

Master thesis project:
Assessment of Privacy in Distributed Detection Problems

This project involves a study of the privacy and secrecy in distributed detection problems. More specific, the study should concentrate on two standard setups. The first consists of two sensors and one fusion center. The second consists of a one sensor node which communicates with a fusion center which has its own observation of the source.

The main objective of the master thesis project is to assess the privacy in such settings which are designed under a peaceful assumption. To this end the reasonable system assumptions should be made and then the optimal detectors should be computed based on the results from literature. This means that Bayesian risk, Neyman-Pearson, and information theoretic cost functions should be considered. In the next step different eavesdropper attacks of the peaceful system should be assumed and the privacy leakage should be measured using different privacy measures from the literature and perhaps new privacy measures should be introduced. The results should be interpreted and discussed. From this, system design problems should be formulated and where possible solutions or solution approaches should be derived.

Requirements: The project is quite ambitious and requires a student with a strong mathematical background, solid background in security, information and communication theory, and good skills in Matlab programming.

REFERENCES:

- [1] *Distributed Detection and Data Fusion*, by Pramod K. Varshney, Springer 1996.
- [2] *Decentralized detection*, by J. N. Tsitsiklis, in Adv. in Statistical Signal Proc., JAI Press, 1993, pp. 297344.
- [3] *Secure Distributed Detection in the Presence of Eavesdroppers*, by V.S.S. Nadendla., H. Chen, and P. K. Varshney.