GRADUATE STUDENT RESEARCH SEMINAR SERIES (2020)

ATTACK DETECTION AND IDENTIFICATION WITH GENERALIZED LUENBERGER OBSERVER

SPEAKER: YU XUAN

This study considers the security of distributed Cyber-Physical Systems (CPS) under malicious attacks, where the CPS components interact over a communication network. We consider the deception attacks both at the individual component level as well as the network level. At the individual level, false-data-injection corrupts sensor measurements and/or actuator signals. While at the network level, the communication between CPS components may be altered by adversarial false-data. We develop a robust model-based detection and identification algorithm for a class of discrete Linear Time Invariant (LTI) systems with delays via a Luenberger-like observer termed Generalized Luenberger Observer (GLO). The optimal GLO provides a tight bound for the residue between the monitor signals and their estimation so that it could distinguish the attack signals from intrinsic bounded noises and modeling uncertainties. Furthermore, a structurally constrained optimal GLO could also identify the place where such CPS attacks take place. Finally, we apply it to an application of the longitudinal platoon with four vehicles.

MONDAY, NOVEMBER 9 3:00 PM

EIB 132