Further with this choice,

$$\hat{\theta}_g = \frac{x_1 + x_{r2}}{2} = \frac{x_1 + x_2}{2}, \tag{23}$$

which is an unbiased estimate that attains the CRLB.

- If $\beta < \frac{1}{4}$, the optimal strategy of the central estimator is given by $w_1 = 1 - \sqrt{\beta}$ and $w_2 = \sqrt{\beta}$. This can be noted by observing that,

$$\begin{aligned} \hat{\theta}_g &= w_1x_1 + w_2x_{r2} \\ &= w_1x_1 + w_2x_2. \end{aligned} \tag{24}$$

Since x_1 and x_2 are independent and $w_1 + w_2 = 1$,

$$\text{var}(\hat{\theta}_g) = (1 - w_2)^2 + w_2^2, \tag{25}$$

which is monotonically decreasing over w_2 that satisfies $w_2^2 < \beta$ for any $\beta < \frac{1}{4}$. Taking the infimum provides the desired result. Notice here that $w_2^2 < \beta$ and hence U_a is concave over ϵ and (22) yields the maximum of U_a.

■

Remark 6: Even when the adversarial sensor does not have access to x_1, her optimal falsification ϵ remains an affine function of her observation x_2. Further if $w_1 + w_2 = 1$, the optimal falsification is 0.

C. Comparison of the two scenarios

A numerical example for Scenario S_1 and S_2 is shown in Fig. 2 with $\beta = \frac{1}{5}$. The variance of the global estimate (16) under Scenario S_1 and the variance of the global estimate (25) under Scenario S_2 are plotted as functions of w_2. We can see that the variance under Scenario S_2 is lower throughout than the one under Scenario S_1. This suggests that more information at the adversarial sensor allows it to degrade the estimate at the central estimator more. We have the following result.

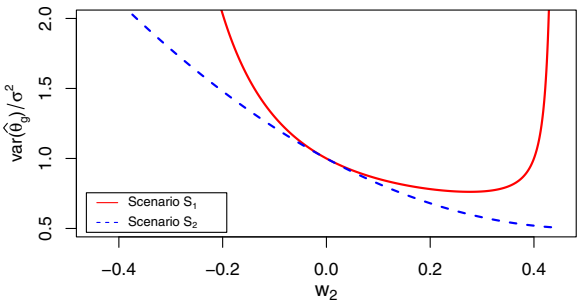

Fig. 2. A numerical example of $\beta = \frac{1}{5}$. The variance of the global estimate (16) under Scenario S_1 and the variance of the global estimate (25) under Scenario S_2 are plotted as functions of w_2.

Corollary 1: If $\beta \geq \frac{1}{4}$, the central estimator can obtain an unbiased estimate that attains Cramer-Rao lower bound by choosing $w_1 = w_2 = \frac{1}{2}$, irrespective of whether the adversarial sensor has access to x_1 or not. If $\beta < \frac{1}{4}$, the central estimator can obtain an unbiased estimate under both scenarios; however, it can obtain an unbiased estimate with a lower error variance if the adversarial sensor does not have access to x_1 than if the adversarial sensor has access to x_1.

Proof: The proof follows from Theorem 1 and Theorem 2 (specifically, (7) and (19)) in a straightforward manner. A pictorial description of the minimum variances for all $\beta < \frac{1}{4}$ is also given in Fig. 3. ■

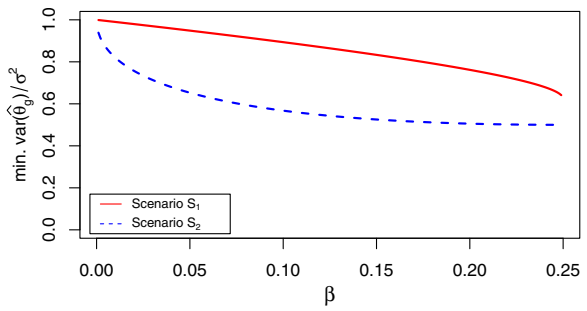

Fig. 3. Minimum variances of the global estimates obtained under both the scenarios for all $0 < \beta < \frac{1}{4}$. Note that the minimum variance under Scenario S_2 (when the adversarial sensor has less information) is always less than the one under Scenario S_1.

Remark 7: For all $\beta > 0$, whether or not the adversarial sensor has access to x_1, the central estimator can find an optimal strategy that linearly fuses the reported values from the adversarial and the loyal sensors, and yields an unbiased estimate with variance smaller than the variance attained by using the measurement from the loyal sensor only.

D. A general case

The arguments above generalize to the case when there exist $n > 1$ loyal sensors for which $x_{r1} = x_1, x_{r2} = x_2, ..., x_{rn} = x_n$ and 1 adversarial sensor. The basic idea is that the central estimator can first fuse the n loyal sensors with identical weights to obtain one equivalent loyal sensor. Specifically, the central estimator forms

$$\begin{aligned}\hat{\theta}_g &= w_1x_1 + w_2x_2 + ... + w_nx_n + w_{n+1}x_{r(n+1)} \\ &= \sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i + w_{n+1}x_{r(n+1)}.\end{aligned} \tag{26}$$

The expected utility of the adversarial sensor thus becomes

$$\begin{aligned}&\mathbb{E}[U_a] = \mathbb{E}[(\hat{\theta}_g - \hat{\theta}_a)^2 - \beta\epsilon^2] \\ &= \mathbb{E}[(\sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i + w_{n+1}x_{r(n+1)} - \hat{\theta}_a)^2 - \beta\epsilon^2] \\ &= \mathbb{E}[(\sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i + w_{n+1}x_{n+1} + w_{n+1}\epsilon - \hat{\theta}_a)^2 - \beta\epsilon^2].\end{aligned} \tag{27}$$

$\mathbb{E}[U_a]$ is concave if and only if

$$w_{n+1}^2 < \beta. \tag{28}$$

Setting $\frac{\mathrm{d}\,\mathbb{E}[U_a]}{\mathrm{d}\epsilon} = 0$ yields the best response of the adversarial sensor.

$$\begin{aligned}&\frac{\mathrm{d}\,\mathbb{E}[U_a]}{\mathrm{d}\epsilon} = 0 \\ &\Longrightarrow 2(w_{n+1}^2 - \beta)\epsilon \\ &\quad + 2(\sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i + w_{n+1}x_{n+1} - \hat{\theta}_a)w_{n+1} = 0 \\ &\Longrightarrow \epsilon = \frac{w_{n+1}}{\beta - w_{n+1}^2}(\sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i + w_{n+1}x_{n+1} - \hat{\theta}_a).\end{aligned} \tag{29}$$

In this general case, the unbiased estimate that attains the Cramer-Rao lower bound is given by

$$\hat{\theta}_a = \frac{\sum_{i=1}^{n} x_i + x_{n+1}}{n+1}. \tag{30}$$

We summarize the result below.

Theorem 3: Consider the formulation in Section II but with n loyal sensors and 1 adversarial sensor.

1) Scenario S_1: When the adversarial sensor has access to $\sum_{i=1}^{n} x_i$,

- The optimal strategy of the adversarial sensor in the SPNE is given by

$$\begin{aligned}x_{r(n+1)} &= x_{n+1} + \epsilon \\ &= x_{n+1} + \frac{w_{n+1}}{\beta - w_{n+1}^2}(\sum_{i=1}^{n} \frac{w_{loyal}}{n} x_i \\ &\quad + w_{n+1}x_{n+1} - \frac{\sum_{i=1}^{n} x_i + x_{n+1}}{n+1}).\end{aligned} \tag{31}$$

- If $w_{loyal} + w_{n+1} = 1$ and $w_{n+1}^2 < \beta$, then $\mathbb{E}[\epsilon] = 0$.
- The optimal strategy of the central estimator in the SPNE is given by

$$\begin{cases} w_i = w_{n+1} = \frac{1}{n+1}, & \beta \geq \frac{1}{(n+1)^2}, \\ w_i = \frac{1 - w_{n+1}}{n}; \quad w_{n+1} = A, & \beta < \frac{1}{(n+1)^2}, \end{cases} \tag{32}$$

where $A = \frac{1}{n+1} - \frac{1}{n+1}\sqrt{1 - (n+1)^2\beta}$ and $i = 1, 2, ..., n$.

2) Scenario S_2: When the adversarial sensor only has access to x_{n+1},

- The optimal strategy of the adversarial sensor in the SPNE is given by

$$\begin{aligned}x_{r(n+1)} &= x_{n+1} + \epsilon \\ &= x_{n+1} + \frac{w_{n+1}}{\beta - w_{n+1}^2}(\sum_{i=1}^{n} \frac{w_{loyal}}{n} \\ &\quad + w_{n+1} - 1)x_{n+1}.\end{aligned} \tag{33}$$

- If $w_{loyal} + w_{n+1} = 1$ and $w_{n+1}^2 < \beta$, then $\epsilon = 0$.
- The optimal strategy of the central estimator in the SPNE is given by

$$\begin{cases} w_i = w_{n+1} = \frac{1}{n+1}, & \beta \geq \frac{1}{(n+1)^2}, \\ w_i = \frac{1 - w_{n+1}}{n}; \quad w_{n+1} = \sqrt{\beta}, & \beta < \frac{1}{(n+1)^2}, \end{cases} \tag{34}$$

where $i = 1, 2, ..., n$.

3) If $\beta \geq \frac{1}{(n+1)^2}$, the central estimator can obtain an unbiased estimate that attains the CRLB by setting $w_i = w_{n+1} = \frac{1}{n+1}$, $i = 1, 2, ...n$ in either scenario. If $\beta < \frac{1}{(n+1)^2}$, the central estimator can obtain an unbiased estimate with lower variance under Scenario S_2 than under Scenario S_1.

An illustration of $n = 10$ loyal sensors and 1 adversarial sensor is presented in Fig. 4, which shows the minimum variance of the global estimate under Scenario S_2 is always less than the one under Scenario S_1 for all $0 < \beta < \frac{1}{(n+1)^2}$.

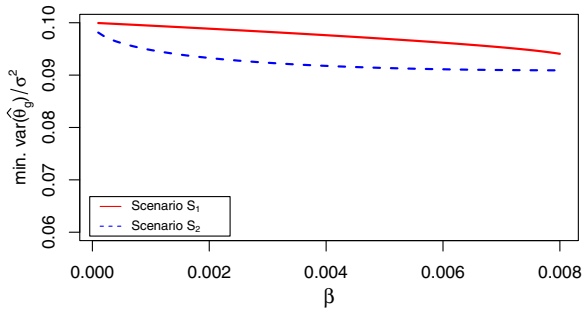

Fig. 4. Minimum variances of the global estimates obtained under both the scenarios for all $0 < \beta < \frac{1}{121}$ with $n = 10$ loyal sensors and 1 adversarial sensor. Note that the minimum variance under Scenario S_2 (when the adversarial sensor has less information) is always less than the one under Scenario S_1.

IV. Further Discussion

We note that the SPNE above automatically satisfies the individual rationality constraint. The adversarial sensor has non-negative utility if she plays her best response. Specifically, her utility in the subgame perfect Nash equilibrium is given by

$$U_a^{opt} = \frac{(w_1 x_1 + w_2 x_2 - \hat{\theta}_a)^2 \beta}{\beta - w_2^2}, \tag{35}$$

which is non-negative since $\beta > 0$ and $w_2^2 < \beta$.

V. Conclusions and Future Work

In this paper, we considered a formulation in which a central estimator seeks to estimate an unknown deterministic parameter using reported measurements from a loyal sensor and an adversarial sensor. We formulated a Stackelberg game in which the central estimator acts as the leader and the adversarial sensor acts as the follower. The Stackelberg game is solved by finding the subgame perfect Nash equilibrium. We show that the falsification of the adversarial sensor can be restricted. Interestingly, we found that the central estimator can obtain a better estimate by fusing the information from the adversarial sensor rather than simply discarding it. When the falsification cost is high enough, the central estimator can obtain an unbiased estimate that attains the Cramer-Rao lower bound. When the falsification cost is low, we present a mechanism that guarantees the best response of the adversarial sensor is truthfully reporting if she does not have access to measurements from the other sensor. If the adversarial sensor has access to measurements from the other sensor, we provided the optimal linear fusion scheme for the central estimator to obtain an unbiased estimate with minimum variance. We also considered a general case where there exist multiple loyal sensors and one adversarial sensor. Future work will involve considering multiple adversarial sensors and dynamic estimation. Also of interest would be simultaneously considering selfish sensors and adversarial sensors.

References

[1] H. Gao, C. H. Liu, W. Wang, J. Zhao, Z, Song, X. Su, J. Crowcroft, and K. K. Leung, "A survey of incentive mechanisms for participartory sensing," *Communication Surveys & Tutorials, IEEE*, vol. 17, no. 2, pp. 918-943, 2015.

[2] F. Restuccia, S. K. Das, and J. Payton, "Incentive mechanisms for participatory sensing: survey and research challenges," *arXiv preprint arXiv:1502.07687*, 2015.

[3] S. Reddy, D. Estrin, M. Hansen, and M. Srivastava, "Examining micro-payments for participatory sensing data collections," in *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM, pp. 33-36, 2010.

[4] Y. Zhang and M. Van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," in *INFOCOM, 2012 Proceedings IEEE*. pp. 2140-2148, 2012.

[5] P. Naghizadeh and M. Liu, "Perceptions and truth: A mechanism design approach to crowd-sourcing reputation," *arXiv preprint arXiv:1306.0173*, 2013.

[6] J.-S. Lee and B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing," in *Pervasive Computing and Communications (PerCom), 2010 IEEE International Conference on*. IEEE, pp. 60-68, 2010.

[7] J.-S. Lee and B. Hoh, "Dynamic pricing incentive for participatory sensing," *Pervasive and Mobile Computing*, vol. 6, no. 6, pp. 693-708, 2010.

[8] K. Chen, V. Gupta, and Y. F. Huang, "On auction design for crowd sensing," in *19th International Conference on Information Fusion (FUSION)*. pp. 334-339, 2016.

[9] D. G. Dobakhshari, N. Li, and V. Gupta, "An incentive-based approach to distributed estimation with strategic sensors," in *Conference on Decision and Control (CDC) 2016*, IEEE, 2016, pp. 6141-6146.

[10] C. Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: fundamental limitations and performance bounds," in *American Control Conference (ACC), 2015*. IEEE, 2015 pp. 195-200.

[11] C. Z. Bai and V. Gupta, "On Kalman filtering in the presence of a compromised sensor: fundamental performance bounds", in *American Control Conference (ACC), 2014*. IEEE, 2014, pp. 3029-3034.

[12] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: attack models and protection schemes," *IEEE Trans. Smart Grid*, 2016, to appear.

[13] Y. Mo, and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Smart Automatic Control*, vol. 60, no. 4, pp. 1145-1151, 2015.

[14] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based dos attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, 2016, to appear.

[15] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120-132, 2013.

[16] C. Wilson and V. Veeravalli, "MMSE estimation in a sensor network in the presence of an adversary," in *International Symposium on Information Theory (ISIT), 2016*, IEEE, 2016, pp. 2479-2483.

[17] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16-29, 2009.

[18] K. Leyton-Brown and Y. Shoha, *Essentials of Game Theory: A Consice Multidisciplinary Introduction*, ser. Synthesis Lectures on Artificial Intelligence and Machine Learning. San Francisco, CA: Morgan Claypool Publ., 2008.