Foundations Of Resilient CybEr-physical Systems (FORCES)

Shankar Sastry

FORCES Principal Investigator and Dean, College of Engineering
University of California, Berkeley

NSF

Berkeley
UNIVERSITY OF CALIFORNIA

MICHIGAN

Massachusetts
Institute of
Technology

VANDERBILT
UNIVERSITY

Motivation: Resilient CPS

Attributes

1. Functional correctness by design
2. Robustness to reliability failures (faults)
3. Survivability against security failures (attacks)

Tools [Traditionally disjoint]

- Resilient Control (RC) over sensor-actuator networks
- Economic Incentives (EI) to influence strategic interaction of individuals within systemic societal institutions

CPS integrated with human decision makers [Tightly coupled RC & EI]

- Spatio-temporal and hybrid dynamics
- Large number of strategic interactions with network interdependencies
- Inherent uncertainties, both public and private

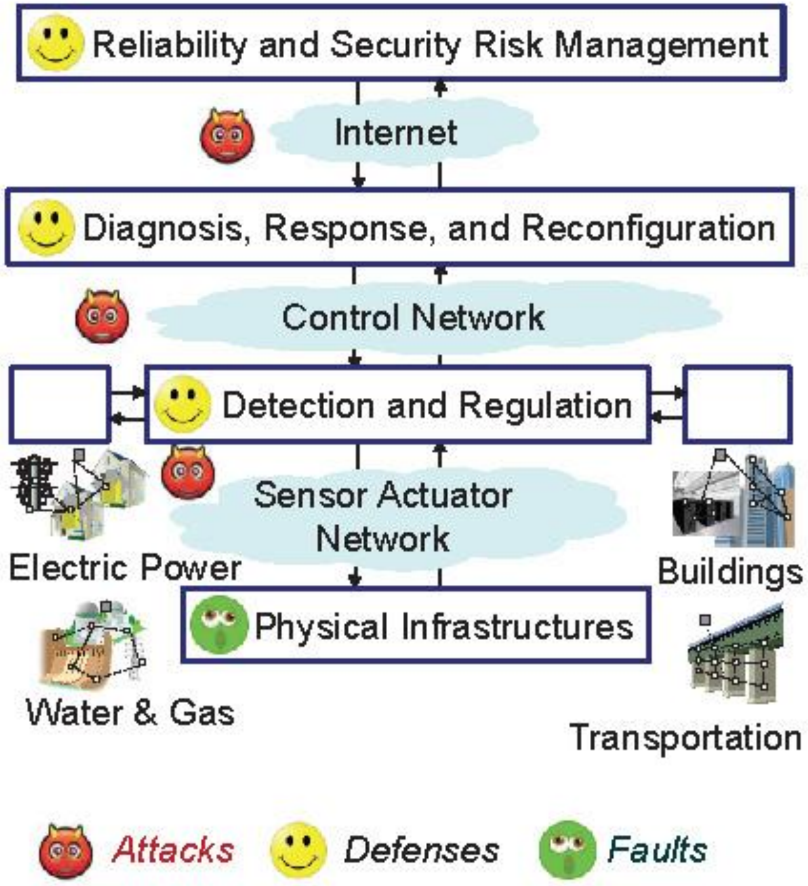
Towards a theory of Resilient CPS

Resilient Control (RC)

- Threat assessment & detection
- Fault-tolerant networked control
- Real-time / predictive response
- Fundamental limits of defenses

Economic Incentives (EI)

- Incentive Theory for resilience
- Mechanisms to align Nash allocations with socially optima
- Interdependent risk assessment
- Insurance & risk redistribution



Functional layers: Regulatory, Supervisory, Management levels

EI-aware RC design

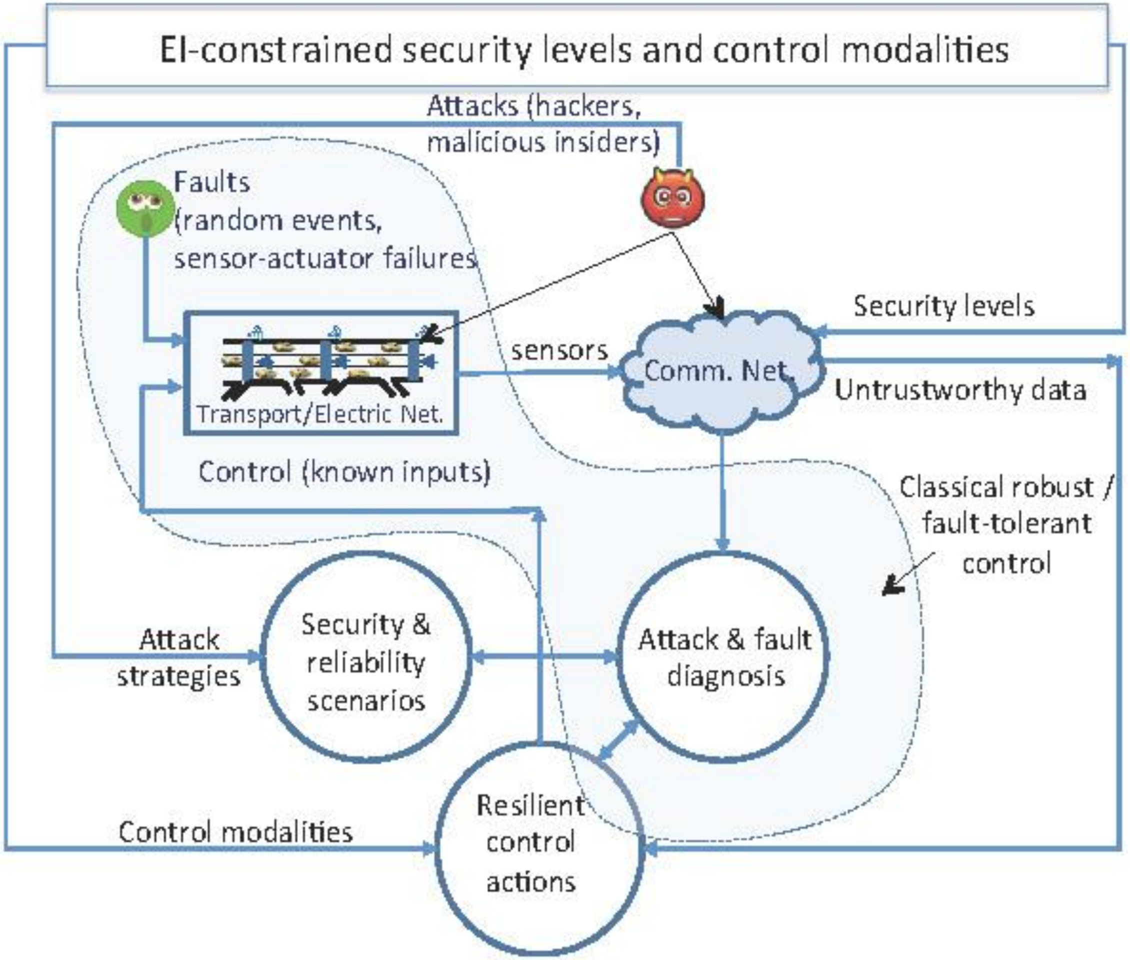
Attack model

- Learn CPS parameters
- Unauthorized access
- DoS / Deception
- Max damage / gain yet evade detection

RC design problem

Max performance subject to

- Security levels & control modalities
- CPS dynamics
- Safety constraints
- Attack / fault hypotheses

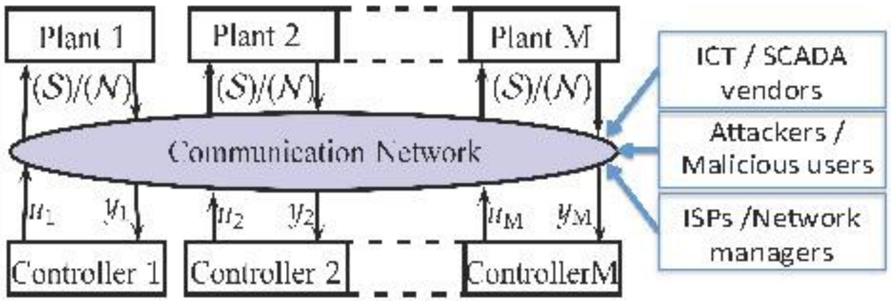

EI-constrained security levels and control modalities
Attacks (hackers, malicious insiders)
Faults (random events, sensor-actuator failures
Transport/Electric Net.
sensors
Comm. Net.
Security levels
Untrustworthy data
Control (known inputs)
Classical robust / fault-tolerant control
Attack strategies
Security & reliability scenarios
Attack & fault diagnosis
Control modalities
Resilient control actions

RC with insecure and unreliable cyber (ICT) components

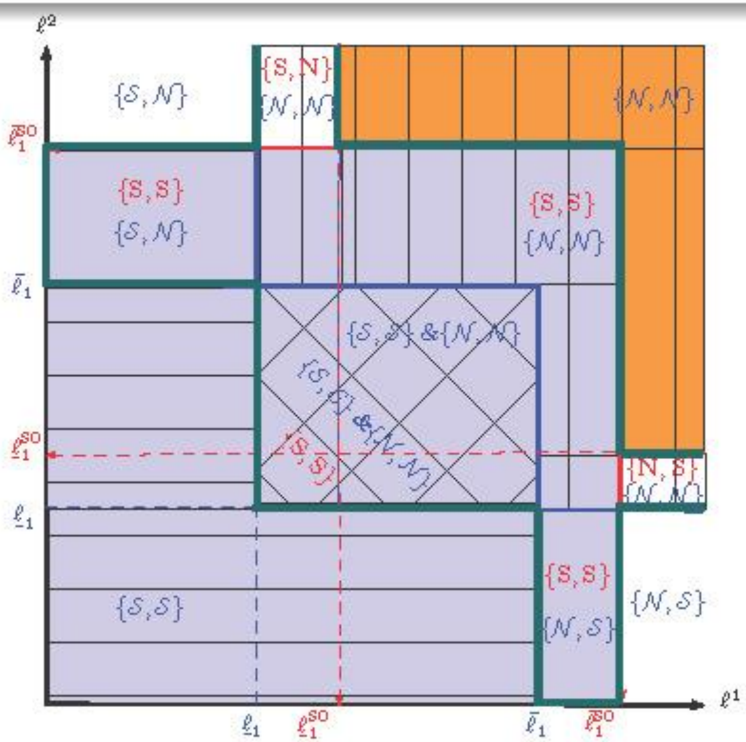
RC-aware EI design

EI for CPS security & reliability

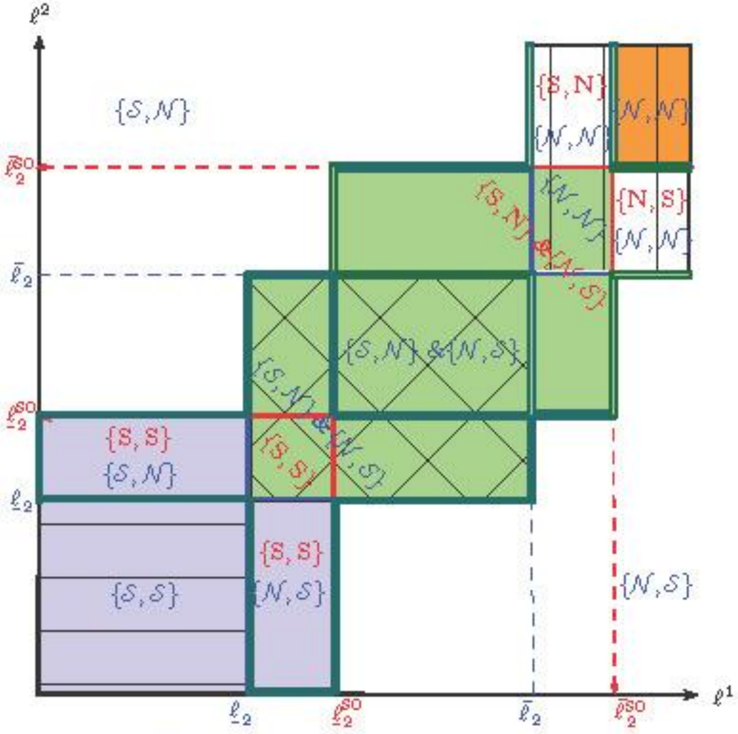
- Network externalities
- Mechanisms design: implement in NE/BNE the social welfare maximizing correspondences



Interdependent security



Increasing incentives



Decreasing incentives

RC+EI: Multi-layer integrated design

Network Games: externalities, investment incentives, residual risk

- Players: Attacker(s), Defenders (CPS owners / Government)
- Failure models: Random, Strategic, Correlated, Byzantine
- Network topologies: Transportation, Electricity T&D, Buildings

Stochastic Control: learning, minimax control, performance benchmark

- Players: Regulators, System operators, CPS managers
- Public uncertainties: Joint distribution of reliability failures (natural events) and security failures (strategic network attacks)
- Control design: Anomaly / intrusion detection, Safety-preserving (switching) control, Supervisory response (reconfiguration / rerouting)

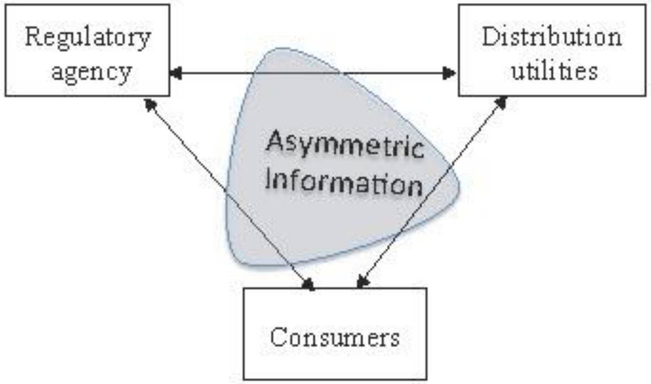
Incentive theory: Mechanism design, mean-field games (static & dynamic)

- Players: Distributors, Large population of travelers / consumers
- Private uncertainties: Individual utilities, asymmetric information
- Mechanisms: Public good provision, Demand response / Pricing

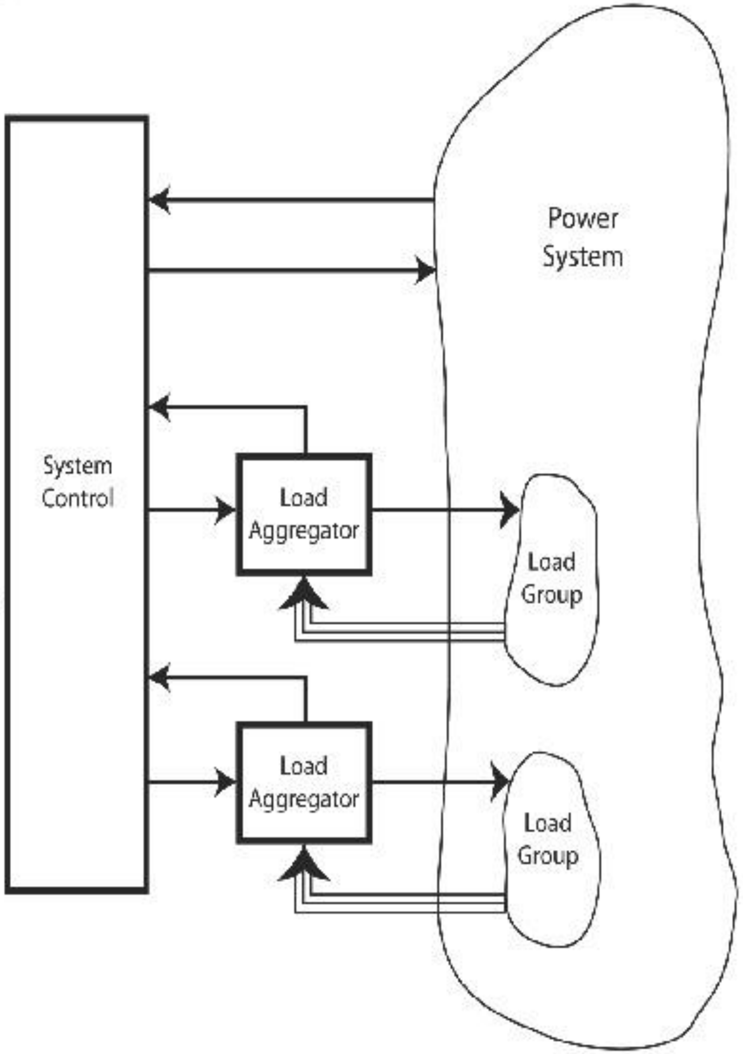
Electricity Transmission and Distribution (T&D)

Wide-area control & Demand response (DR)

- Data: NASPInet (PMUs), NESCOR, IEC & IEEE models, power system simulators
- RC tools: distributed load control, load aggregation (mean-field), balancing (esp. renewables), PHEV charging
- EI tools: DR pricing schemes, T&D regulation, ↓ (non-)technical losses



Regulated electricity distribution

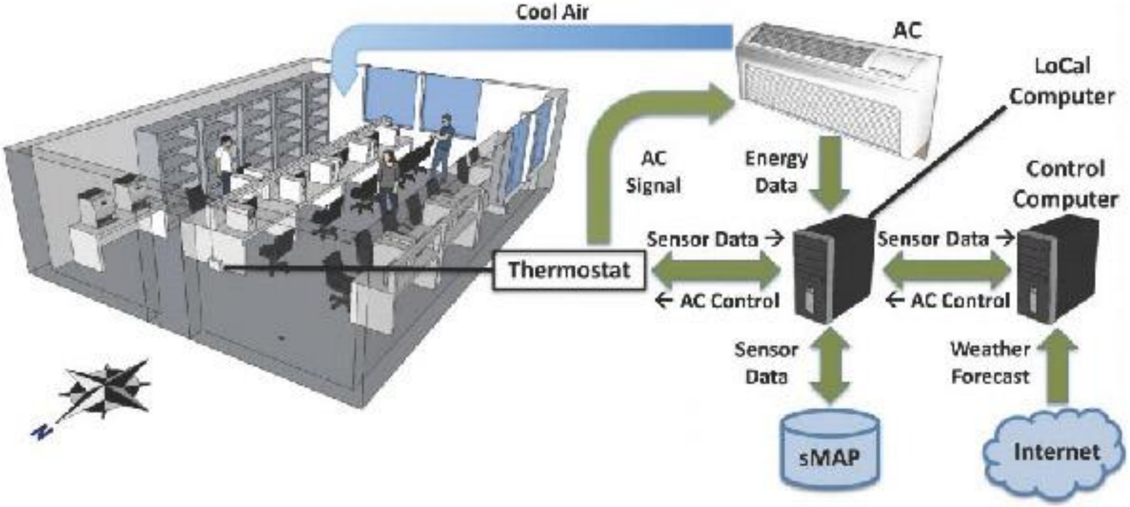


Distributed load control

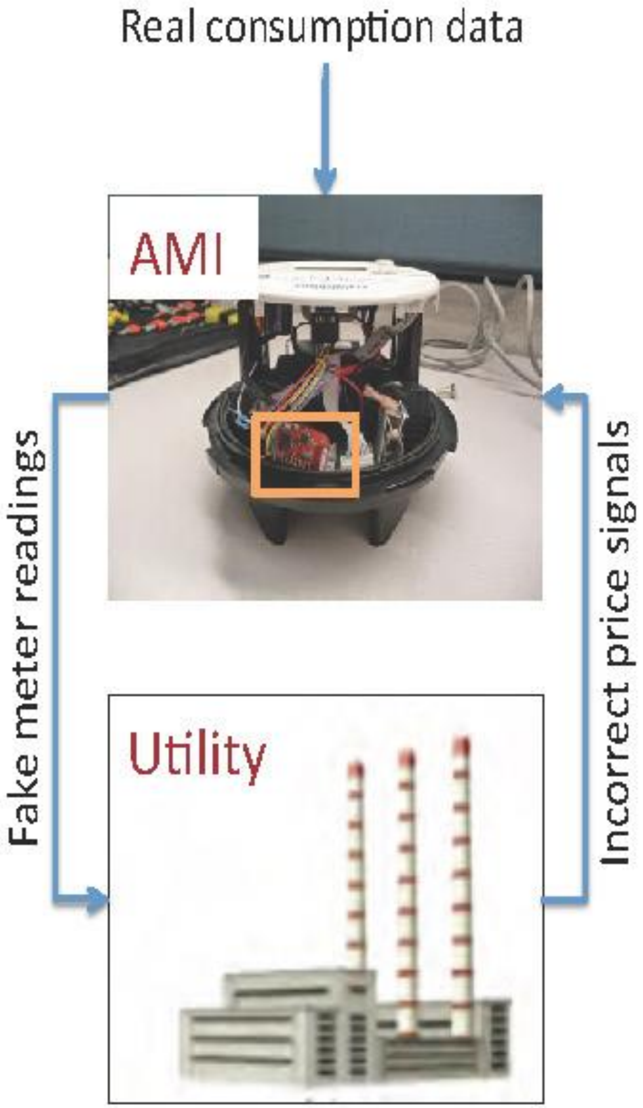
Smart meters and utility networks

Building energy management & DR incentives

- Data: Utility pricing, building operations and loads, consumption patterns
- RC tools: Data fusion, model estimation, integrating occupancy, price, & weather predictions, model-predictive control
- EI tools: Residential DR, AMI security & privacy, ↓ electricity theft/non-payment



BRITE testbed at UCB

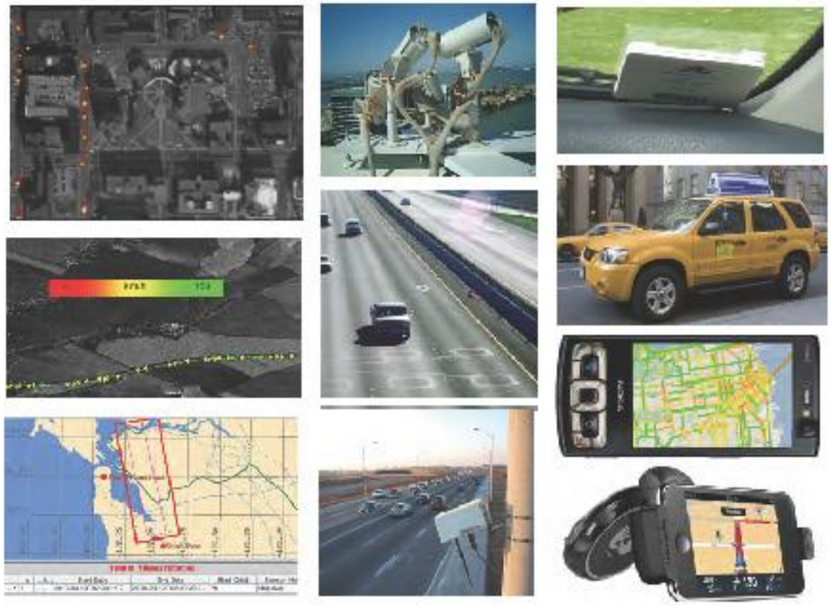


Attacks to AMIs

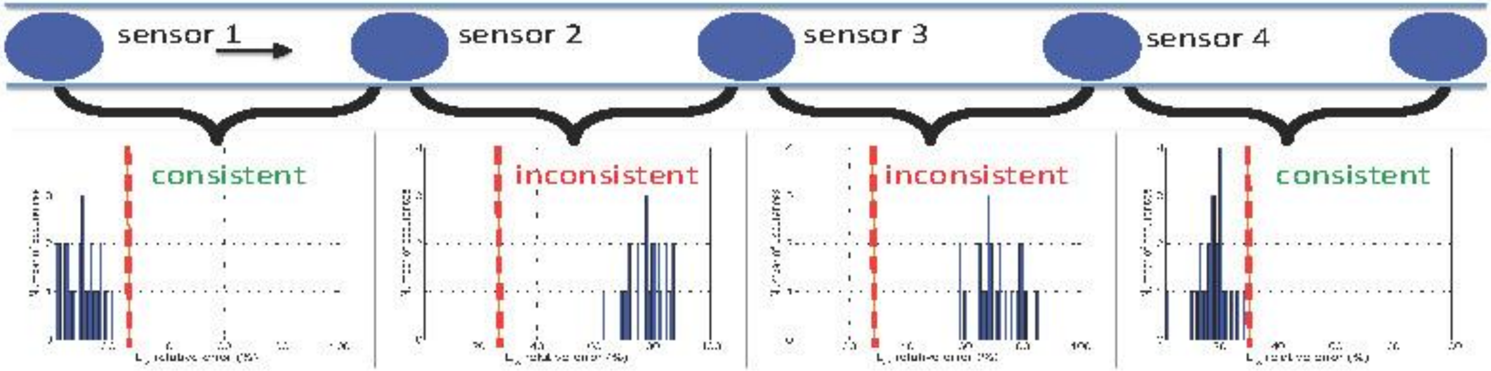
Road Traffic Operations

Mobile Millennium System

- Industry grade platform
- 60 million data points/day
- Tools: Data fusion & consistency, privacy preserving sampling, nowcast, routing, operational control, traveler incentive design
- Real security & reliability scenarios



Traffic data sources

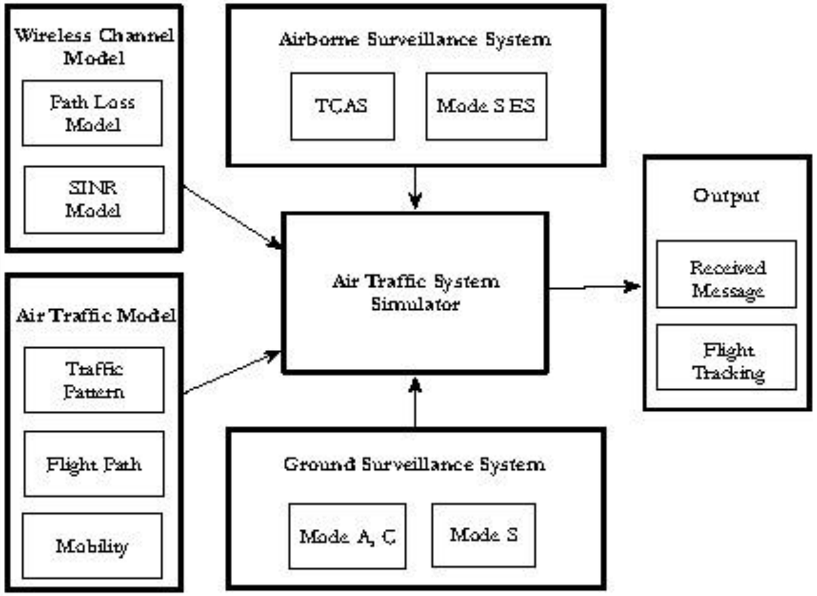


Diagnostics and intrusion detection for traffic information systems

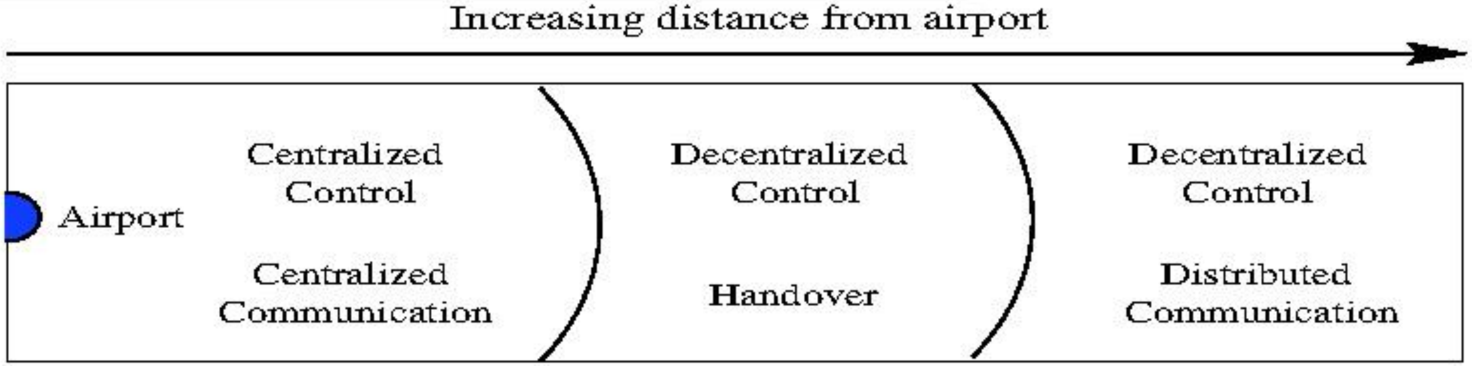
Air Traffic Operations

National Airspace System

- Data: Airport operations, aircraft trajectories, aviation weather
- Airport: Algorithms for ATC choice modeling, scheduling, congestion control, and resource re-allocation
- Airspace: Methods for surveillance (conformance monitoring, threat detection), sectorization, re-routing
- NextGen security & reliability



Air traffic system simulation


Increasing distance from airport
Airport
Centralized Control
Centralized Communication
Decentralized Control
Handover
Decentralized Control
Distributed Communication

Varying degrees of EI+RC integration for air traffic control and comm. systems