Asymptotic Perfect Secrecy in Distributed Estimation for Large Sensor Networks

Jun Guo[⋆], Hao Chen[⋆] and Uri Rogers[†]

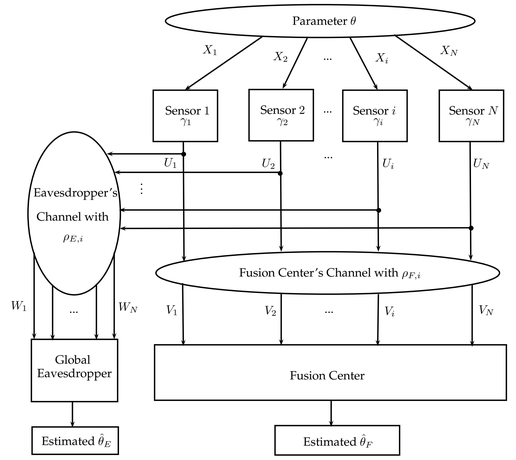
[⋆] Boise State University, [†] Eastern Washington University

BOISE STATE UNIVERSITY
COLLEGE OF ENGINEERING

Introduction

Large WSNs are widely employed in many applications, such as surveillance, health-care, cyber-physical systems, diagnostics of complex systems 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 WSNs, 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, and will be our focus. We focus on solving eavesdropping attacks against WSNs using physical-layer security approach. In this paper, we show that asymptotic perfect secrecy is possible by increasing the number of sensors.

Sensor Network Model



Secrecy Constrained Distributed Estimation Model.

- Sensor observations: $f(\mathbf{X}|\theta) = \prod_{i=1}^{N} f(X_i|\theta)$
- Estimation problem: $X_i = \theta + Z_i;\ \ i = 1, 2, \ldots, N,$ where Z_i is an additive i.i.d zero mean observation noise with pdf $f(\cdot)$
- I.I.D., quantizer: $U_i = \begin{cases} 1, & X_i > \eta \\ 0, & X_i \leq \eta \end{cases} \forall i,$
- Independent and identical BSC between sensors and the receivers where BER
  $\rho_{E,1} = \rho_{E,2} = \ldots = \rho_{E,N} = \rho_E$
  $\rho_{F,1} = \rho_{F,2} = \ldots = \rho_{F,N} = \rho_F$
- Channel qualities: $\rho_F < \rho_E$ by using beamforming or directional antenna
- Sensor outputs: $\begin{array}{l} \Pr(U_i = 1|\theta) = \beta = \Pr(\theta + Z_i > \eta) = Q(\eta - \theta), \\ \Pr(U_i = 0|\theta) = 1 - \beta = 1 - \Pr(U_i = 1|\theta), \end{array}$
- The observations at the FC and Eve: $\begin{array}{l} \Pr(V_i = 1|\theta) = (1 - 2\rho_F)\Pr(U_i = 1|\theta) + \rho_F, \\ \Pr(W_i = 1|\theta) = (1 - 2\rho_E)\Pr(U_i = 1|\theta) + \rho_E. \end{array}$

Estimation Performance: Fisher Information

- $I(\eta, \theta, \rho) = \frac{f^2(\eta-\theta)(1-2\rho)^2}{(\rho+(1-2\rho)Q(\eta-\theta))(1-\rho-(1-2\rho)Q(\eta-\theta))}$
- For unbiased estimation: $\epsilon_F \triangleq E\left(\hat{\theta} - \theta\right)^2 \geq \text{CRLB}(\mathbf{V}; \theta) = \frac{1}{\mathbf{I}(\mathbf{V};\theta)}$
- Fisher information at the FC: $\mathbf{I}(\mathbf{V}; \theta) \triangleq -E_{\mathbf{V}}\left(\frac{\partial^2 \log p(\mathbf{V};\theta)}{\partial \theta^2}\right) = NI(\eta, \theta, \rho_F)$

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.
- FI ratio R as an intermediate step to achieve these secrecy requirements, with a higher R indicating improved secrecy.
- $R(\eta, \theta) \triangleq \frac{\mathbf{I}(\eta,\theta,\rho_F)}{\mathbf{I}(\eta,\theta,\rho_E)} = 1 + \frac{\frac{\rho_E(1-\rho_E)}{(1-2\rho_E)^2} - \frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2}}{-\left(Q(\eta-\theta)-\frac{1}{2}\right)^2 + \frac{1}{4} + \frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2}}.$
- 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 $\frac{\rho_E(1-\rho_E)}{(1-2\rho_E)^2} - \frac{\rho_F(1-\rho_F)}{(1-2\rho_F)^2} > 0$
- $R(\eta, \theta)$ 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, $\sup(R) = \frac{\rho_E(1-\rho_E)(1-2\rho_F)^2}{\rho_F(1-\rho_F)(1-2\rho_E)^2}$
- Need to design η and N jointly to realize maximum achievable performance at the FC and secrecy against Eve

Asymptotic Perfect Secrecy and Asymptotic Perfect Estimation

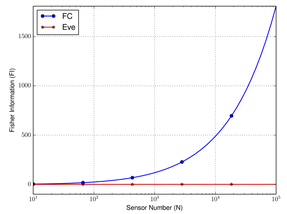
- Asymptotic perfect secrecy criterion: $\mathbf{I}(\mathbf{W}; \theta) = NI(\eta, \theta, \rho_E) \to 0,\ \ N \to \infty$
- Asymptotic perfect estimation criterion: $\mathbf{I}(\mathbf{V}; \theta) = NI(\eta, \theta, \rho_E) \to \infty,\ \ N \to \infty$
- Achieving asymptotic perfect: Since the FC has noiseless channels such that $\rho_F = 0$, the maximum FI ratio $\sup(R) = \infty$
- It is possible to simultaneously achieve both asymptotic perfect estimation and asymptotic perfect secrecy by choosing the appropriate η as a function of N.

An Example: Mean Estimation in Gaussian Noise

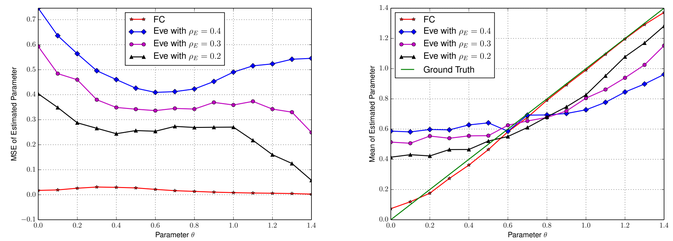
- Normalized $Z_i \sim \mathcal{N}(0, 1);\ \ f(x) = \frac{1}{\sqrt{2\pi}} e^{\frac{-x}{2}}.$
- Selecting η such that $e^{\frac{-(\eta-\theta)^2}{2}} = N^{\frac{-2}{3}}$, results in $\eta = \sqrt{\frac{4}{3}\log N} + \theta.$
- Choosing $\eta = \sqrt{\frac{4}{3}\log N}$, $\eta \gg \theta$ for a fixed but unknown θ, and N sufficiently large, $e^{-(\eta-\theta)^2} \propto N^{\frac{-3}{4}}.$
- Fusion Center: $NI_F \propto N\sqrt{\frac{4}{3}\log N}\, N^{\frac{-2}{3}} = N^{\frac{1}{3}}\sqrt{\frac{4}{3}\log N} \to \infty.$
- Eve: $NI_E \propto N\left(N^{\frac{-2}{3}}\right)^2 = N^{\frac{-1}{3}} \to 0.$
- Estimators: $\hat{\theta}_F = \left(\eta - Q^{-1}\left(\frac{\bar{V}-\rho_F}{1-2\rho_F}\right)\right); \hat{\theta}_E = \left(\eta - Q^{-1}\left(\frac{\bar{W}-\rho_E}{1-2\rho_E}\right)\right)$

Simulation Results

Parameter settings: $\theta \in [0, 1.4]$, $\rho_F = 0$, $\rho_E = 0.4$, $\eta = \sqrt{\frac{4}{3}\log N}$, $N = 100$.



Fisher Information for the FC and Eve with different number of sensors.



MSE of estimation and Mean of estimated parameter.

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
- We 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 by increasing the number of sensors.
- An example with Gaussian noise is given to show that 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.

Partial References

- D. Castanon and D. Teneketzis, "Distributed estimation algorithms for nonlinear systems," in IEEE Transactions on Automatic Control, vol. 30, no. 5, pp. 418-425, May 1985.
- J. A. Gubner, "Distributed estimation and quantization," IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 1456–1459, Jul 1993.
- 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.
- 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.

junguo@u.boisestate.edu, haochen@boisestate.edu, urogers@ewu.edu