ASYMPTOTIC PERFECT SECRECY IN DISTRIBUTED DETECTION AGAINST A GLOBAL EAVESDROPPER

Jun Guo[⋆] *Xia Li*[⋆] *Uri Rogers*[†] *Hao Chen*[⋆]

[⋆] ECE, Boise State Univ
[†] ECE, Eastern Washington Univ

ABSTRACT

This paper examines the secrecy in distributed detection under threat of a global eavesdropper (Eve) which has access to all sensors decisions. To measure secrecy, we compare the detection performance at the fusion center (FC) and at Eve in terms of their respective Kullback-Leibler Divergence (KLD). When the channels between sensors and the FC are noiseless and the channels between sensors and Eve are noisy, we show that the KLD ratio between the FC and Eve can be made arbitrarily large, provided the log-likelihood ratio at local sensors is unbounded. As a result, a perfect secrecy can be achieved asymptotically by making the KLD at Eve arbitrarily small with almost 0 detectability while keeping the KLD at the FC arbitrary large, for an almost error-free detection. This result reveals an intriguing relationship between networks size and networks secrecy.

Index Terms— Asymptotic Perfect Secrecy, Distributed Detection, Eavesdropping, Wireless Sensor Networks

1. INTRODUCTION

Comprised of a large number of low cost, low power sensors, wireless sensor networks (WSNs) are widely employed in many applications such as environmental monitoring, healthcare, and diagnostics of complex systems [1]. As a key function in WSNs, distributed detection has been an important and active research area over the past several decades [2–10]. In the presence of cyber-attacks, WSNs must be carefully designed to meet both the security and secrecy requirements.

Recently, several attempts were made to address the issue of eavesdropping for distributed detection, when an attacker has partial or full access to sensor outputs [11]. Marano et al. designed censoring rules for local sensors based on the assumption that the attacker does not have direct access to sensors data but can monitor the transmission activity of the channel [12]. For a two-sensor network where the attacker has partial access to the WSN, Li et al. jointly designed sensor quantizer and fusion rules to maximize the Fusion Center (FC) detection probability by constraining both the FC false alarm probability and the attacker detection probability [13]. Performance metric such as Kullback-Leibler Divergence (KLD) has been widely used for asymptotic performance measure as it represents the exponential decay of missed detection error probability in the Nayman-Pearson formulation [14]. Nadenla et al. considered the secrecy problem in distributed detection against eavesdropping attacks for WSNs in parallel networks with N sensors, one FC and one global Eavesdropper (Eve), where the goal is to maximize KLD at the FC for one sensor, D_F, under the constraint that KLD at Eve for one sensor, D_E, is no more than a prespecified threshold T_E [15]. While these approaches are effective in accomplishing their stated objectives, none provide asymptotic perfect secrecy (APS), as Eve still receives some useful information. For example, since $T_E \neq 0$, as the number of sensors N increases, the overall detection performance at Eve will improve exponentially regardless of how noisy the Eve's channels are, and become nearly perfect when N is sufficiently large! Although carefully designed encryption schemes may provide a nearly perfect secrecy solution [16], they are often too complicated to be implemented and the latency associated with the long block codes is not desired in WSNs with stringent time delay and power constraints.

In this paper, we investigate the secrecy problem in distributed detection for WSNs in parallel networks with N sensors, one FC and one global Eve, similar as in [15]. Considering the detection performance as a function of KLD at the FC and at Eve for all N sensors, $\mathbb{D}_{\mathbb{F}}$ and $\mathbb{D}_{\mathbb{E}}$, the perfect secrecy is achieved if $\mathbb{D}_{\mathbb{F}}$ can be made arbitrarily large and $\mathbb{D}_{\mathbb{E}} \to 0$. Towards this end, we first study the behavior of likelihood ratio quantizer (LRQ) in terms of the ratio between $\mathbb{D}_{\mathbb{F}}$ and $\mathbb{D}_{\mathbb{E}}$. We discover a novel LRQ property of the aforementioned KLD ratio $\mathbb{D}_{\mathbb{F}}/\mathbb{D}_{\mathbb{E}}$ which can be made arbitrarily large, by carefully choosing the local sensor decision rules. As an application of this novel LRQ property when the FC channels are noiseless and Eve channels are noisy, the constraint of $\mathbb{D}_{\mathbb{F}} \geq T_F$ and $\mathbb{D}_{\mathbb{E}} \leq T_E$ can be satisfied simultaneously, for any arbitrary $T_F, T_E > 0$, as $N \to \infty$. In other words, the FC and local sensors can share data without being snooped by Eve when Eve has a noisy channel. Contrary to the belief that larger networks are less secure, our result shows that secrecy can be improved and APS can be achieved by *increasing* the network size.

2. DISTRIBUTED DETECTION WITH A GLOBAL EAVESDROPPER

We consider binary distributed hypotheses testing in a parallel WSN consisting of N sensors as shown in Fig. 1. Let the hypotheses H_0 and H_1 represent the target absence and presence, respectively. Upon observing the phenomenon X_i, sensor i makes a binary decision $U_i \in \{0,1\}$ based on its decision rule γ_i, such that $P(U_i = 1) = \gamma_i(X_i),\ i = 1,2,\ldots,N$. The sensors and the FC are connected via binary symmetric channels (BSC) [17] [18]. Sensor i sends the decision U_i to the FC over a BSC with transition error probability (TEP) $\rho_{F,i} < \frac{1}{2}$; meanwhile, a global Eve also observes the sensor decisions, U_i, with a BSC with TEP $\rho_{E,i} < \frac{1}{2}$. We assume that Eve's channels are noisier than the FC's, $\rho_{E,i} > \rho_{F,i}$ by the use of secrecy keys or directional antennas at sensors [19] [20]. We assume the channels are also independent and identically such that $\rho_F = \rho_{F,i}$, $\rho_E = \rho_{E,i}$, $1 \le i \le N$. Let $p_k(X_i) = p(X_i; H_k)$ be the probability density function (pdf) under H_k at sensor i, where $k = 0, 1$. We assume that $p_0(X_i)$ and $p_1(X_i)$ are continuous pdfs with no point mass and sensors observations are independent and identically distributed (i.i.d.),

$$p(X_1, X_2, \ldots, X_N; H_j) = \prod_{i=1}^{N} p(X_i; H_j),\ \ j = 0, 1,$$

where $i = 1, \ldots, N$. The cases where the sensor observations/channels are independent but not identical can be analyzed in a similar fashion.

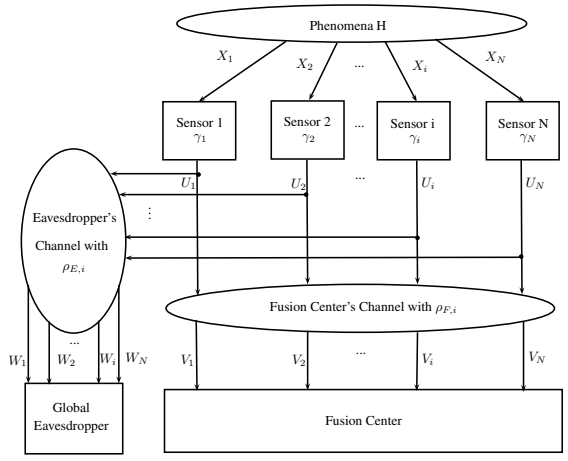

Fig. 1. Distributed detection with a global Eve.

Under the i.i.d. condition, it has been shown that the identical sensor decision rule design where each sensor uses the same likelihood ratio test (LRT) with the same threshold is asymptotically optimal [8, 21]. That is, the optimal decision rule $\gamma_i(\cdot)$ at sensor i is given by

$$\gamma_i(x) = \gamma(x) = \begin{cases} 1 & \frac{p_1(x)}{p_0(x)} \ge \eta \\ 0 & \frac{p_1(x)}{p_0(x)} < \eta. \end{cases} \tag{1}$$

Let the false alarm probability of the ith local sensor be $\alpha_i = P(U_i = 1; H_0) = P\left(\frac{p_1(X_i)}{p_0(X_i)} > \eta_i; H_0\right)$ and the detection probability be $\beta_i = P(U_i = 1; H_1) = P\left(\frac{p_1(X_i)}{p_0(X_i)} > \eta_i; H_1\right)$. Because of the i.i.d. condition on both detection and transmission, we have $\alpha = \alpha_i;\ \ \beta = \beta_i;\ \ \rho_F = \rho_{F,i};\ \ \rho_E = \rho_{E,i}$, where $i = 1, \ldots, N$. And the relationship between α_i and β_i is given by [22]

$$\frac{d\beta_i}{d\alpha_i} = \eta_i = \eta. \tag{2}$$

Therefore, if $\ln\left(p_1(X_i)/p_0(X_i)\right)$ is unbounded, then $\eta \to \infty$ when $\alpha, \beta \to 0$, or $\eta \to 0$ when $\alpha, \beta \to 1$.

Due to the BSC between the local sensors and the FC, the received decision V_i, from the ith local sensor at the FC has the following performance,

$$\begin{aligned} P(V_i = 1; H_0) &= \alpha_F = \alpha(1-\rho_F) + (1-\alpha)\rho_F \\ &= \rho_F + (1-2\rho_F)\alpha, \\ P(V_i = 1; H_1) &= \beta_F = \beta(1-\rho_F) + (1-\beta)\rho_F \\ &= \rho_F + (1-2\rho_F)\beta. \end{aligned} \tag{3}$$

Similarly, at Eve, the received decision W_i, has the following performance,

$$\begin{aligned} P(W_i = 1; H_0) &= \alpha_E = \rho_E + (1-2\rho_E)\alpha, \\ P(W_i = 1; H_1) &= \beta_E = \rho_E + (1-2\rho_E)\beta. \end{aligned} \tag{4}$$

3. SECRECY IN DISTRIBUTED DETECTION

3.1. KLD in Distributed Detection

When the decision center observations are i.i.d., Stein's lemma [6] and large deviation theory [23, 24] provide a bound on the probability of missed detection (P_m) via the error exponent $D(p_0(\cdot)||p_1(\cdot))$, where p_0, p_1 are the pdf under H_0 and H_1 hypotheses, respectively. Specifically, $-\lim_{N\to\infty} \frac{1}{N} \log P_m \le D(p_0(\cdot)||p_1(\cdot))$ when the false alarm probability (P_f) is constrained to be less than a fixed constant, and the equality can be achieved by the optimal LRT or other asymptotic optimal detectors such as type based detectors so that [16]

$$P_m \approx e^{-ND(p_0(\cdot)||p_1(\cdot))} \tag{5}$$

For binary sensor decisions with $P(U_i = 1; H_0) = \alpha$ and $P(U_i = 1; H_1) = \beta$, we have $P(U_i = 0; H_0) = 1 - \alpha$ and

$P(U_i = 0; H_1) = 1 - \beta$, the KLD [25] for each sensor is

$$D\left(p_0||p_1\right) = \alpha \log \frac{\alpha}{\beta} + (1-\alpha) \log \frac{(1-\alpha)}{(1-\beta)} = D\left(\alpha, \beta\right).$$

3.2. Asymptotic Perfect Secrecy

The system secrecy is measured by information leakage of the total sensors to Eve when the FC is required to perform distributed detection subject to required system performance constraints on P_m and P_f. The KLD of each received sensor decision V_i at the FC is $D_F = D(\alpha_F, \beta_F)$ and KLD of each received sensor decisions W_i at the Eve is $D_E = D(\alpha_E, \beta_E)$. Owing to i.i.d. condition, the total KLD at the FC is introduced to measure the system secrecy, which is $\mathbb{D}_{\mathbb{F}} = N \times D_F$, similarly, $\mathbb{D}_{\mathbb{E}} = N \times D_E$. Therefore, from (5), with optimal detectors, $P_m \approx e^{-\mathbb{D}_{\mathbb{F}}}$ at the FC and $P_m \approx e^{-\mathbb{D}_{\mathbb{E}}}$ at Eve for any given P_f–probability of false alarm constraints. Using the relationship between the KLD and the detection performance, we formalize the secrecy problem as two constrained optimization problems

$$\mathbb{D}_{\mathbb{F}} \geq T_F, \;\; \text{s.t.} \min \;\; \mathbb{D}_{\mathbb{E}}, \tag{6}$$

where $T_F > 0$, is a threshold to guarantee the overall detection performance of the FC, meanwhile if $\mathbb{D}_{\mathbb{E}}$ is 0, perfect secrecy is achieved. Or conversely, to achieve perfect secrecy, one seeks to

$$\max \;\; \mathbb{D}_{\mathbb{F}}, \;\; \text{s.t.} \;\; \mathbb{D}_{\mathbb{E}} \to 0, \;\; \text{as} \;\; N \to \infty \tag{7}$$

In [15], authors re-formulate the optimization problem as $\max(\mathbb{D}_{\mathbb{F}} - \mathbb{D}_{\mathbb{E}}) = \max(N(D_F - D_E))$; however, it may not be an ideal metric of measuring asymptotically perfect secrecy. Elaborations on this would give in section 4. We, instead, propose to use the KLD ratio between the FC and Eve for all N sensors (8) in that a novel property of the KLD ratio can be used to develop a scheme that achieves asymptotic perfect secrecy.

$$R(\alpha) = \frac{\mathbb{D}_{\mathbb{F}}}{\mathbb{D}_{\mathbb{E}}} = \frac{N \times D_F}{N \times D_E} = \frac{N \times D(\alpha_F, \beta_F)}{N \times D(\alpha_E, \beta_E)}. \tag{8}$$

Theorem 1. *For a WSN with the TEP at the FC, ρ_F and the TEP at Eve, ρ_e, if the local sensor log-likelihood ratio $\ln\left(p_1(x)/p_0(x)\right)$ is unbounded from above, then the KLD ratio between the FC and Eve $R(0) = \lim_{\alpha \to 0} R(\alpha, \beta\left(\alpha\right)) = \frac{(1-2\rho_F)^2(1-\rho_E)\rho_E}{(1-2\rho_E)^2(1-\rho_F)\rho_F}$; similarly, if $\ln\left(p_1(x)/p_0(x)\right)$ is unbounded from below, then the KLD ratio between the FC and Eve, $R(1) = \lim_{\alpha \to 1} R(\alpha, \beta\left(\alpha\right)) = \frac{(1-2\rho_F)^2(1-\rho_E)\rho_E}{(1-2\rho_E)^2(1-\rho_F)\rho_F}$.*

Proof. If $\ln\left(p_1(x)/p_0(x)\right)$ is unbounded below, then as $\alpha \to 1$, $\eta \to 0$, applying L'Hopital's rule to the ratio $R(\alpha)$,

$$\begin{aligned}
R(1) &= \lim_{\alpha \to 1} \frac{\frac{d}{d\alpha} D\left(\alpha_F, \beta_F\right)}{\frac{d}{d\alpha} D\left(\alpha_E, \beta_E\right)} \\
&= \lim_{\alpha \to 1} \frac{\frac{d\alpha_F}{d\alpha}\left(\frac{d}{d\alpha_F} D\left(\alpha_F, \beta_F\right)\right)}{\frac{d\alpha_E}{d\alpha}\left(\frac{d}{d\alpha_E} D\left(\alpha_E, \beta_E\right)\right)} \\
&= \lim_{\substack{\alpha \to 1 \\ \beta \to 1 \\ \eta \to 0}} \frac{(1-2\rho_F)\left(\eta \frac{\beta_F - \alpha_F}{(1-\beta_F)\beta_F} + \log \frac{\alpha_F(1-\beta_F)}{\beta_F(1-\alpha_F)}\right)}{(1-2\rho_E)\left(\eta \frac{\beta_E - \alpha_E}{(1-\beta_E)\beta_E} + \log \frac{\alpha_E(1-\beta_E)}{\beta_E(1-\alpha_E)}\right)} = \\
&\lim_{\substack{\alpha \to 1 \\ \beta \to 1 \\ \eta \to 0}} \frac{(1-2\rho_F)^2(\beta-\alpha)\left(\frac{\eta}{(1-\beta_F)\beta_F} + \frac{\log\left(1+\frac{\alpha_F-\beta_F}{\beta_F(1-\alpha_F)}\right)}{\beta_F - \alpha_F}\right)}{(1-2\rho_E)^2(\beta-\alpha)\left(\frac{\eta}{(1-\beta_E)\beta_E} + \frac{\log\left(1+\frac{\alpha_E-\beta_E}{\beta_E(1-\alpha_E)}\right)}{\beta_E - \alpha_E}\right)}.
\end{aligned}$$

Since

$$\lim_{x \to 0} \frac{\log(1+x)}{x} = 1,$$

$$\lim_{\substack{\alpha \to 1 \\ \beta \to 1}} \frac{\log\left(1 + \frac{\alpha_F - \beta_F}{\beta_F(1-\alpha_F)}\right)}{\beta_F - \alpha_F} = \lim_{\substack{\alpha \to 1 \\ \beta \to 1}} \frac{-1}{\beta_F\left(1-\alpha_F\right)},$$

Therefore,

$$\begin{aligned}
R\left(1\right) &= \lim_{\substack{\alpha \to 1 \\ \beta \to 1 \\ \eta \to 0}} \frac{(1-2\rho_F)^2\left(\frac{\eta}{(1-\beta_F)\beta_F} - \frac{1}{\beta_F(1-\alpha_F)}\right)}{(1-2\rho_E)^2\left(\frac{\eta}{(1-\beta_E)\beta_E} - \frac{1}{\beta_E(1-\alpha_E)}\right)} \\
&= \frac{(1-2\rho_F)^2\left(1-\rho_E\right)\rho_E}{(1-2\rho_E)^2\left(1-\rho_F\right)\rho_F}.
\end{aligned}$$

Similarly, if $\ln\left(p_1(x)/p_0(x)\right)$ is unbounded above, then as $\alpha \to 0$, $\eta \to \infty$,

$$R(0) = \frac{(1-2\rho_F)^2\left(1-\rho_E\right)\rho_E}{(1-2\rho_E)^2\left(1-\rho_F\right)\rho_F} = R(1). \tag{9}$$

□

Remark 1. When the FC's channels are perfect such that $\rho_F = 0$ and Eve's channels are noisy such that $\rho_E > 0$, we have $R(1) = \infty$ or $R(0) = \infty$, given the log-likelihood ratio is unbounded from at least one end. This can be used to design APS distributed detectors. Specifically, if local sensors operate at either end of the receiver operating characteristic (ROC) curves, Eve over a noisier BSC will be unable to obtain any useful information from local sensors. As a result of this property, we show that asymptotic perfect secrecy is achievable.

4. EXPERIMENTAL RESULTS

In this section, we illustrate the performance trade-offs at Eve and the FC via the classic distributed detection of a constant signal in zero mean additive white Gaussian noise,

$$H_1: \quad X_i = A + Z_i$$

$$H_0: \quad X_i = Z_i,$$

where $Z_i \sim \mathcal{N}(0,1)$ is the normalized observation noise with standard Gaussian distribution, $A > 0$ is the constant signal to be detected, and signal-to-noise ratio, SNR $= A^2$. In this settings, the log-likelihood ratio $\log p_1(x_i)/p_0(x_i) = Ax - \frac{A^2}{2}$ is unbounded. And the detection probability is given by $\beta(\alpha) = Q(Q^{-1}(\alpha) - 10^{\text{SNR}/20})$.

We first examine system secrecy when the FC has a non-perfect channel, $\rho_F = 0.01$ to validate the results obtain in Theorem 1. The upper subfigure of Fig. 2 shows the performance comparison between the FC and Eve in terms of KLD when N = 1, SNR $= 0$ dB $(A = 1)$ and $\rho_E = 0.3$; the middle plot shows the corresponding KLD ratio where the maximum achievable KLD ratio, $R = 129.7$, is achieved at both end of the ROC curve, and the marker stars indicate the limit derived in (9), which is consistent with the proof in Section 3.

To achieve APS, we compare the detection performance at Eve and the FC in terms of their total KLD $\mathbb{D}_{\mathbb{E}}$ and $\mathbb{D}_{\mathbb{F}}$, where $\mathbb{D}_{\mathbb{E}}$ is set as $\frac{0.02}{\sqrt{N}}$, SNR $= 0$ dB, $\rho_F = 0$, $\rho_E = 0.3$ (Fig. 3). It is shown that as N increases, $\mathbb{D}_{\mathbb{E}} \to 0$ and $\mathbb{D}_{\mathbb{F}} \to \infty$, i.e., the FC can make perfect detection and the detectability at Eve would essentially be negligible.

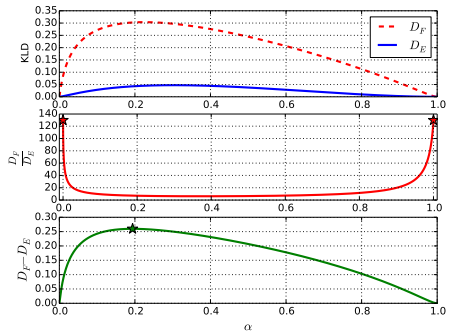

Fig. 2. KLD Performance of the FC and Eve when $N = 1$.

In Fig. 4, ROC curves are plotted using two different metrics to measure secrecy, the total KLD difference [15] and the total KLD ratio. Other conditions are set as SNR $= 0$ dB, $\rho_F = 0$, $\rho_E = 0.3$. If the KLD ratio is chosen as the metric and $\mathbb{D}_{\mathbb{E}}$ is constrained at 0.02 for different N, the corresponding Eve curves are almost overlapped and close to diagonal line which implies 0 detectability. Meanwhile, the detectability of the FC keeps increasing as the number of sensors increase. However, if the KLD difference, $\max(N(D_F - D_E))$ in Fig. 2, is chosen as the metric, where $D_E = 0.041$, even though the corresponding FC's detection performance is nearly perfect, we can see that Eve's detectability is growing as N increases; when $N \to \infty$, Eve's detection performance is going to be as good as the FC's. All of the prior simulations support our claim that if KLD ratio is chosen as the secrecy metric in the distributed detection system, APS can be achieved.

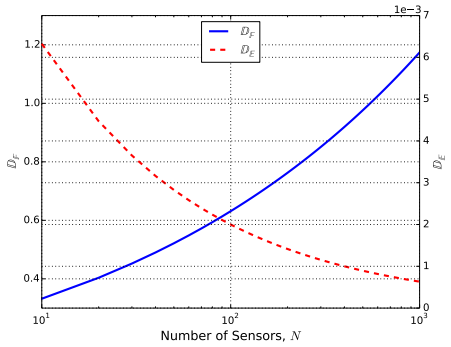

Fig. 3. The KLD at the FC and at Eve for N sensors.

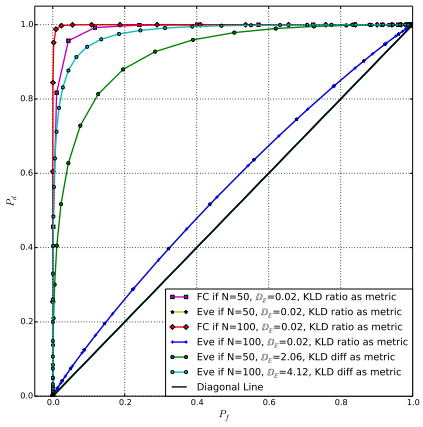

Fig. 4. ROC curves for the FC and Eve.

5. CONCLUSION

We proposed to use the KLD ratio as a secrecy design metric for distributed detection subject to eavesdropping attacks. We proved that under the condition that Eve has a noisy channel and the FC has a noiseless channel, APS is possible between local sensors and the FC in the presence of a global Eve. Interestingly, our result shows that WSNs becomes more secure against eavesdropping attacks as the number of nodes increases, until ultimately perfect secrecy is achieved.

6. REFERENCES

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

[2] A. Swami, Q. Zhao, Hong Y.-W., and L. Tong, *Wireless Sensor Networks:Signal Processing and Communications Perspectives*, John Wiley & Sons, Ltd., 2007.

[3] Pramod K. Varshney, *Distributed Detection and Data Fusion*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1st edition, 1996.

[4] R. Viswanathan and P.K. Varshney, "Distributed detection with multiple sensors i. fundamentals," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54–63, Jan 1997.

[5] R.S. Blum, S.A. Kassam, and H.V. Poor, "Distributed detection with multiple sensors i. advanced topics," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 64–79, Jan 1997.

[6] J.-F. Chamberland and V.V. Veeravalli, "Decentralized detection in sensor networks," *Signal Processing, IEEE Transactions on*, vol. 51, no. 2, pp. 407–416, Feb 2003.

[7] J. Chamberland and V.V. Veeravalli, "Wireless sensors in distributed detection applications," *Signal Processing Magazine, IEEE*, vol. 24, no. 3, pp. 16–25, May 2007.

[8] J. N. Tsitsiklis, "Decentralized detection," in *Advances in Signal Processing*, H. V. Poor and J. B. Thomas, Eds., vol. 2, pp. 297–344. JAI Press, 1993.

[9] Z. Chair and P.K. Varshney, "Optimal data fusion in multiple sensor detection systems," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. AES-22, no. 1, pp. 98–101, Jan 1986.

[10] B. Chen, L. Tong, and P. K. Varshney, "Channel-aware distributed detection in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 23, no. 4, pp. 16–26, July 2006.

[11] B. Kailkhura, V. S. Siddhardh Nadendla, and P. K. Varshney, "Distributed Inference in the Presence of Eavesdroppers: A Survey," *ArXiv e-prints*, Feb. 2015.

[12] S. Marano, V. Matta, and P.K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *Signal Processing, IEEE Transactions on*, vol. 57, no. 5, pp. 1976–1986, May 2009.

[13] Zuxing Li, T.J. Oechtering, and J. Jalden, "Parallel distributed neyman-pearson detection with privacy constraints," in *Communications Workshops (ICC), 2014 IEEE International Conference on*, June 2014, pp. 765–770.

[14] S. Marano, V. Matta, and Lang Tong, "Distributed detection in the presence of byzantine attacks," *Signal Processing, IEEE Transactions on*, vol. 57, no. 1, pp. 16–29, Jan 2009.

[15] V.S.S. Nadendla, Hao Chen, and P.K. Varshney, "Secure distributed detection in the presence of eavesdroppers," in *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*, Nov 2010, pp. 1437–1441.

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

[17] G. Liu, B. Xu, M. Zeng, and H. Chen, "Distributed estimation over binary symmetric channels in wireless sensor networks," *Wireless Sensor Systems, IET*, vol. 1, no. 2, pp. 105–109, June 2011.

[18] W.W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*, Wireless Communications and Mobile Computing. Wiley, 2010.

[19] Lingxuan Hu and David Evans, "Using directional antennas to prevent wormhole attacks," 2004.

[20] 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.

[21] D. Warren and P. Willett, "Optimum quantization for detector fusion: some proofs, examples and pathology," *Journal of the Franklin Institute*, vol. 336, pp. 323–359, 1999.

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

[23] J.A. Bucklew, *Large deviation techniques in decision, simulation, and estimation*, Wiley-interscience publication. Wiley, 1990.

[24] Po-Ning Chen, "General formulas for the neyman-pearson type-ii error exponent subject to fixed and exponential type-i error bounds," *Information Theory, IEEE Transactions on*, vol. 42, no. 1, pp. 316–323, Jan 1996.

[25] S. Kullback and R. A. Leibler, "On information and sufficiency," *Ann. Math. Statist.*, vol. 22, no. 1, pp. 79–86, 03 1951.