Improving the Security of EMS/SCADA Systems Monitoring Central Heating and Cooling Plants (CHCP)

Mahnoosh Alizadeh, Anna Scaglione

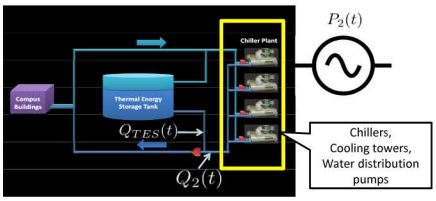
Goals

- In CHCPs, devices are controlled by computer programs running on local Programmable Logic Controllers (PLC) associated with each of them. The PLCs therefore verify that the operations of these devices are within the safety limits.
- An intelligently designed cyber-attack would be one in which local safety requirements are not violated, but the global state is unsafe or suboptimal due to coordinated bad behavior of the networked systems.
- The attack can be initialized by a trusted person, such as the operator (poor controls or malicious intentions).
- Few SCADA systems can prevent such attacks.
- A purely cyber solution: Use historical training data from expected use cases to characterize legitimate global states → False alarms rates can be high, esp. with a large number of operational patterns → not widely adopted by operators.
- Mixing cyber and physical safety: harder to implement, more reliable.
- Our goal: **propose security enhancements for an accurate interpretation of overall system state.**
- Our idea: giving an online assessment of *how bad is the situation that happened*, compared to *what should have happened*.

Fundamental Questions/Challenges

- Understand the fundamental relations between the quantities that the sensors are measuring.
  - CHCP units can have various designs: constant flow rate primary, primary/secondary (primary constant, secondary constant, or variable), variable primary.
  - The system is composed of many small components, e.g., pumps, fans, control units, and the heat rejection device. What is a sufficient level of detail for modeling?
  - Measurements are related using nonlinear mechanical or thermodynamic laws.
- Several challenges are faced:
  - Getting access to lower-level SCADA data to perform experiments.
  - Modeling the manual control component in the loop: We need to understand the rules used by operators to control the system, which are potentially suboptimal and based on "cognitive biases."
  - Meters have large errors → can result in false alarms.

Research Plan



- Study assessment model for central chilling (power hog).
  - Model cooling demand stochastically.
    - Various real-time measurements available from UCD CHCP, including primary and secondary flows, pump flows, supply and return temperatures of water, tank status, consumed power.
  - Model how various components inside the yellow box work together to serve the load, e.g., chillers (prime movers like motors inside), pumps, boilers, heat exchangers (e.g., cooling tower).
- Identify commands the attacker can use to harm the electrical network or the equipment inside the plant without triggering any alarm.
- Study communication protocols and identify how the attacker can issue such commands remotely.

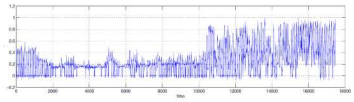
Research Results

- Principle: supply/demand balance:

$$Q(t) = \sum Q_j(t) + \frac{1}{24}\dot{m}_{ch}(t)\Delta T_{des}(t)$$

Campus cooling load | Chiller plant j cooling tons | Flow out of tank | Designed temp diff

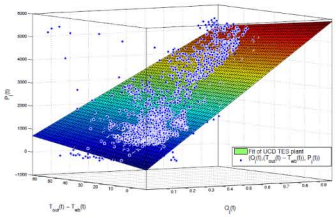
Normalized cooling load obtained from University of California Davis Thermal Energy Storage Plant for the first 5 months of 2012



- How is the power consumption of each plant related to cooling load?

$$P_j(t) = a_{j0} + a_{j1}Q_j(t) + a_{j2}(T_{out}(t) - T_{wb}(t)) + a_{j3}Q_j(t)\,(T_{out}(t) - T_{wb}(t))$$

Data from University of California Davis Thermal Energy Storage Plant. The plant has four 2000-ton chillers. It currently serves the base load of the Davis campus. The TES Tank has a design capacity of 40,000 ton-hrs at 14 degrees differential temp



- Need to set thresholds for deviations from this power to generate alert.
- Alternative: stochastic model.
- How to improve: include more parameters, such as chiller sequencing.
- **Online Assessment:** Use Model Predictive Control principles to identify the best- and worst-case operation scenarios.

$$G = \min_{Q_j(\ell)} \mathbb{E}_{Q(\ell)} \left\{ \sum_{\ell=t}^{t+T} \mathrm{Cost}(\ell) \right\} \qquad B = \max_{Q_j(\ell)} \mathbb{E}_{Q(\ell)} \left\{ \sum_{\ell=t}^{t+T} \mathrm{Cost}(\ell) \right\}$$

  - S.t. all local physical constraints that raise alarms if violated.
  - E.g., individual chiller capacities.
    - GPM of pumps.
- Possible strategies for attacks:
  - Shift load to peak hours to increase electricity bill.
  - Operate chillers at part load → lower efficiency.
  - Pump out water with unacceptable temperatures so load cannot be served (violate the balance constraint).
- **Evaluation of security:** Compare actual operations costs with MPC forecasts.

Broader Impact

- The same type of specification-based intrusion detection can be applied to other current existing SCADA systems as well, if proper models are made.
- The developed model can be used for planning and control purposes as well, e.g., demand side management and renewable integration and planning for EMS.

Future Efforts

- Go one level down in detail for modeling the plant components.
- Perform simulations to assess possible damage levels.
- Further develop the online assessment tool.