2017 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

Towards Secure Networked Cyber-Physical Systems: A Theoretic Framework with Bounded Rationality

- Walid Saad (Lead PI)
- Virginia Tech
- walids@vt.edu
- CNS-1446621

- Arif Sarwat (PI), Kamal Akkaya (co-PI), Ismail Guvenc (co-PI)
- Florida International University
- asarwat@fiu.edu
- CNS-1446570

- Saroj Biswas (PI), Aunshul Rege (co-PI), Li Bai (co-PI)
- Temple University
- sbiswas@temple.edu
- CNS-1446574

VIRGINIA TECH™

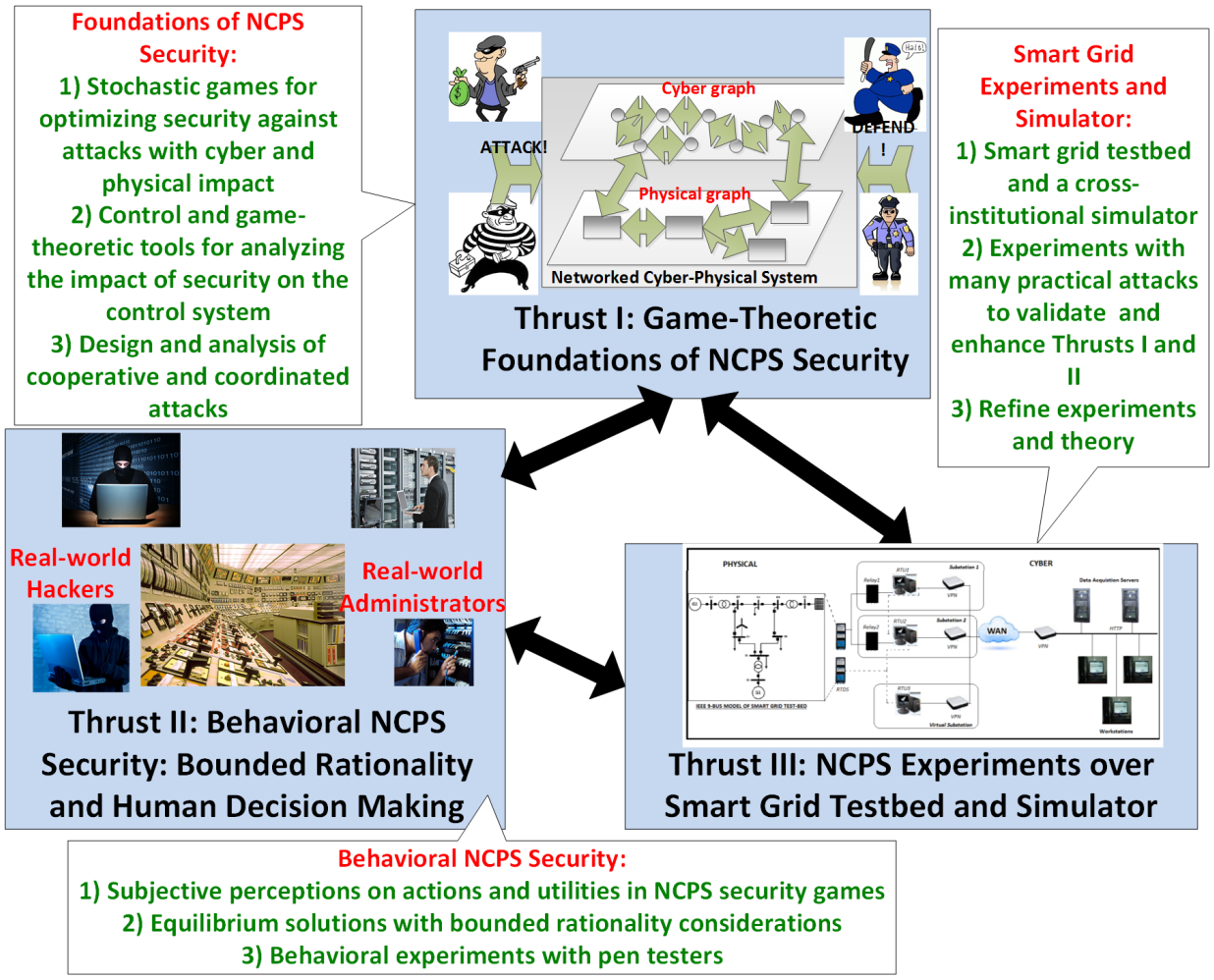
FIU | FLORIDA INTERNATIONAL UNIVERSITY

TEMPLE UNIVERSITY®

Project Description and Goals

The **goal** of this project is to develop a unified and **domain-agnostic** framework for designing secure and trustworthy **networked cyber-physical systems (NCPSs)** by leveraging on the synergies between the cyber, physical, and human realms.

- **Thrust I:** A blend of control and stochastic game techniques for developing new approaches to secure NCPSs against both cyber and physical threats.
- **Thrust II:** Novel behavioral game-theoretic frameworks for NCPS security that incorporate notions of bounded rationality in human decision making.
- **Thrust III:** Implementation over a cross-institutional smart grid testbed for validation and evaluation.



Recent Results

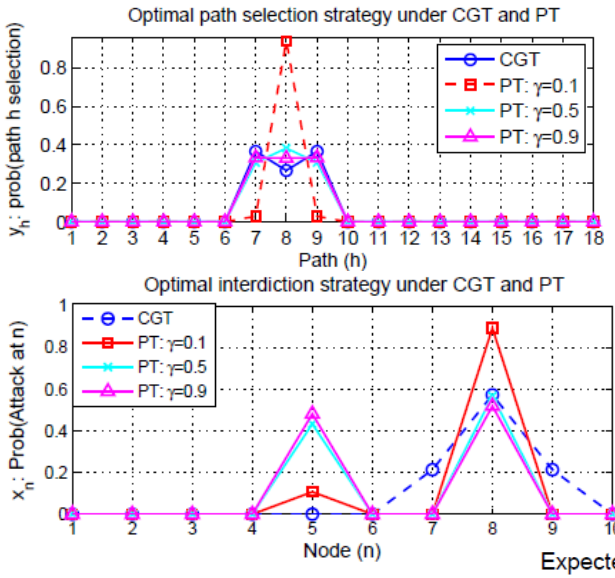
Prospect Theory for Secure Delivery Drones

❑ Network interdiction game:

- Path selection strategy (mixed) vs. interdiction strategy (mixed).
- **Goal:** minimize vs. maximize expected delivery time.

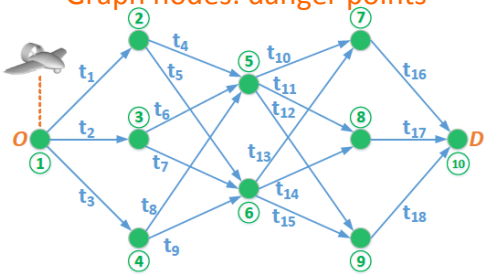
❑ *Prospect Theory (PT) vs. Classical Game Theory (CGT)*:

- Expected delivery time valued w.r.t target time, R ***(framing effect)***
  - E.g. emergency medicine delivery, amazon prime air's 30 min,…
- Disparate perceptions of risks, prob. of successful attack, ***(weighting effect)***.



O: origin, D: Destination

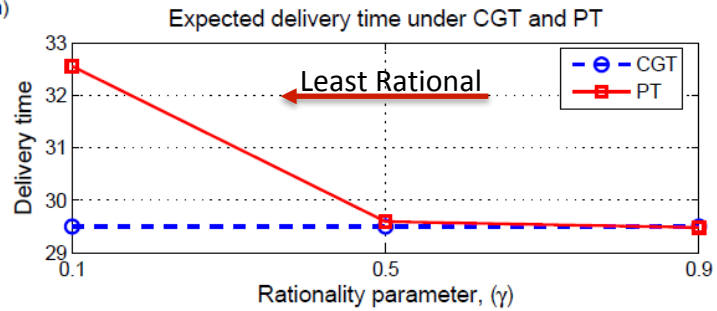
Graph nodes: danger points



Subjective perception of risk levels (with R=30)

→ risky strategy

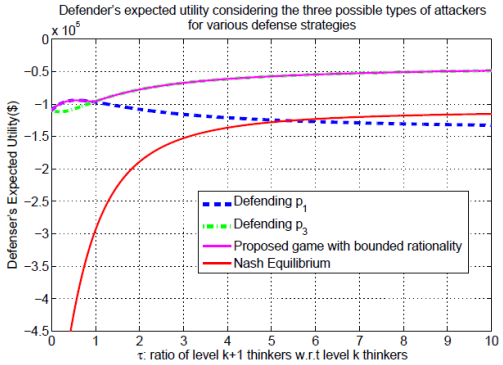
→ longer delivery time



Propagation of Threats in NCPS with Smart Grid Application

❑ Cognitive Hierarchy Theory and Hypergames:

- Higher level thinkers:
  - Better system knowledge.
  - Better computational capabilities.
  - Wider attack space.
- Multiple ***levels of thinking.***
  - *Level 0:* attacks randomly.
  - *Level 1:* attacks line with highest flow.
  - *Level 2:* attacks node triggering worst cascading failures.



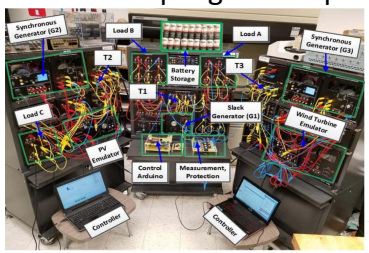
Experimental Analysis

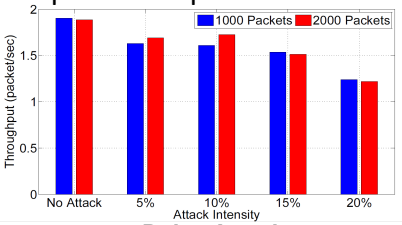
❑ Impact of cyber attacks on physical NCPS

- Two identical hardware-based IEEE 9-bus testbeds at Temple and FIU
- DoS, packet drop, message integrity, and delay attacks tested on the two testbeds.

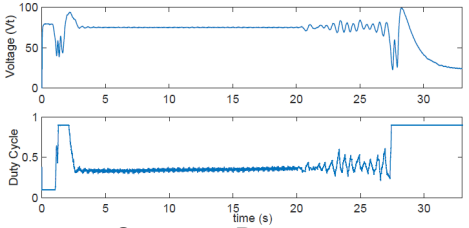
❑ Cyber attacks in grid tied generator control

- Hold the last received data in the event of packet drop.
- Stable if packet drop probability < threshold.
- Faster sampling rate improves packet drop threshold.





Delay Attack



Generator Response