Security metrics and allocation of security resources for control systems

Jezdimir Milošević

KTH Royal Institute of Technology

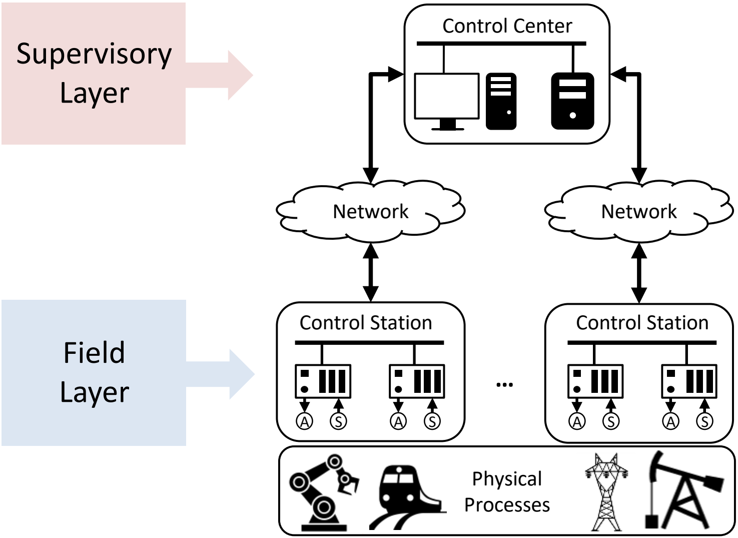
Supervisors: Prof. Henrik Sandberg and Prof.Karl Henrik Johansson
Opponent: Asst. Prof. Ling Shi, Hong Kong University of Science and Technology

March 27th, 2020

Motivation

- What are control systems?
- Why are control systems important to secure?
- Why are control systems challenging to secure?

What are control systems?



Why are control systems important to secure?

- These systems operate physical processes important for our society



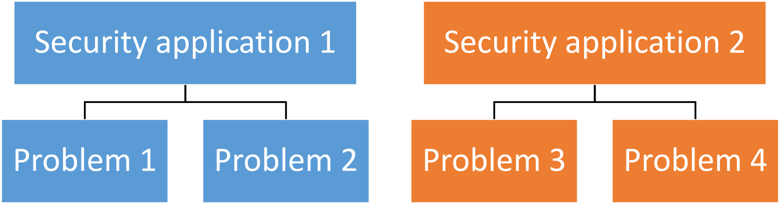

Why are control systems challenging to secure?

- Large number of security vulnerabilities

- Long life cycle

- Large scale

Structure of the thesis



Related publications:

Problem 1: J. Milošević et al., "Estimating the impact of cyber-attack strategies for stochastic control systems," IEEE TCNS. Accepted, 2019.

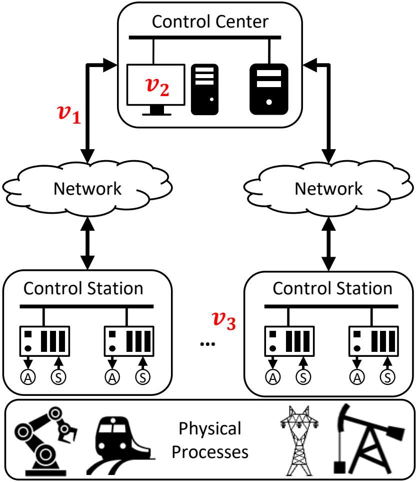
Problem 2: J. Milošević et al., "Security measure allocation for industrial control systems: Exploiting systematic search techniques and submodularity," IJRNC. Accepted, 2018.

Problem 3: J. Milošević et al., "Actuator security indices based on perfect undetectability: Computation, robustness, and sensor placement," IEEE TAC. Accepted, 2020.

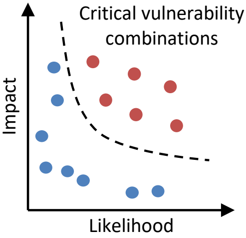
Problem 4: J. Milošević et al., "A monitoring game based on actuator security indices," under preparation for journal submission.

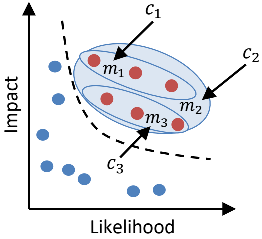
Application 1: Classifying and preventing security vulnerabilities

- We are given a set of security vulnerabilities $\mathcal{V} = \{v_1, v_2, \dots\}$
- A vulnerability $v \in \mathcal{V}$ can model:
  - Unprotected communication channels (v_1)
  - Antivirus software not updated (v_2)
  - Absence of physical protection (v_3)



Application 1: Related problems





P1: Impact estimation. How to estimate the impact of attack strategies using physical models of control systems?

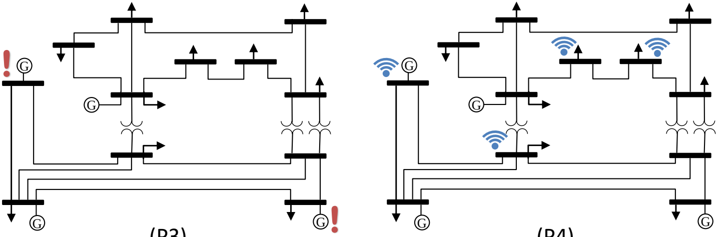
P2: Security measure allocation. How to prevent the critical vulnerability combinations cost-effectively?

Application 2: Security of actuators in large scale-systems

Actuators are...

- Important (direct interaction with physical processes)
- Often expensive (e.g., large generators in power systems)
- Vulnerable (several attacks against or using actuators have occurred)

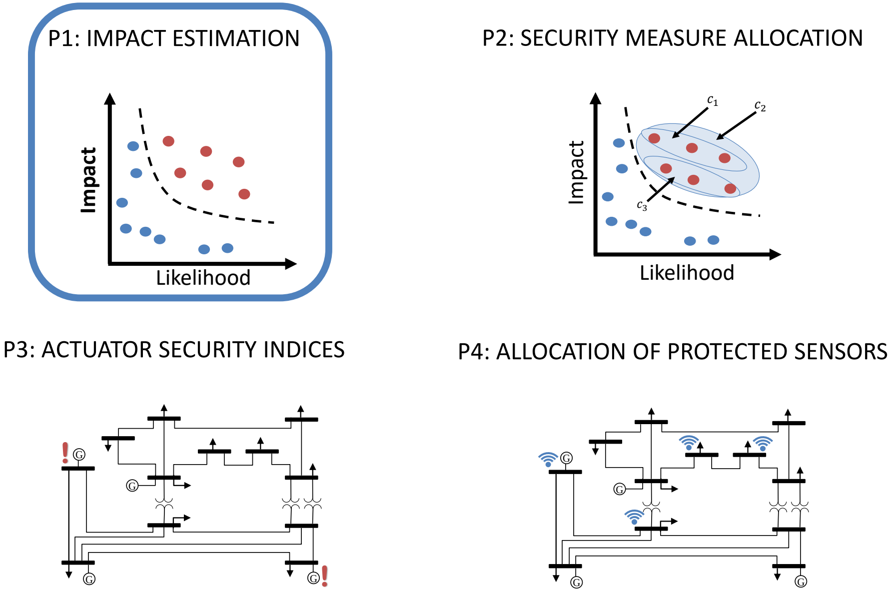
Application 2: Related problems



(P3) (P4)

P3: Actuator security indices. How to find vulnerable actuators in large-scale control systems?

P4: Allocation of protected sensors. How to strategically place a limited number of protected sensors in a large-scale control system?


P1: IMPACT ESTIMATION
Impact
Likelihood
P2: SECURITY MEASURE ALLOCATION
c_1
c_2
c_3
Impact
Likelihood
P3: ACTUATOR SECURITY INDICES
P4: ALLOCATION OF PROTECTED SENSORS

Problem 1: Impact estimation

$$\begin{aligned} \underset{\text{Attack}}{\text{maximize}} \quad & \text{Impact metric} \\ \text{subject to} \quad & \text{Laws of physics are satisfied} \\ & \text{Attack remains stealthy} \\ & \text{Attack follows an attack strategy} \end{aligned}$$

- Essence: Check if the attacker can make large impact and remain stealthy

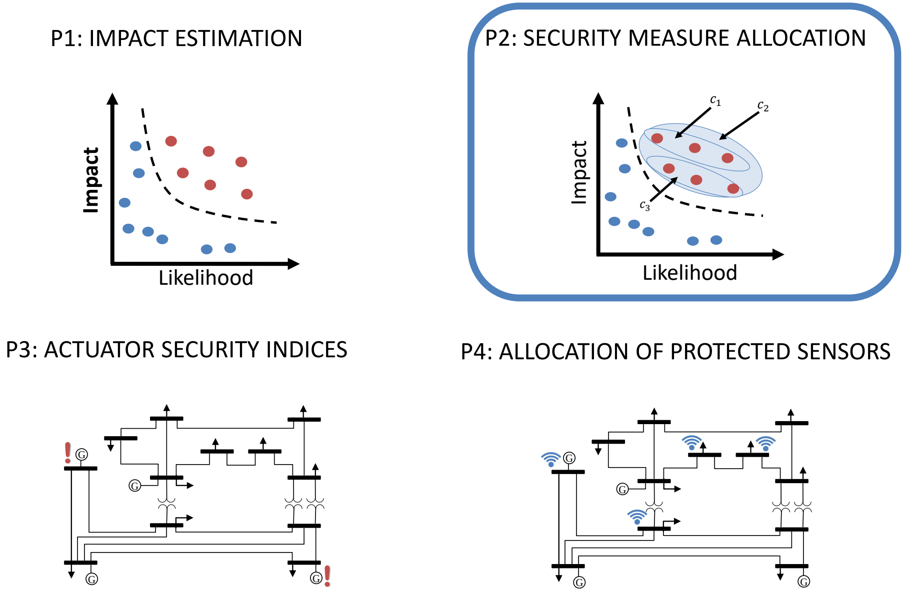
Problem 1: Impact estimation

$$
\begin{aligned}
\underset{a_{0:N},\, y_r}{\text{maximize}} \quad & I(a_{0:N}, y_r) \\
\text{subject to} \quad & x_e(k+1) = Ax_e(k) + Bv(k) + Ey_r + G(a(k) + a_s(k)) \quad \text{(Physics)} \\
& \tilde{r}(k) = Cx_e(k) + Dv(k) + Fy_r + H(a(k) + a_s(k)) \quad \text{(Physics)} \\
& \|Qy_r\|_\infty \leq 1 \quad \text{(Physics)} \\
& \mathcal{D}(\tilde{r}_{0:N} || r_{0:N}) \leq \epsilon \quad \text{(Stealthiness)} \\
& F_a a_{0:N} = 0 \quad \text{(Imposing strategy)} \\
& a_{s0:N} = T_1 x_e(N_s) + T_2 y_r + T_3 v_{N_s:-1} \quad \text{(Imposing strategy)}
\end{aligned}
$$

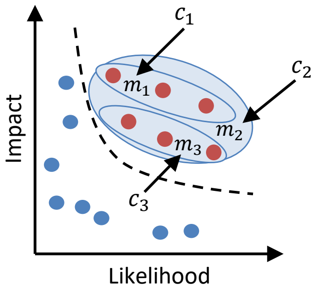
- Essence: Check if an attack can make large impact and remain stealthy
- Problem 1 is difficult to solve

Chapter 4: Summary of the results

- We proposed two impact metrics suitable for stochastic systems (I_P, I_E)
- The optimal value of the metric I_P can be computed efficiently **(Thm 4.1)**
- Lower and upper bounds for the metric I_E that are efficient to compute **(Thm 4.2)**
- The framework is compatible with a number of attack strategies proposed in the literature **(Prop 4.2–4.4)**
- By exploiting the properties of the strategies, the impact can be computed more efficiently **(Prop 4.5–4.7)**
- Applicability demonstrated on a control system of a chemical process


P1: IMPACT ESTIMATION
Impact
Likelihood
P2: SECURITY MEASURE ALLOCATION
c_1
c_2
c_3
Impact
Likelihood
P3: ACTUATOR SECURITY INDICES
G
P4: ALLOCATION OF PROTECTED SENSORS
G

Problem 2: Security measure allocation

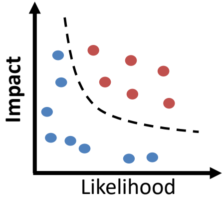


- Essence: Find the least expensive subset of security measures that prevents all the critical vulnerability combinations
- Problem 2 is difficult to construct (we need to find all of the critical vulnerability combinations)
- Problem 2 is NP-hard **(Prop 5.1)**

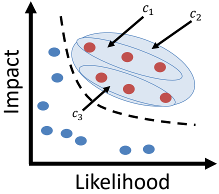
Chapter 5: Summary of the results

- **Algorithm 5.1**: Systematically constructs Problem 2
  - Relies on several systematic search tools
  - Provably constructs Problem 2 **(Thm 5.1)**
  - In the worst case, searches through all the combinations
  - Tested in a simulation study: Managed to construct Problem 2 in all the cases
- Two approaches for solving Problem 2
  - A1: Simplify Problem 2 and use integer linear program solvers
  - A2: Use a polynomial-time algorithm to compute a suboptimal solution **(Thm 5.2)**
  - Both of the approaches performed satisfactorily in a simulation study

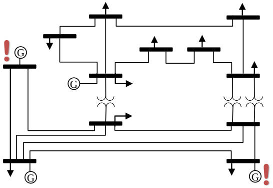
P1: IMPACT ESTIMATION



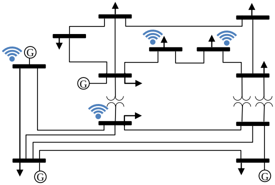
P2: SECURITY MEASURE ALLOCATION



P3: ACTUATOR SECURITY INDICES



P4: ALLOCATION OF PROTECTED SENSORS



Problem 3: Actuator security index δ

Problem of computing $\delta(u_i)$:

$$\begin{aligned} \underset{\text{Attack}}{\text{minimize}} \quad & \text{Resources} \\ \text{subject to} \quad & \text{Laws of physics are satisfied} \\ & \text{Attack remains stealthy} \\ & \text{Actuator } u_i \text{ attacked} \end{aligned}$$

- $\delta(u_i)$: Security index of actuator u_i
- Large $\delta(u_i) \Longrightarrow$ Actuator u_i is secure
- Small $\delta(u_i) \Longrightarrow$ Actuator u_i is vulnerable

Problem 3: Actuator security index δ

Problem of computing $\delta(u_i)$:

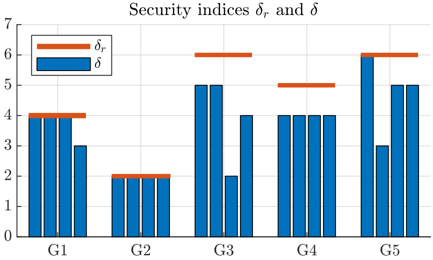
$$
\begin{aligned}
\underset{a}{\text{minimize}} \quad & \|a\|_0 \\
\text{subject to} \quad & x(k+1) = Ax(k) + B_a a(k) && \text{(Physics)} \\
& y(k) = Cx(k) + D_a a(k) && \text{(Physics)} \\
& y \equiv 0,\ x(0) = 0_{n_x} && \text{(Stealthiness)} \\
& a_i \not\equiv 0 && (u_i \text{ is attacked})
\end{aligned}
$$

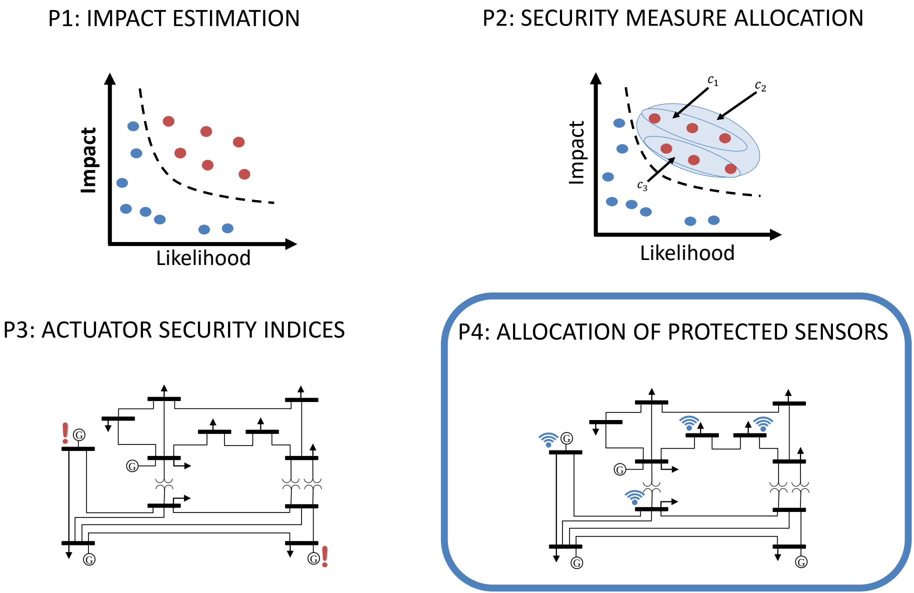
- The security index δ is
  - NP-hard to compute **(Thm 6.1)**
  - vulnerable to system variations (δ changes when A, B, C change)
  - based on the assumption that the attacker knows the entire system model
- Conclusion: This index is not suitable for large-scale systems

Chapter 6: Summary of the results

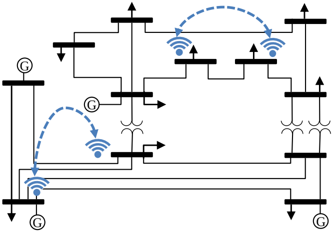
- We introduced the robust security index δ_r, which...
  - is efficient to compute **(Thm 6.2 + Prop 6.4)**
  - characterizes actuators vulnerable in all system realizations
  - can be related to full and limited model knowledge attackers **(Prop 6.5–6.7)**
  - can be improved efficiently even in large systems **(Thm 6.3 + Prop 6.8)**

- Drawback: Cannot detect actuators that are vulnerable in some realizations




P1: IMPACT ESTIMATION
Impact
Likelihood
P2: SECURITY MEASURE ALLOCATION
Impact
Likelihood
c_1
c_2
c_3
P3: ACTUATOR SECURITY INDICES
P4: ALLOCATION OF PROTECTED SENSORS

Problem 4: Placement of protected sensors



- The game is based on the security index δ_{ER} (related to both δ and δ_r)
- Goal: Find a NE monitoring strategy

- Problem of computing a NE monitoring strategy

$$\begin{aligned} \underset{\sigma, z}{\text{maximize}} \quad & z \\ \text{subject to} \quad & A\sigma \geq z\vec{1} \end{aligned}$$

- Main issue: The size grows exponentially with the number of protected sensors

Chapter 7: Summary of the results

- We derived an ϵ-NE monitoring strategy **(Thm 7.1)**
- Cases when this ϵ-NE monitoring strategy becomes exact **(Cor 7.1–7.3)**
- Three ways to improve the ϵ-NE monitoring strategy **(Prop 7.1–7.3)**
- Simulation study: The ϵ-NE monitoring strategy proves to be optimal and efficient to construct

Concluding remarks

Summary and possible extensions

- Two security applications considered:
  - Classifying and preventing security vulnerabilities
  - Security of actuators in large-scale systems
- Security metrics for determining where to focus security resources
  - Application 1: Impact metrics
  - Application 2: Actuator security indices
- Tools for allocating security resources in a cost-effective manner
  - Application 1: Allocation of security measures
  - Application 2: Allocation of secured sensors
- Possible extensions:
  - Generalizing models
  - Improving efficiency of Algorithm 5.1
  - Relaxing assumptions made in the security game

Thank you for your attention!