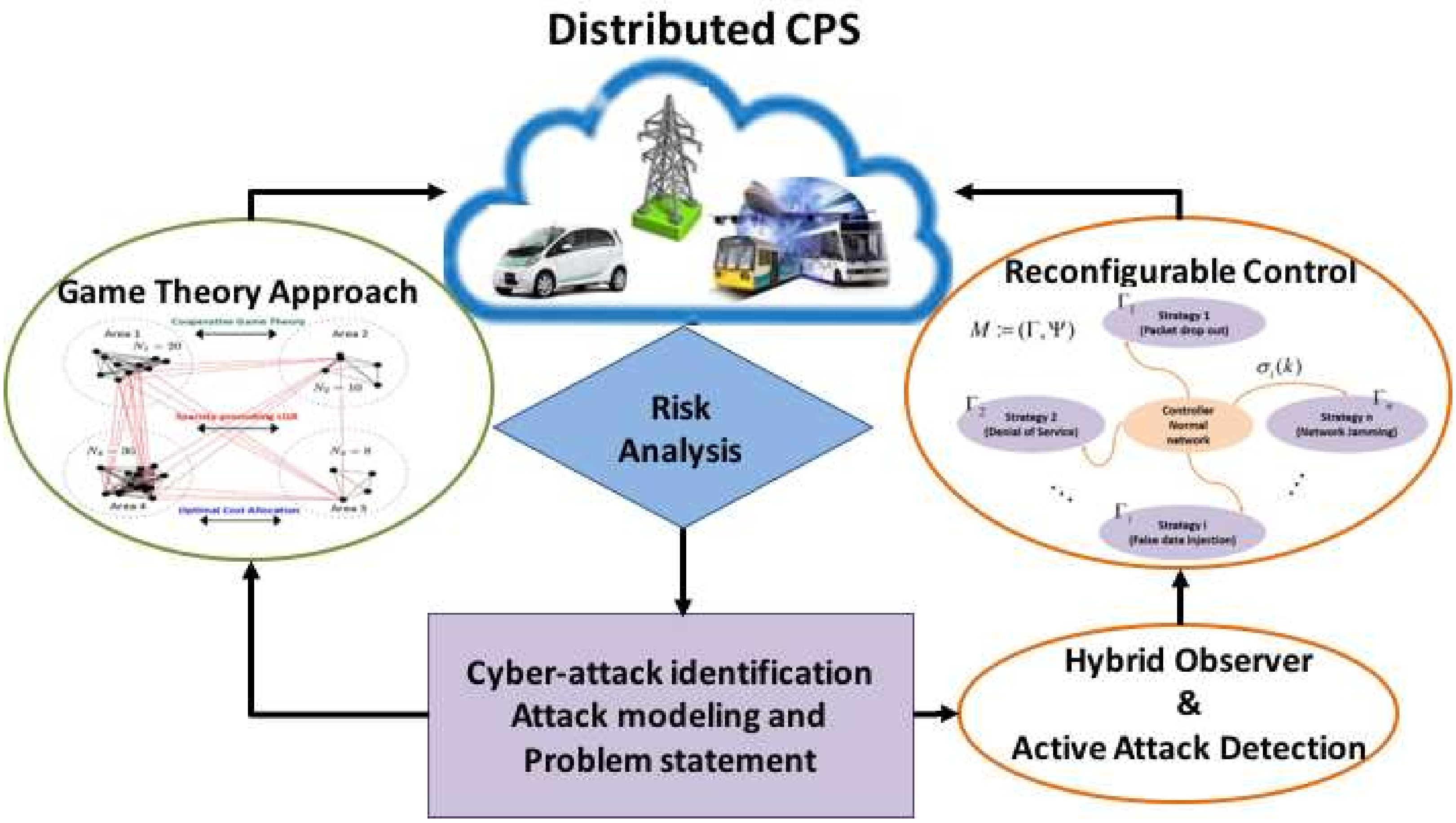
Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications

PI : Dr. Pierluigi Pisu
Automotive Engineering Department (CUICAR)
Co-PI : Dr. Richard Brooks
Electrical and Computer Engineering Department
Co-PI : Dr. Jim Martin
School of Computing
Clemson University

February 15, 2016

Overview

I. Overview
▷ Overview
II. Motivation & Introduction
III. Problem Statements
IV. Scenario I
V. Scenario II
VI. Experimental Setup



Motivation 1

I. Overview
II. Motivation & Introduction
▷ Motivation 1
Motivation 2
III. Problem Statements
IV. Scenario I
V. Scenario II
VI. Experimental Setup

- Intrusion detection systems (IDS) neither reliably detect nor distinguish cyber-attacks from normal operations.
- Some IDS product comparisons find using an IDS worse than letting hackers into your system.
- There are additional challenges for Cyber-Physical Systems.
- Damages in connected vehicle applications can include:
  - False data injection to lower system performance (ex. fuel efficiency)
  - Vehicle collisions.
- Cyber-security for connected vehicles has many interested parties: individual owners, OEMs, component suppliers, fleet operators, car dealerships, insurance companies, police, EPA, vehicle repair shops, pedestrians and effectively society as a whole.

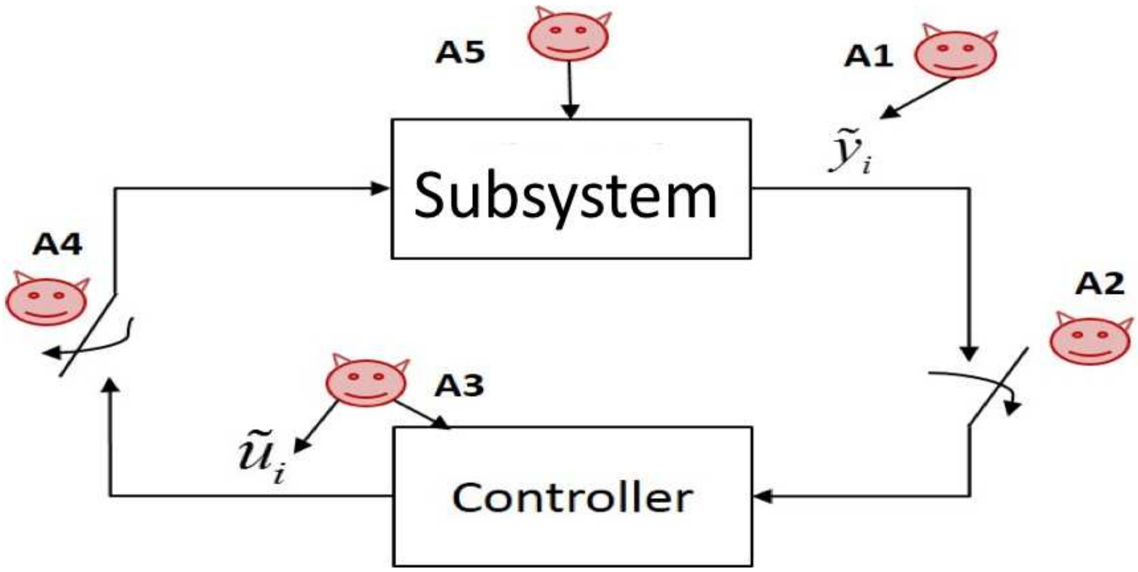
Motivation 2

I. Overview
II. Motivation & Introduction
Motivation 1
▷ Motivation 2
III. Problem Statements
IV. Scenario I
V. Scenario II
VI. Experimental Setup

- Cyber Physical System (CPS), consists of:
  - Physical plant
    - Multiple parties / Complex interactions
    - Sensors / Actuators
  - Communications network
    - Global
    - Local
- Intentional disruption
  - Fraudulent information
  - Denial of service
  - Code/data inertion, etc.
- Physical failure
  - Sensors / Actuators

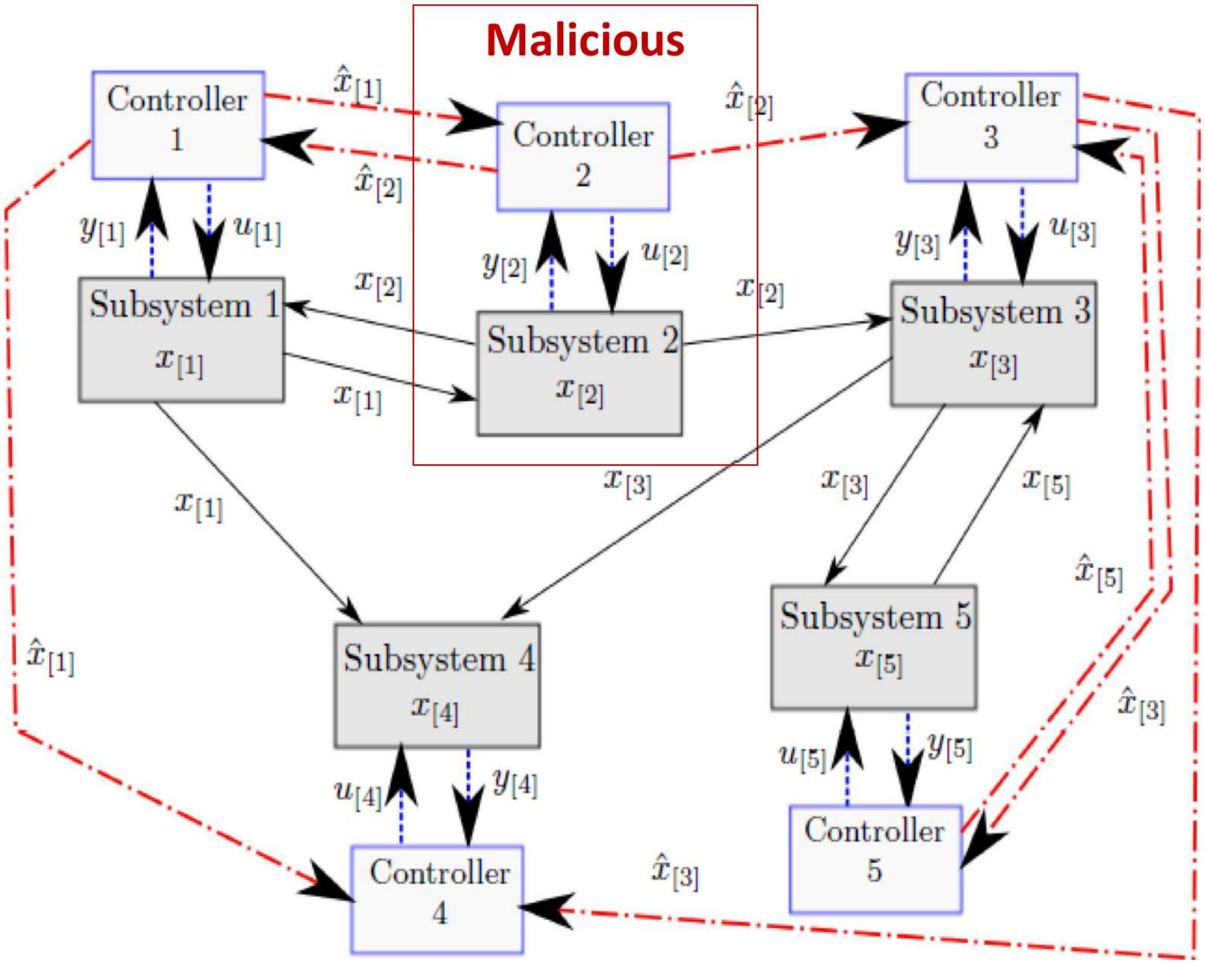
Cyber attacks on individual subsystem

I. Overview
II. Motivation & Introduction
III. Problem Statements
▷ Cyber attacks on individual subsystem
Compromised subsystem in a distributed CPS
IV. Scenario I
V. Scenario II
VI. Experimental Setup



Compromised subsystem in a distributed CPS

I. Overview
II. Motivation & Introduction
III. Problem Statements
Cyber attacks on individual subsystem
▷ Compromised subsystem in a distributed CPS
IV. Scenario I
V. Scenario II
VI. Experimental Setup



Cyber attacks on individual subsystem

I. Overview

II. Motivation & Introduction

III. Problem Statements

IV. Scenario I

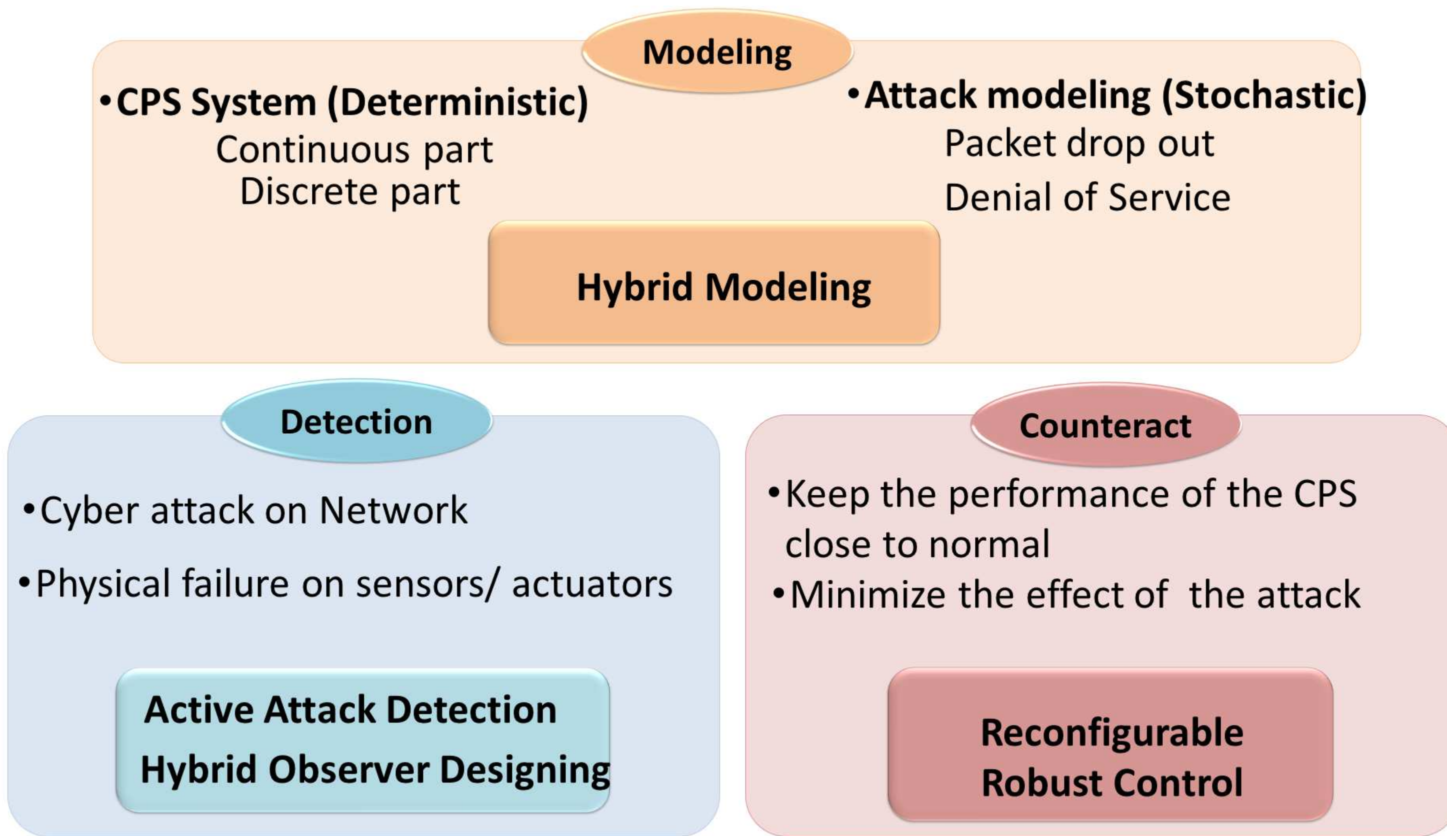
▷ Cyber attacks on individual subsystem

Hybrid Modeling and Control

Detection

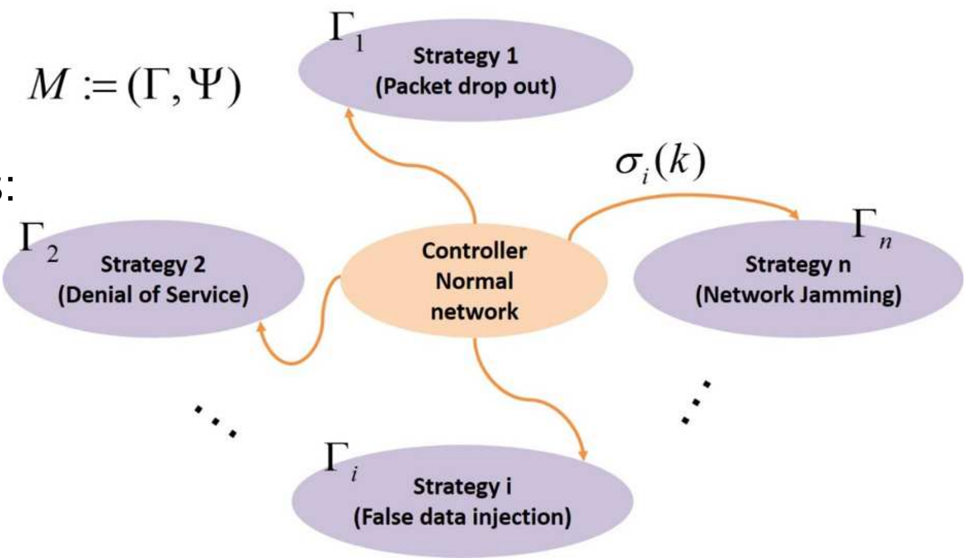
V. Scenario II

VI. Experimental Setup



Hybrid Modeling and Control

- Hybrid system
  - Different strategy for different cyber-attacks
  - Switch between strategies based on detection decision
  - M: Hybrid system
  - Γ: Set of discrete states of M
  - Ψ: Continuous dynamics of M
  - $\sigma(k)$: Event
- Assumptions
  - Continuous sub-systems: LTI systems



Detection

I. Overview
II. Motivation & Introduction
III. Problem Statements
IV. Scenario I
Cyber attacks on individual subsystem
Hybrid Modeling and Control
▷ Detection
V. Scenario II
VI. Experimental Setup

- Hybrid Observer
  - Considers CPS cyber and physical states
  - Makes decisions on cyber-attack by monitoring the augmented system
  - Has the potential to detect a wider range of cyber-attacks that includes common attacks (jamming, false data injection, etc.) as well as intelligent attacks (stealth, covert and replay attacks)
- Active Attack Detection
  - In cases where the reachable output set of different attacks and the normal operating point of a system overlap, due to system uncertainties or control action masking attack effect, mere observer based attack detection would not work well
  - Inappropriate control signal, over a small duration, would be utilized for the identification of system anomaly

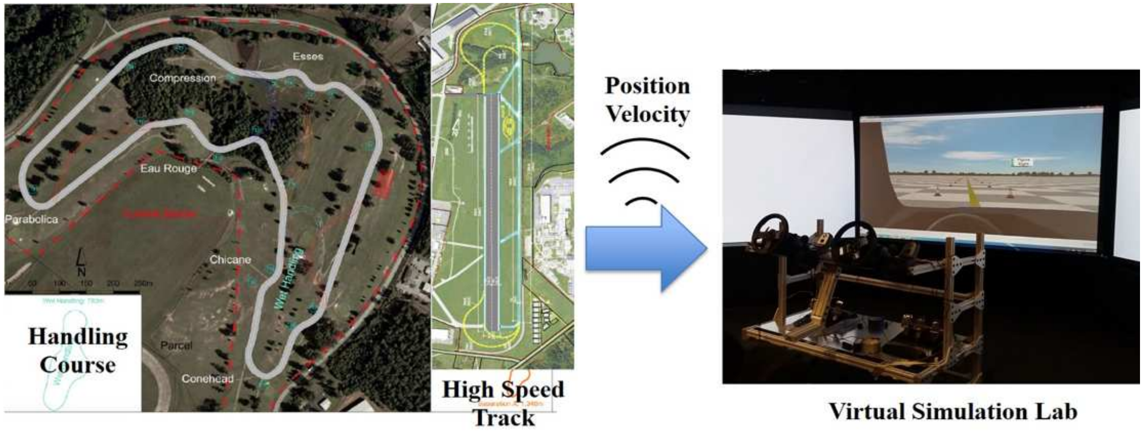
Compromised subsystem in a distributed CPS

I. Overview
II. Motivation & Introduction
III. Problem Statements
IV. Scenario I
V. Scenario II
▷ Compromised subsystem in a distributed CPS
VI. Experimental Setup

- Game Theory : Attack Resilient Countermeasure
  - One or more subsystems in distributed CPS are malicious
  - Byzantine Generals
  - Malicious components try to maximize the global cost function
  - The rest of the group want to minimize the cost function
  - Game theory - Maximin, Minimax, Saddle point, Mixed strategies
  - Control countermeasure uses game theory

I. Overview
II. Motivation & Introduction
III. Problem Statements
IV. Scenario I
V. Scenario II
VI. Experimental Setup
▷ Experimental Setup

- Experimental testing and validation has 2 main components
  - CV testbed located at South Carolina Technology
    - More than 2.5-miles of straightaway test track,
    - 2.5-mile interstate-grade test track (expandable up to 17.5 miles) DSRC-based communication network for V2V and V2I
  - Aviation Center (SC-TAC); a CV virtual/simulation lab at CU-ICAR



Connected Vehicle Testbed at SC-TAC