ASYMPTOTIC PERFECT SECRECY IN DISTRIBUTED ESTIMATION FOR LARGE SENSOR NETWORKS

Jun Guo, Hao Chen

ECE, Boise State University

Uri Rogers

ECE, Eastern Washington University

ABSTRACT

This paper considers asymptotic perfect secrecy and asymptotic perfect estimation in distributed estimation for large sensor networks under threat of an eavesdropper, which has access to all sensor outputs. To measure secrecy, we compare the estimation performance at the fusion center and at eavesdropper in terms of their respective Fisher Information. We analyze the Fisher Information ratio between the fusion center and eavesdropper and derive the maximum achievable ratio when the channels between sensors and eavesdropper are noisy binary symmetric channels. Furthermore, when the fusion center has noiseless channels, we show that the Fisher Information ratio can be made arbitrarily large by careful design of the sensor quantization rules. As a result, asymptotic perfect secrecy can be achieved by making the Fisher Information at Eve arbitrarily small while keeping the Fisher Information at the fusion center arbitrarily large. The secrecy design method in this paper might greatly enhance the secrecy in distributed estimation for large sensor networks.

***Index Terms*—** Eavesdropping, Distributed Estimation, Asymptotic Perfect Secrecy, Physical Layer Security

1. INTRODUCTION

A large sensor network (SN) consists of a large number of low-cost, low-power, mobile and miniature sensors. Large SNs are widely employed in many applications, such as surveillance, health-care, cyber-physical systems, diagnostics of complex systems [1] and so on. For these applications, the data collected by the sensors are extremely sensitive, and care must be taken to ensure this information is not leaked to any third party. In SNs, the sensor outputs often must be transmitted across a wireless communication network to legitimate users e.g., fusion center (FC), for final inference-making. Because of the wireless network links, the data are more vulnerable to security breaches. An eavesdropping attack, where a listener (Eve) taps the wireless link between the sensors and the FC, forms the basis or starting point for many different attack strategies [2], and will be our focus.

The strategies of mitigating eavesdropping attacks can be mainly classified into two categories, computational security and information-theoretic (physical layer) approaches [3]. The computational security approaches (cryptosystems) may not work well if the devices (nodes in SNs) do not have the computational power [4]. On the other hand, information-theoretic security approaches, utilizing the characteristics of the physical layer, have gained considerable attention as a complement to computational security methods to enhance the security, secrecy and privacy of SNs [5–8]. Even though the work in [9] based on information-theoretic approach may provide a nearly perfect secrecy, the solution tends to require long block codes that are complicated to be implemented in SNs with their stringent constraints on time delay, bandwidth, and power [10]. Therefore, a new approach based on physical layer security approach is needed for large SNs to mitigate eavesdroppers.

Aiming to estimate the values of a group of parameters based on a network of collaborating sensors [11–14], distributed estimation has been an important and active research area over the past several decades. Several attempts were made to address the issue of eavesdroppers in distributed estimation. Aysal et al. proposed to solve the problem by adding a stochastic cipher as a security module, to randomly change the sensor outputs and disguise them from the eavesdropper [15]. Guo et al. considered using multiple-input multiple-output beamforming strategies to combat the eavesdroppers, where local sensors use the analog amplify and forward scheme to communicate with the FC over a slow-fading orthogonal multiple access channel [16]. In [17], Khan and Stanković proposed to securely estimate distributed data in cyber-physical systems by verifying statistical consistency on the nodal, local information and physical-layer feedback.

Notice that the aforementioned efforts considered SNs with a fixed number of sensors and did not focus on achieving asymptotic perfect secrecy (APS), where Eve could not obtain any useful information when there is no limitations on the number of sensors. In this paper, we investigate APS and concentrate on enhancing the secrecy of distributed estimation against eavesdroppers in large SNs using physical layer security approach. To measure secrecy, we compare the estimation performance at the FC and at Eve in terms of their respective Fisher Information (FI). We analyze the FI ratio between the FC and Eve and derive the maximum achievable ratio when the channels between sensors and Eve are noisy binary symmetric channels (BSCs). Furthermore, when the

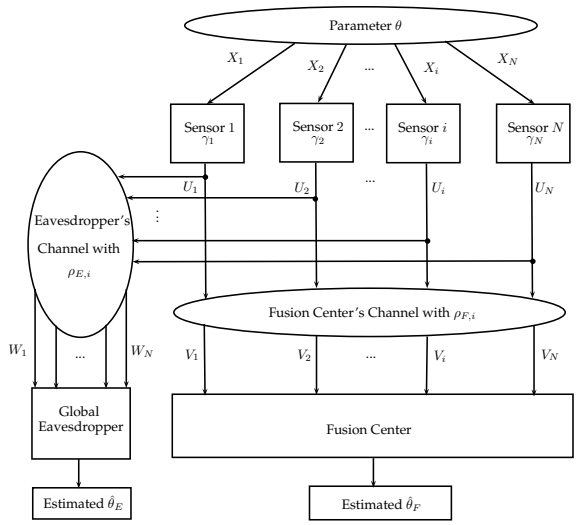

Fig. 1: Parallel sensor network model under eavesdropper attack, who eavesdropson the output of sensor i, transmitted wirelessly via a BSC with BER $\rho_{E,i}$. The FC receives sensor i data through another BSC with BER $\rho_{F,i} < \rho_{E,i}$.

FC has noiseless channel, we show that the FI ratio can be made arbitrarily large by careful design of the sensor quantization rules. As a result, APS can be achieved by making the FI at Eve arbitrarily small while keeping the FI at the FC arbitrarily large.

2. DISTRIBUTED SENSOR NETWORK MODEL

The parallel SN model is shown in Fig 1, where parameter θ is fixed but unknown. In many applications, the sensors are either randomly deployed or placed in similar locations to the environment to be monitored. In such scenarios, the sensor observations can be assumed to be conditionally independent and identically distributed (i.i.d) given the underlying parameter θ. Under this assumption, the sensor observations $\mathbf{X} = [X_1, X_2, \ldots, X_N]$ can be written as follows,

$$f(\mathbf{X}|\theta) = \prod_{i=1}^{N} f(X_i|\theta),$$

where $f(\mathbf{X}|\theta)$ and $f(X_i|\theta)$ are known probability density functions (pdfs) and X_i is the observation of sensor i.

In this paper, we consider the classic estimation problem,

$$X_i = \theta + Z_i, \;\; i = 1, 2, \ldots, N, \tag{1}$$

where Z_i is an additive i.i.d zero mean observation noise with pdf $f(\cdot)$. Due to the bandwidth constraint between local sensors and the FC, we assume the X_i are quantized to a single bit of compressed data, U_i, via the quantization rule

$$U_i = \begin{cases} 1, & X_i > \eta_i \\ 0, & X_i \leq \eta_i \end{cases} \; \forall i, \tag{2}$$

where the threshold, η_i, is fixed and known to both the FC and Eve. To reduce the system complexity and improve system robustness, we assume that the sensors employ identical quantization rules such that $\eta_1 = \eta_2 = \cdots = \eta_N = \eta$. Because the sensors observations are conditionally i.i.d., we have

$$\Pr(U_i = 1|\theta) = \beta = \Pr(\theta + Z_i > \eta) = Q(\eta - \theta),$$
$$\Pr(U_i = 0|\theta) = 1 - \beta = 1 - \Pr(U_i = 1|\theta),$$

where $Q(t) = \int_t^\infty f_Z(x)dx$ is the complementary distribution function of Z.

The communication channels between sensors and the receivers are assumed to be BSCs. Sensor i sends decision U_i to the FC over a BSC with bit error rate (BER) $\rho_{F,i} < \frac{1}{2}$, with the received decision V_i. All of the sensors outputs are eavesdropped by Eve via a set of parallel wiretapping channels. Eve receives W_i, from sensor i as an output of a separate BSC channel with BER $\rho_{E,i} < \frac{1}{2}$. We assume that Eve's channel is noisier than the FC's such that $\rho_{E,i} > \rho_{F,i}$ [18,19]. Assuming that the sensors are within similar distances to Eve and the FC, then the channels can be assumed to be independent and identical, i.e., $\rho_F = \rho_{F,1} = \cdots = \rho_{F,N}$ and $\rho_E = \rho_{E,1} = \cdots = \rho_{E,N}$.

As a result, the observations at the FC and Eve possess the following quality,

$$\Pr(V_i = 1|\theta) = (1 - 2\rho_F)\Pr(U_i = 1|\theta) + \rho_F,$$
$$\Pr(W_i = 1|\theta) = (1 - 2\rho_E)\Pr(U_i = 1|\theta) + \rho_E.$$

For the purposes of this paper we analyze identical channels, although non-identical channels can be treated in a similar fashion.

3. ESTIMATION PERFORMANCE AND ASYMPTOTIC PERFECT SECRECY

We now evaluate the estimation performance at the FC and Eve, using the widely employed Mean Squared Error (MSE) metric. The Cramér-Rao inequality given observations $\mathbf{V} = [V_1, \ldots, V_N]^T$ and known quantization rules [20, 21], establishes a MSE lower bound for any unbiased estimator of $\hat{\theta}_F$, ϵ_F. Specifically [22],

$$\epsilon_F \triangleq E\left(\hat{\theta} - \theta\right)^2 \geq \text{CRLB}(\mathbf{V};\theta) = \frac{1}{\mathbf{I}(\mathbf{V};\theta)}, \tag{3}$$

where CRLB is Cramér-Rao lower bound [23] and $\mathbf{I}(\mathbf{V};\theta)$ is the FI, given by,

$$\mathbf{I}(\mathbf{V};\theta) \triangleq E_{\mathbf{V}}\left(\frac{\partial \log p(\mathbf{V};\theta)}{\partial\theta}\right)$$
$$\overset{(a)}{=} \sum_{i=1}^{N} E_{V_i}\left(\frac{\partial \log p(V_i;\theta)}{\partial\theta}\right)$$
$$\overset{(b)}{=} NI(\eta, \theta, \rho_F),$$

where $p(\mathbf{V};\theta)$ is probability density function (PDF) of parameter θ given $\mathbf{V}$ [23]. Note, (a) and (b) follow from the sensors observations conditionally i.i.d property, the identical channels assumption, and

$$I(\eta,\theta,\rho) = \frac{f^2(\eta-\theta)(1-2\rho)^2}{(\rho+(1-2\rho)Q(\eta-\theta))(1-\rho-(1-2\rho)Q(\eta-\theta))} \quad (4)$$

is the per sensor FI when the sensor observation is received over a BSC with BER ρ.

Similarly, at Eve with $\mathbf{W} = [W_1,\ldots,W_N]^T$, the MSE lower bound, ϵ_E, for any unbiased estimator $\hat{\theta}_E$ is

$$\epsilon_F \triangleq E\left(\hat{\theta}-\theta\right)^2 \geq \text{CRLB}(\mathbf{W};\theta) = \frac{1}{\mathbf{I}(\mathbf{W};\theta)} = \frac{1}{NI(\eta,\theta,\rho_E)}.$$

3.1. Fisher Information Ratio

Based on the CRLB, the secrecy design problems can be framed as maximizing the FI at the FC while minimizing the FI at Eve. Therefore, we introduce the FI ratio R as an intermediate step to achieve these secrecy requirements, with a higher R indicating improved secrecy. The FI ratio is defined as follows,

$$\begin{aligned} R(\eta,\theta) &\triangleq \frac{\mathbf{I}(\eta,\theta,\rho_F)}{\mathbf{I}(\eta,\theta,\rho_E)} \\ &= \frac{(1-2\rho_F)^2(\rho_E+(1-2\rho_E)Q(\eta-\theta))}{(1-2\rho_E)^2(\rho_F+(1-2\rho_F)Q(\eta-\theta))} \\ &\times \frac{(1-\rho_E-(1-2\rho_E)Q(\eta-\theta))}{(1-\rho_F-(1-2\rho_F)Q(\eta-\theta))} \\ &= \frac{\left(\frac{\rho_E}{1-2\rho_E}+Q(\eta-\theta)\right)\left(\frac{1-\rho_E}{1-2\rho_E}-Q(\eta-\theta)\right)}{\left(\frac{\rho_F}{1-2\rho_F}+Q(\eta-\theta)\right)\left(\frac{1-\rho_F}{1-2\rho_F}-Q(\eta-\theta)\right)} \\ &= \frac{-Q^2(\eta-\theta)+Q(\eta-\theta)+\frac{\rho_E(1-\rho_E)}{(1-2\rho_E)^2}}{-Q^2(\eta-\theta)+Q(\eta-\theta)+\frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2}} \\ &= 1+\frac{\frac{\rho_E(1-\rho_E)}{(1-2\rho_E)^2}-\frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2}}{-\left(Q^2(\eta-\theta)-\frac{1}{2}\right)^2+\frac{1}{4}+\frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2}}. \end{aligned} \quad (5)$$

Notice that the function $\frac{\rho(1-\rho)}{(1-2\rho)^2}$ is a monotone increasing function for $\rho < 0.5$, and since $\rho_F < \rho_E < \frac{1}{2}$, then $\frac{\rho_E(1-\rho_E)}{(1-2\rho_E)^2} - \frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2} > 0$. Therefore, $R(\eta,\theta)$ is a decreasing function of $Q(\eta-\theta)$ when $Q(\eta-\theta) \in (0,0.5]$ and increasing function of $Q(\eta-\theta)$ when $Q(\eta-\theta) \in [0.5,1)$. The supremum of the FI ratio,

$$\sup(R) = \frac{\rho_E(1-\rho_E)(1-2\rho_F)^2}{\rho_F(1-\rho_F)(1-2\rho_E)^2}, \quad (6)$$

is achieved when $Q(\eta-\theta)$ approaches to 0 or 1. However, such choices of Q are not desirable in that they result in $f(\eta-\theta) = -\frac{dQ(\eta-\theta)}{d\eta} = 0$ and further the FI at the FC, $NI(\theta,\eta,\rho_F)$=0, indicating that the FC does not obtain any useful information for estimation either. Nevertheless, as R is a continuous function of Q, to achieve the design goal, we can choose $Q(\eta-\theta)$ close to 0 or 1 and increase the number of sensors N. In other words, we need to design η and N jointly to realize maximum achievable performance at the FC and secrecy against Eve.

3.2. Asymptotic Perfect Secrecy

In order to achieve APS against Eve, we require

$$\mathbf{I}(\mathbf{W};\theta) = NI(\eta,\theta,\rho_E) \to 0, \;\; N \to \infty. \quad (7)$$

Naturally, we also require the SN to have an asymptotic perfect estimation (APE) at the FC, i.e.,

$$\mathbf{I}(\mathbf{V};\theta) = NI(\eta,\theta,\rho_E) \to \infty, \;\; N \to \infty. \quad (8)$$

Notice that when the FC has noiseless channels such that $\rho_F = 0$, the maximum FI ratio $\sup(R) = \infty$, indicating it is possible to simultaneously achieve both APE and APS by choosing the appropriate η as a function of N. Next, we demonstrate how to do so for the case where the observation noises are Gaussian distributed, with similar design approaches employed for other noise distributions.

4. ESTIMATION IN GAUSSIAN NOISE

We now consider the case where the observation noise, Z_i, follows the standard Gaussian distribution with zero mean and unit variance, where $f(x) = \frac{1}{\sqrt{2\pi}}e^{\frac{-x}{2}}$. According to the Mills ratio [24], $x+1 > \frac{f(x)}{Q(x)} > x$, we have

$$\frac{f(x)}{xQ(x)} \to 1, \;\; \text{as} \;\; x \to \infty.$$

Selecting η such that $e^{\frac{-(\eta-\theta)^2}{2}} = N^{\frac{-2}{3}}$, results in $\eta = \sqrt{\frac{4}{3}\log N}+\theta$. Thus, by choosing $\eta = \sqrt{\frac{4}{3}\log N}$, $\eta \gg \theta$ for a fixed but unknown θ, and N sufficiently large, $e^{-(\eta-\theta)^2} \propto N^{\frac{-3}{4}}$. As a result, the total FI at the FC

$$\begin{aligned} N\mathbf{I}_F &\propto N(\eta-\theta)f(\eta-\theta) = N(\eta-\theta)\frac{1}{\sqrt{2\pi}}e^{\frac{-(\eta-\theta)^2}{2}} \\ &\propto N\sqrt{\frac{4}{3}\log N}\,N^{\frac{-2}{3}} = N^{\frac{1}{3}}\sqrt{\frac{4}{3}\log N} \to \infty. \end{aligned} \quad (9)$$

The total FI at Eve is,

$$\begin{aligned} N\mathbf{I}_E &\propto Nf^2(\eta-A) = N\frac{1}{2\pi}e^{-(\eta-\theta)^2} \\ &\propto N\left(N^{\frac{-2}{3}}\right)^2 = N^{\frac{-1}{3}} \to 0. \end{aligned} \quad (10)$$

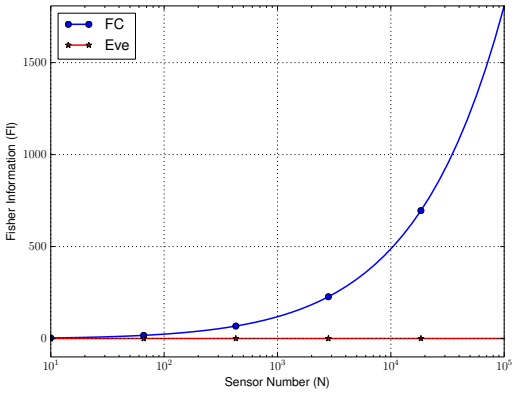

Fig. 2: Total Fisher Information for the FC and Eve with different number of sensors given $\theta = 1, \eta = \sqrt{\frac{4}{3}\log N}$.

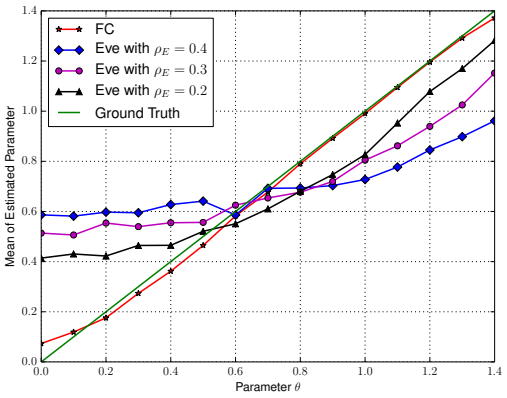

Fig. 3: Mean of estimated signals by the FC and Eve with different BERs. The FC's estimation is close to the ground truth.

In summary, by choosing $\eta = \sqrt{\frac{4}{3}\log N}$, then both APS and APE can be achieved under standard Gaussian observation noise. Other observations noise can be analyzed in a similar fashion.

5. SIMULATION

In this section, we compare the estimation performance at Eve and at the FC via the distributed estimation of a fixed but unknown signal with zero mean additive white Gaussian noise. Specifically, the sensor observations are given in Equation (1), where $Z_i \sim \mathcal{N}(0,1)$ is the normalized observation noise following a standard Gaussian distribution. Both the FC and Eve employ Maximum Likelihood Estimation (MLE) to obtain $\hat{\theta}_F$ and $\hat{\theta}_E$ based on $\mathbf{V}$ and $\mathbf{W}$, respectively. The two MSE estimates are

$$\begin{aligned} \hat{\theta}_F &= \left(\eta - Q^{-1}\left(\frac{\bar{V}-\rho_F}{1-2\rho_F}\right)\right) \\ \hat{\theta}_E &= \left(\eta - Q^{-1}\left(\frac{\bar{W}-\rho_E}{1-2\rho_E}\right)\right), \end{aligned} \tag{11}$$

where $\bar{V}$, $\bar{W}$ are the mean of received outputs for the FC and Eve, respectively.

We first examine the system secrecy when the FC has a perfect channel, $\rho_F = 0$, Eve has a noisy channel, $\rho_E = 0.40$, and the threshold $\eta = \sqrt{\frac{4}{3}\log N}$. First, the FI as a function of N for $\theta = 1$ is displayed in Fig. 2. We see that the FI at the FC is increasing with the number of sensors, while the FI at Eve is close to zero, consistent with the proofs for Equation (9) and (10).

Under the same conditions of η, ρ_E and ρ_F, via Monte-Carlo simulation with 1000 trials, we plot the resulting mean and MSE of the estimated parameters θ_F and θ_E by the FC and Eve in Fig 3 and Fig. 4, respectively, where $\theta \in [0, 1.4]$,

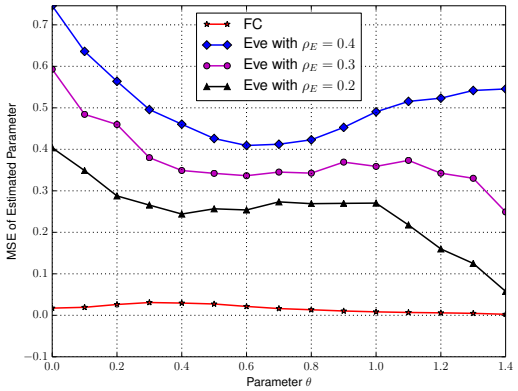

Fig. 4: MSE of estimated signals by the FC and Eves with different BERs.

and the number of sensors is fixed at $N = 100$. In both figures, the trends show that Eve, with a larger BSC BER, cannot accurately estimate θ. Meanwhile, the FC can almost perfectly estimate the parameter, where the estimated parameter mean is close to the ground truth in Fig 3 and the MSE is close to zero in Fig 4.

6. CONCLUSION

We considered the asymptotic secrecy design problem in distributed estimation for large SNs that were subject to an eavesdropping attack. The maximum achievable secrecy performance was derived and it was proved that under the condition that Eve has a noisy channel and the FC has a noiseless channel, both APS and APE can be achieved. The secrecy design method in this paper might greatly enhance the secrecy in distributed estimation for large sensor networks.

7. REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292 – 2330, 2008.

[2] Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi-Wing Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[3] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct 2015.

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 8, no. 2, pp. 2–23, Second 2006.

[5] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *Automation Science and Engineering, IEEE Transactions on*, vol. PP, no. 99, pp. 1–13, 2015.

[6] M. Baldi, M. Bianchi, N. Maturo, and F. Chiaraluce, "A physical layer secured key distribution technique for IEEE 802.11g wireless networks," *Wireless Communications Letters, IEEE*, vol. 2, no. 2, pp. 183–186, April 2013.

[7] S. Mathur, A. Reznik, Chunxuan Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *Wireless Communications, IEEE*, vol. 17, no. 5, pp. 63–70, October 2010.

[8] H. Taha and E. Alsusa, "A MIMO precoding based physical layer security technique for key exchange encryption," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, May 2015, pp. 1–5.

[9] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, 2011.

[10] B. Kailkhura, V. S. Siddhardh Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: a survey," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 40–46, June 2015.

[11] A. Willsky, M. Bello, D. Castanon, B. Levy, and G. Verghese, "Combining and updating of local estimates and regional maps along sets of one-dimensional tracks," *IEEE Transactions on Automatic Control*, vol. 27, no. 4, pp. 799–813, Aug 1982.

[12] D. Castanon and D. Teneketzis, "Distributed estimation algorithms for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 30, no. 5, pp. 418–425, May 1985.

[13] Y. A. Chau and E. Geraniotis, "Distributed multisensor parameter estimation in dependent noise," *IEEE Transactions on Communications*, vol. 40, no. 2, pp. 373–384, Feb 1992.

[14] J. A. Gubner, "Distributed estimation and quantization," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1456–1459, Jul 1993.

[15] T.C. Aysal and K.E. Barner, "Sensor data cryptography in wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 273–289, June 2008.

[16] X. Guo, A. S. Leong, and S. Dey, "Power allocation for distortion minimization in distributed estimation with security constraints," in *2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, June 2014, pp. 299–303.

[17] U. A. Khan and A. M. Stankovic, "Secure distributed estimation in cyber-physical systems," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2013, pp. 5209–5213.

[18] Lingxuan Hu and David Evans, "Using directional antennas to prevent wormhole attacks," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2004, San Diego, California, USA*, 2004.

[19] Su Yi, Yong Pei, and Shivkumar Kalyanaraman, "On the capacity improvement of ad hoc wireless networks using directional antennas," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, New York, NY, USA, 2003, MobiHoc '03, pp. 108–116, ACM.

[20] H.L. Van Trees, *Detection, Estimation, and Modulation Theory*, Detection, Estimation, and Modulation Theory. Wiley, 2004.

[21] A. Vempaty, H. He, B. Chen, and P. K. Varshney, "On quantizer design for distributed bayesian estimation in sensor networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 20, pp. 5359–5369, Oct 2014.

[22] H. Chen and P. K. Varshney, "Performance limit for distributed estimation systems with identical one-bit quantizers," *IEEE Transactions on Signal Processing*, vol. 58, no. 1, pp. 466–471, Jan 2010.

[23] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory*, Prentice Hall PTR, 1993.

[24] M. R. Sampford, "Some inequalities on mill's ratio and related functions," *Ann. Math. Statist.*, vol. 24, no. 1, pp. 130–132, 03 1953.