Anomaly Detection in Liquid Pipelines Using Modeling, Co-Simulation and Dynamical Estimation

Abstract:
Historically, supervisory control and data acquisition (SCADA) systems have relied on obscurity to safeguard against attacks. Indeed, external attackers lacked knowledge about proprietary system designs and software to access systems and execute attacks. The trend to interconnect to the Internet and incorporate standardized protocols, however, has resulted in an increase in the attack surface – attackers can now target SCADA systems and proceed to impact the physical systems they control. Dynamical estimation can be used to identify anomalies and attempts to maliciously affect controlled physical systems. This paper describes an intrusion detection method based on the dynamical estimation of systems. A generic water pipeline system is modeled using state space equations, and a discrete-time Kalman filter is used to estimate operational characteristics for anomaly-based intrusion detection. The effectiveness of the method is evaluated against deception attacks that target the water pipeline system. A co-simulation that integrates computational fluid dynamics software and MATLAB/Simulink is employed to simulate attacks and develop detection schemes.