Problem Statement:
Motivation: Existing metrics for secrecy, including non-interference, mutual-information/min-entropy, and Jensen-Shannon divergence, do not support an easy computation of quantitative measure of the level of secrecy loss over sequences of input/output. Similarly, a computable quantitative metric for system’s resiliency to attacks of sensors, actuators and other components is also missing.

Goals:
• Develop computable notion of secrecy and resiliency for cyber-physical systems, modeled as stochastic hybrid automata
• Assess secrecy/resiliency loss as function of compromised sensors, actuator and other components
• Develop configuration tool that enhances secrecy and resiliency

Proposed Technical Approach:
Quantifying Secrecy (Confidentiality) for CPS
• Model systems as stochastic hybrid (discrete+continuous states) automata
• Use methods based on statistical and Bayesian inference to quantify level of secrecy

Quantify Resiliency (Integrity) against Attacks for CPS
• Compute residue of observed versus nominal system outputs to identify attacks
• Use statistical inference to quantify attack detectability (resiliency), identify compromised components, perform system reconfiguration for attack-mitigation

Estimated Cost and Schedule:
Cost: One graduate student for a period of up to 3 years

Deliverables and Schedule:
• Year 1 will focus of developing notion of secrecy for CPS and algorithm for computing it;
• Year 2 will focus on developing notion of resiliency for CPS and algorithm for computing it.
• Year 3 will develop the necessary tools for evaluating secrecy/resiliency and report experimental results.
All findings of the results will be reported through public domain conferences/journals.
Secrecy: Information vs. Behaviors

- Behaviors cannot be encrypted for secrecy, but information can.

- Secrecy can stem from ambiguity caused by partial observability.

- For secrets $s \in K$, $Pr_{amb}(s) = \frac{Pr(Cover(s))}{Pr(Cover(s) + Secret(s))} = \frac{Pr(Green)}{Pr(Green + Red)}$

- Secrecy level $\tau$ under tolerance $\rho$: $Pr(s \in K : Pr_{amb}(s) > \rho) > \tau$
  (Secrets with ambiguity higher than $\rho$ occur with prob. higher than $\tau$)

- Computation of secrecy level for CPS (a Stochastic Hybrid Automaton)
Various metrics for secrecy have been explored in literature

- **Non-interference**: binary qualitative property (not quantitatively measure the level of secrecy)
- **Mutual-information and min-entropy**: probabilistic quantitative notions, but are typically limited to one-step input/output.
- **Jensen-Shannon divergence**: measure secrecy over sequences of inputs/outputs, but it is complex to compute, and only certain upper bounds may be obtained under certain conditions.

Our approach of secrecy metric

- Defined over sequences of inputs/outputs
- Computable for finite-state probabilistic systems modeled as Markov Chains

References:

Secrecy: Computation of Secrecy Level

\[ P(i,j) \leq P(i,k) + P(k,j) \]

\[ \sum_{k \in \Omega} P(i,k) + P(k,j) \]

\[ (2,2, Z_2) \]

\[ (0,0, Z_0) \]

\[ (1,D, Z_0) \]

\[ (3,D, Z_1) \]

\[ (1,D, Z_2) \]

\[ (2,D, Z_3) \]

\[ (3,D, Z_4) \]

\[ (0,D, Z_5) \]

\[ (2,D, Z_6) \]

\[ (3,D, Z_7) \]

\[ (0,D, Z_8) \]

\[ (2,D, Z_9) \]

\[ (3,D, Z_{10}) \]

\[ (0,D, Z_{11}) \]

\[ (2,D, Z_{12}) \]

\[ (3,D, Z_{13}) \]

\[ (0,D, Z_{14}) \]

\[ (2,D, Z_{15}) \]

\[ (3,D, Z_{16}) \]

\[ (0,D, Z_{17}) \]

\[ (2,D, Z_{18}) \]

\[ (3,D, Z_{19}) \]

\[ (0,D, Z_{20}) \]

\[ (2,D, Z_{21}) \]

\[ (3,D, Z_{22}) \]

\[ (0,D, Z_{23}) \]

\[ (2,D, Z_{24}) \]

\[ (3,D, Z_{25}) \]

\[ (0,D, Z_{26}) \]

\[ (2,D, Z_{27}) \]

\[ (3,D, Z_{28}) \]

\[ (0,D, Z_{29}) \]

\[ (2,D, Z_{30}) \]

\[ (3,D, Z_{31}) \]

\[ (0,D, Z_{32}) \]

\[ (2,D, Z_{33}) \]

\[ (3,D, Z_{34}) \]

\[ (0,D, Z_{35}) \]
Proposed Technical Approach

- Quantifying **Secrecy (Confidentiality)** for CPS
  - Model systems as stochastic hybrid (discrete+continuous states) automata
  - Use methods based on statistical and Bayesian inference to quantify level of secrecy

- Quantify **Resiliency (Integrity)** against Attacks for CPS
  - Compute residue of observed versus nominal system outputs to identify attacks
  - Use statistical inference to quantify attack detectability (resiliency), identify compromised components, perform system reconfiguration for attack-mitigation
Resiliency: Attack Detection and Mitigation

- Attack detected if observed vs. nominal outputs differ beyond a threshold

\[ r^n := \frac{1}{n} \sum_{k=1}^{n} |E(\hat{y}_k) - y_k| > \rho \]

- Issues: False-positive/-negative rates; condition for detection; identify anomalous components; mitigation through reconfiguration