Statistical detection/isolation of cyber-physical attacks on SCADA systems

Proposal of Open invited track for the 20th IFAC World Congress

Track organizers:

Igor Nikiforov

Michèle Basseville

Abstract:

Undoubtedly, the security of supervisory control and data acquisition (SCADA) systems against cyber (-physical) attacks is extremely important. Recent incidents with essential large-scale services like electric power grids, transportation systems, communication networks, oil and gas pipelines, water distribution systems show that the negative economic and humanitarian impact of such attacks can be considerable.

IFAC technical committee(s): TC 6.4. Fault Detection, Supervision & Safety of Technical Processes-SAFEPROCESS

Detailed description:

Undoubtedly, the security of supervisory control and data acquisition (SCADA) systems against cyber (-physical) attacks is extremely important. Recent incidents with essential large-scale services like electric power grids, transportation systems, communication networks, oil and gas pipelines, water distribution systems show that the negative economic and humanitarian impact of such attacks can be considerable.

Modern SCADA systems can be attacked externally and internally at different levels: communication network, supervisory control level, and also technical (physical) processes by using physical breach. The cyber-physical attacks, i.e. the simultaneous attacks on the cyber and technical facilities are considered as the most dangerous.

This emerging area of research covers different methods of on-line (sequential) detection/isolation of cyber-physical attacks. The goal of the attack detection/isolation system is to detect as soon as possible such attacks in order to avoid grave consequences but also to satisfy a given level of false alarms. In the framework of this track, a special attention will be paid to statistical detection methods and machine learning methods for attack detection.

The goal of this track is to bring together the theoreticians and practitioners of cyber-physical attack detection/isolation and the specialist in SCADA systems security in order to define the most useful models and scenarios of such attacks and the best methods for their detection/isolation.