POLITECNICO MILANO 1863 | DIPARTIMENTO DI ENERGIA

EDI Lab Energy Data and Information Lab

RESEARCH THESIS ON:

ASSESSMENT OF DATA INTEGRITY CYBERATTACKS ON IOT OPERATION AND MAINTENANCE PLATFORMS

CONTEXT OF THE RESEARCH

Prognostics and Health Management (PHM) systems increasingly support Operation and Maintenance (O&M) of critical assets in multiple sectors. They do so by combining sensor measurements from Internet-of-Things (IoT) platforms with big data analytics and Artificial Intelligence (AI) that enable the estimation of State of Health (SoH) and Remaining Useful Life (RUL) of assets. These estimates are the basis for modern Predictive Maintenance (PM) frameworks, where interventions are optimally scheduled based on the real condition of assets rather than at fixed periodic intervals or after they fail. The effectiveness of IoT-PM systems relies on the integrity of the historical datasets and measurements used to train, calibrate and/or update underlying PHM models. Data Integrity (DI) cyber-attacks can exploit these dependences by deliberately manipulating data exchanges to bias SoH or RUL estimates: for instance, an overestimated RUL may postpone necessary maintenance and increase exposure to failure, whereas an underestimated RUL may trigger early, unnecessary interventions with increased costs. Therefore, the consequences of DI attacks extend beyond inaccurate estimates to system-wide reliability, safety and economic impacts.

This thesis offers the opportunity to combine distributed asset condition modeling with DI attack simulation in IoT-PHM systems. The student will investigate how poisoning training/monitoring data affects SoH/RUL estimates and impacts maintenance decisions. The comparison between normal and attacked scenarios will establish when and how compromised data leads to harmful outcomes, ultimately informing defense mechanisms for asset owners.

OBJECTIVE OF THE RESEARCH

This thesis aims to quantify, through simulation, the effects of DI attacks in PM frameworks by poisoning data used for SoH/RUL estimation, and assessing their impact on operational costs and failure exposure in IoT-PHM systems. The research comprises the following expected activities:

- *Literature review*. Review data poisoning, IoT vulnerabilities and emerging cyber-threats to PM frameworks, including attack detectability, uncertainty and available defenses.
- *Problem formulation*. Select a network of interacting assets, assign condition models, SoH/RUL estimators and maintenance policies, and map data flows exposed to poisoning.
- *Threat modeling*. Define attacker knowledge, data access, manipulations and poisoning budgets. Develop direct and stealthy attacks on asset- and system-level SoH/RUL estimates.
- *Scenario generation*. Integrate degradation models, IoT data flows, estimators, maintenance and attacks to simulate normal and attacked scenarios under uncertainty (e.g., Monte Carlo simulation).
- *Performance evaluation*. Compare SoH/RUL estimation deviations and their impacts on maintenance timing, operating and maintenance costs, and failure exposure under the selected PM policy.
- *Mitigation assessment*. Test at least one defense mechanism for its ability to mitigate data poisoning effects.

The student will have the opportunity to contribute to scientific publications based on the outcomes of the project. The expected duration of the research activities is 8 to 9 months plus thesis writing.

CANDIDATE PROFILE

- Scientific programming skills (e.g., Python, MATLAB, Julia); knowledge of Git and OOP.
- Good technical communication skills in English.
- No more than two exams remaining.
- Familiarity with cybersecurity and knowledge of graph theory and energy systems is welcome.

RESEARCH TEAM

For further information, please contact:

- Dr. Juan-Pablo Futalef (juanpablo.futalef@polimi.it)
- Prof. Enrico Zio (enrico.zio@polimi.it), 02 2399 6340