Professor Subhrakanti Dey, Hamilton Institute, Maynooth University.

Title: Remote estimation over lossy channels in the presence of an eavesdropper

Abstract:

While cryptographic security has been the dominant security mechanism for cyber-security, physical layer security has become increasingly popular in the wireless communications area. In the context of wireless sensor and actuator networks deployed towards industrial control systems, however, it remains less explored. As several recent attacks on industrial plants and public infrastructure have shown, achieving secure estimation and control in such systems is extremely important. Recent research has investigated various types of active and passive attacks, and design and analysis of relevant defence mechanisms in this context, ranging from physical layer watermarking, detection of data integrity attacks, and various other algorithms for enhancing security and privacy in such networks.

In this talk we will consider security aspects of remote state estimation in the presence of an eavesdropper (a passive attacker), where the objective is to keep estimates of sensitive data or information secure but meaningful. A sensor transmits local state estimates over a packet dropping link to a remote estimator, while an eavesdropper can successfully overhear each sensor transmission with a certain probability. The objective is to determine suitable transmission scheduling schemes or design other artefacts such as addition of artificial noise (for example, if the transmitter is equipped with multiple antennas), in order to minimize the estimation error covariance at the remote estimator, while trying to keep the eavesdropper error covariance above a certain level. This is done by solving an optimization problem that minimizes a linear combination of the expected estimation error covariance and the negative of the expected eavesdropper error covariance. Structural results on the optimal transmission policy are derived, and shown to exhibit a thresholding behaviour in the estimation error covariances. Furthermore, for unstable systems, it is shown that in the infinite horizon situation there exist transmission policies which can keep the expected estimation error covariance bounded at the legitimate estimator while the expected eavesdropper error covariance becomes unbounded, thus making it useless. A different secrecy measure based on an information theoretic security notion will also be investigated.