Foundations of Secure Cyber-Physical Systems NSF-CPS #1136174 URL: http://securecps.ee.ucla.edu/

Suhas Diggavi (PI) Rafail Ostrovsky Amit Sahai Mani Srivastava Paulo Tabuada
University of California, Los Angeles

UCLA

16-17 November 2015 — NSF CPS PI meeting

Goals

Motivation:

- CPS ubiquitous and security is critical
- Address synchronized attacks on sensors/actuators, plants and networks
- Information security insufficient

Approach:

- Develop holistic CPS security framework.
- Exploit physical system properties + mathematical models → devise provably secure protocols
- Validation on CPS testbeds

Main Contribution

Technical achievements:

- Secure estimation
- Secure active sensing
- SMT solvers for CPS security
- Software obfuscation
- Interactive wireless security
- Secure and private distributed control

Academic impact: Over 50 publications (to date) in top-tier conferences and journals, along with recognitions through paper awards. Over 30 plenary lectures, tutorials and invited talks by PIs.

Press coverage: In Wired magazine, IEEE Spectrum etc.

Connecting to DARPA: Ideas from project used by DARPA's red team in HACMS project.

Secure Computation from Leaky Correlated Randomness

Motivation

- Secure control requires to compute functions securely
- A functionality for secure computation: Random oblivious transfer correlations
- How much leakage is tolerable when recovering oblivious transfer correlations

Results

- Fractional leakage of 1/4 bits is achievable for oblivious transfer → Optimal for oblivious transfer!
- Show existence of a correlation which is more tolerable than oblivious transfer correlations → tolerates up to 1/2 fractional leakage

Secure active sensing: attacks and defenses

Motivation

- Readings from the wheel sensors affect the behavior of the vehicle Anti-lock Brake System (ABS)
- ABS sensors can be spoofed through a relatively simple mechanism of a **non-invasive** attack
- If one or more of these sensors is compromised, the ABS can be tricked into thinking that the car is operating nominally when in fact the car has entered a potentially life-threatening skid
- Devise security mechanisms and characterize fundamental limitations on the attacker imposed by nature

Figure : Consequences of an ABS attack

Defense Mechanism

- Detecting sensor attacks is an authentication problem
- By placing "physical" challenges, a secure sensor can authenticate if the response is from a "trusted" gear
- Challenge: changing the magnetic field, randomly, from ON to OFF and from OFF to ON
- Attacker side: Small probability of detection → Fundumental delayed response to the challenge
- Use the delay in order to detect the attack or even securely sense

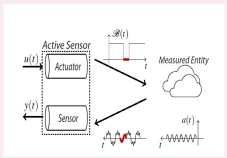


Figure : Challenge-Response Mechanism

Results

- Accurate detection of adversarial attack, and estimate the wheel's speed

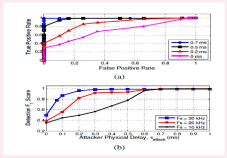


Figure : Performance of defense scheme

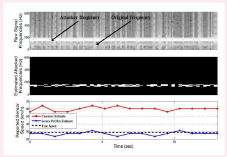


Figure : Estimation scheme

Secure MMSE estimation and SMT solvers

Motivation

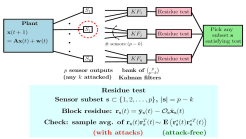
- Critical infrastructures supported by feedback control loops
- Attacking sensors and actuators can disable control mechanism
- Stochastic dynamical systems under attack experience adversarial noise along with measurement and process noise
- State estimation → basic component!

Approach

- Previous works considered secure estimation and control for deterministic dynamical systems
- Develop optimal MMSE estimation in the presence of adversarial attacks on the measurements of the sensors
- The proposed state estimator involves Kalman filters operating over subsets of sensors to search for a sensor subset which is reliable for state estimation
- To improve the subset search time: propose Satisfiability Modulo Theory (SMT) based techniques to exploit the combinatorial nature of searching over sensor subsets

Main Results

- A cross-validating estimation architecture that asymptotically achieves the MMSE performance when we know which measurements were attacked
- Coding-theoretic interpretation for the necessary and sufficient conditions for secure state estimation in deterministic dynamical systems



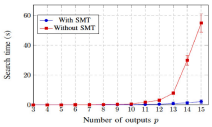


Figure : Comparison of sensor subset search times

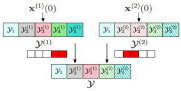


Figure : Coding-theoretic interpretation for secure state estimation

UCLA