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

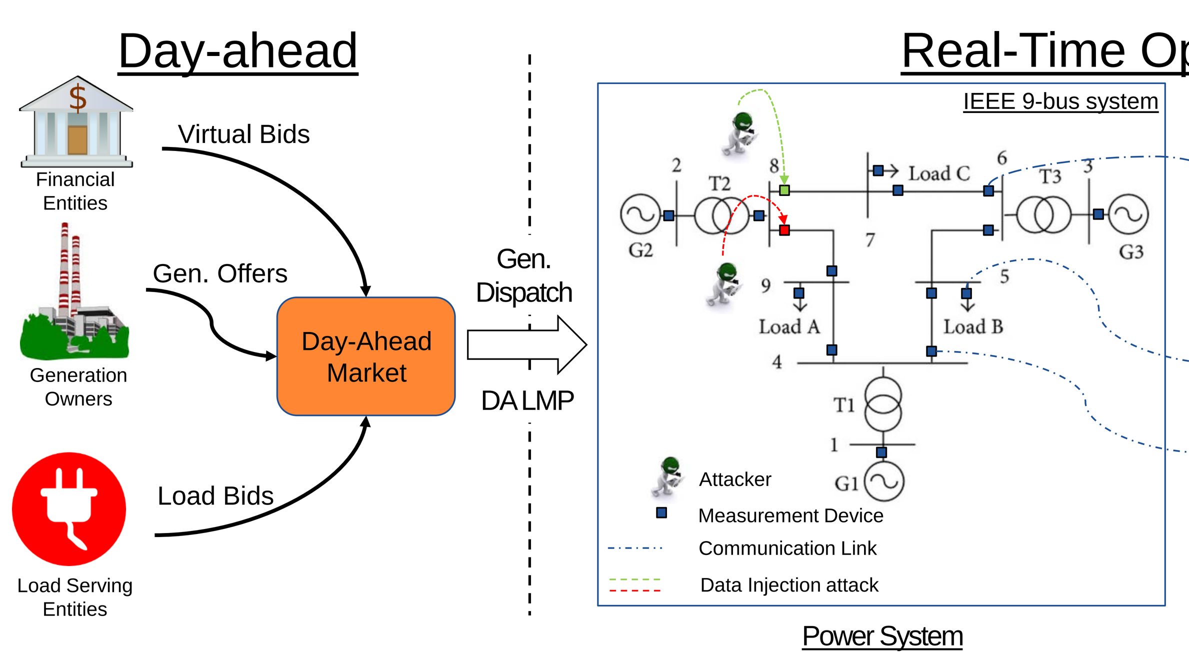
VT: Walid Saad (PI), FIU: Arif Sarwat (PI), Ismail Guvenc, Kemal Akkaya,
Temple: Saroj Biswas (PI), Aunschul Rege, Li BAi

Data Injection Attacks on Smart Grids with Multiple Adversaries – System Model

❖ Data Injection Attack:
- ➢ Target: state estimator.
- ➢ Objective: manipulate LMPs.
- ➢ Financial framework: virtual bidding.

❖ Strategic model: A Stackelberg game.
- ➢ Leader: System operator.
- ➢ Followers: Attackers.
- ➢ Integration of costs of attacks and defense in system model.

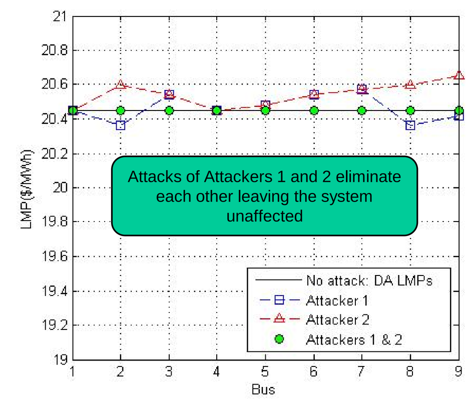
❖ Attackers' strategic interaction in reaction to the leader's defense strategy:
- ➢ A Noncooperative Game.
- ➢ Adversarial nature of attackers: attacks can cancel out.



Power System

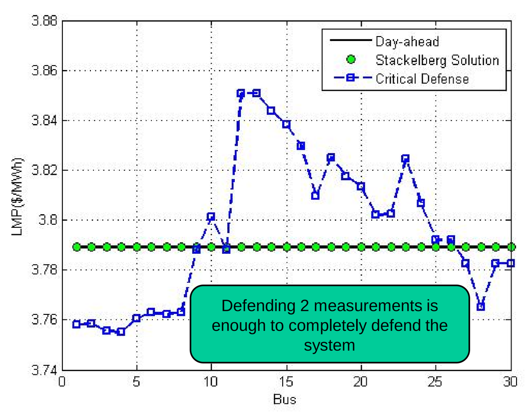
Data Injection Attacks on Smart Grids with Multiple Adversaries – Results

IEEE 9-bus test system: 2 attackers and 1 defender

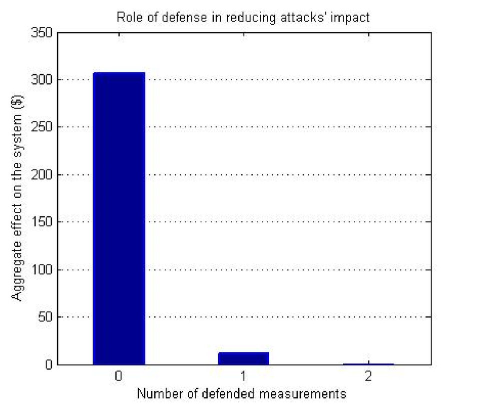


Attackers adversarial strategies:
Attackers can choose to launch eliminating attacks at equilibrium without any taken defensive action.
No Defense Is Required!

IEEE 30-bus test system: 3 attackers (each attacking 3 measurements) and 1 defender



Stackelberg equilibrium with 2 defended measurements:
Superiority of the optimal defense strategy over the seemingly intuitive strategy of defending the two measurements that can affect the system the most (critical defense).



Role of defense: Defending a small fraction of vulnerable measurements has a huge impact:
Defending 1 measurement (10% of vulnerable measurements): huge decrease in attacks' effect.
Defending 2 measurements (20% of vulnerable measurements): eliminate attacks' effect.

Algorithm 1 Distributed Learning Automata

Input: Number of attackers M
Action space of each attacker $\mathcal{Z}^{(m)}$
Output: Strategy vector of each player $\boldsymbol{q}^{(m)}$
1: Initialize $\boldsymbol{q}^{(m)}(0)$
2: **while** Not Converged **do**
3: Randomly select $z^{(m)}(t)$ based on $\boldsymbol{q}^{(m)}(t)$
4: Collect payoff $U_m(t)$
5: Update strategy vector
$\boldsymbol{q}^{(m)}(t+1) = \boldsymbol{q}^{(m)}(t) + bU_m(t)\left(\boldsymbol{e}^{(m)}(t) - \boldsymbol{q}^{(m)}(t)\right)$
6: Check Convergence
7: **if** Converged **then**
8: Break
9: **end if**
10: **end while**
11: **return** Strategy vector $\boldsymbol{q}^{(m)}$

Finding the equilibrium:
Distributed learning algorithm that operates under limited system information is proposed and shown to converge to the game solution.

Future Work:

❖ Investigate the bounded rationality of attackers and defenders interacting over a networked cyber-physical system (NCPS) and the effect of such cognitive limitation on NCPS security.

❖ Devise a comprehensive and generic framework modeling the strategic interaction of attackers and defenders over a cyber-physical system.

Resource Allocation for Critical Infrastructure Protection

❖ A contract-theoretic approach is proposed to solve the problem of resource allocation in critical infrastructure protection with asymmetric information.

❖ A control center (CC) is used to design contracts and offer them to infrastructures' owners.

❖ Contracts are designed to maximize the CC's benefit and motivate each infrastructure to accept a contract and get proper resources for protection.

❖ Critical infrastructures (CIs) are defined by both vulnerability levels (Weakness level) and criticality levels (importance); unknown to the CC.

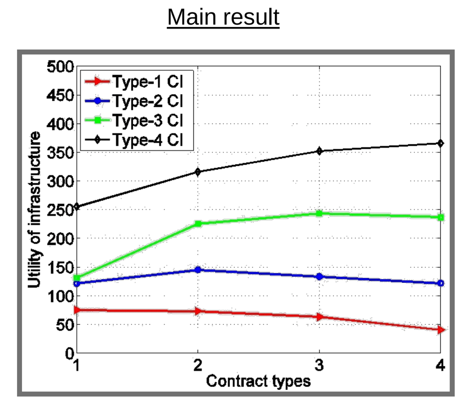
❖ Therefore, each CI can claim that it is the most vulnerable or critical to get more resources.

❖ Optimal contract algorithm handles such an asymmetric information while providing optimal contracts that motivate each CI to reveal its actual type.

Optimal contract algorithm

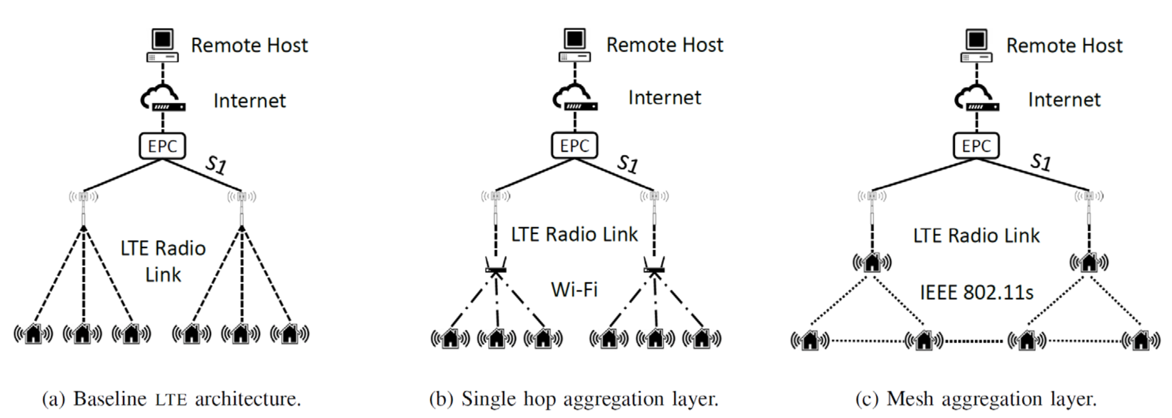
Algorithm 1: Optimized Contract implementation of CC for Resource Allocation
Input: $\mathcal{M}, \mathcal{K}, p_{i,w_j}, q_{i,\theta_j}, T_{\max}, T_{i,min}$
Output: $(T, R(T))$
1. CC declares its willingness to protect some infrastructures
2. Receive request from infrastructures willing to be protected
3.**Solve the optimal contract** for current infrastructures
if *The program has a solution, i.e, the avaialble resources are sufficient for all users* **then**
  Contracts are ready, proceed to step 4
else
  Remove the least critical infrastructure (begin with higher probability)
  return to step 3
4. **The CC Offers the contracts and waits for feedback**
if *All infrastructures accepted the offered contracts* **then**
  proceed to step 5
else
  return to step 3, for any previously excluded infrastructures
5. Sign contracts with infrastructures and allocate resources

Main result



The utility of each Infrastructure when choosing the contract designed for its type and contracts designed for other types. It is clear that the infrastructure will get the maximum utility when choosing the contract designed for its type.

Hybrid Wi-Fi/LTE Aggregation Architecture for Smart Meter Communications



(a) Baseline LTE architecture. (b) Single hop aggregation layer. (c) Mesh aggregation layer.

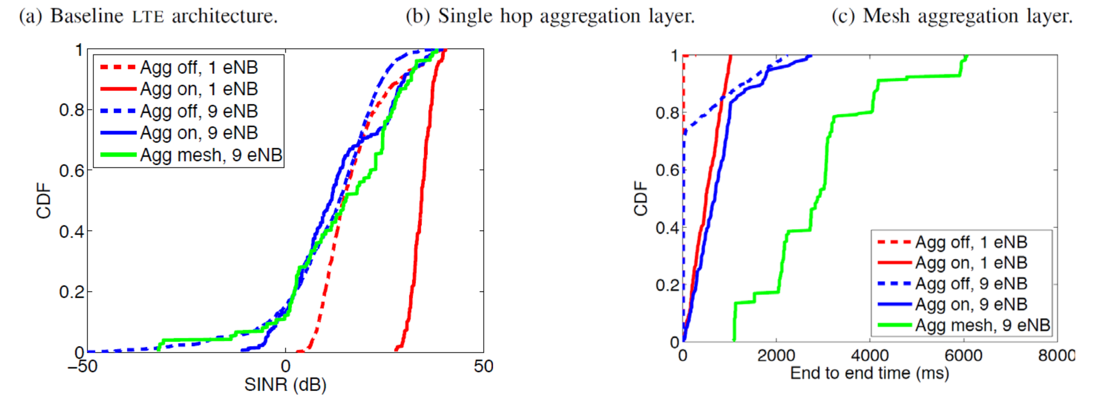


TABLE I: LTE simulation settings in NS-3.

Parameter	Value	Unit
E-UTRA operating band	1	
DL/UL EARFCN	100/18100	
Downlink central frequency	2120	MHz
Uplink central frequency	1930	MHz
Bandwidth	4.5	MHz
Duplexing scheme	Frequency division duplex	
Cycic prefix length	4.69	μs
Maximum UE Tx power	23.0	dBm
Maximum eNB Tx power	46.0	dBm
UE Rx noise figure	9	dB
eNB Rx sensitivity	5	dB
Uplink power control α	0	
HARQ	Enable	
Uplink grant MCS	1	
Scheduler algorithm	Proportional fair	
Inter site distance	2000	m
Bearers/UE	2	
SRS period	3200 (non standard)	ms
UE hight	1.5	m
UE speed	0	m/s
eNB sites	3	
eNB height	30	m
Shadow σ external wall	1	dBm
Shadow σ outdoor	1	dBm
Shadow σ indoor	1.5	dBm
Roof-top level	5	m
eNB antenna	Parabolic antenna	
eNB antenna beamwidth	120	degree
IP standard	IPv4	
IEEE 802.11 MAC	IEEE 802.11b	

Adversarial Decision-Making Behavior

❖ Objective:
- ➢ Understand the adversarial mindset in infrastructure cyberattacks
- ➢ Validating the cyber kill chain
- ➢ Estimating probability of various types of attackers' and defenders' actions for game theoretic analysis.

❖ Methodology:
- ➢ Interviews with 10 control systems penetration testers
- ➢ Observations of one red-blue cybersecurity exercise
- ➢ Conduct surveys among penetration testers

❖ Findings:
- ➢ Decision-making continuously evolves, with reconnaissance being the most relevant
- ➢ Intrusion chains are structured as intrusion 'cycles', depending on defender actions, adversarial inadequacy, and maintaining presence inside targeted environment.
- ➢ Multiple intrusions chains are evident at any given time suggesting complexities in existing game theoretical explanations.

❖ Ongoing Work:
- ➢ Designing surveys to capture and validate intrusion chains and attack vectors
- ➢ Designing red-blue cybsersecurity experiments

Coordinated Cyber-Physical Attack Experiments over Smart Grid Testbed

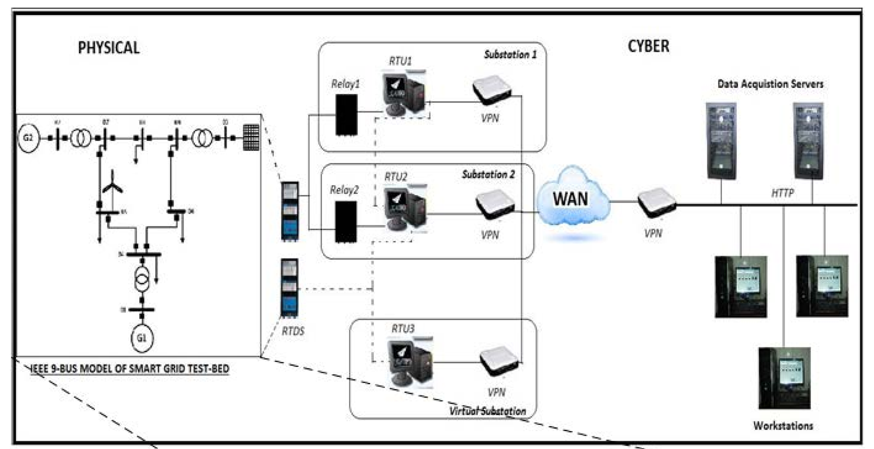
❖ Coordinated Cyber-Physical Attack:
- ➢ Element: Including Physical attacks and denial-of service (DoS) attacks.
- ➢ Target: transmission lines of the smart grid.
- ➢ Objective: "Disruption" of the load.

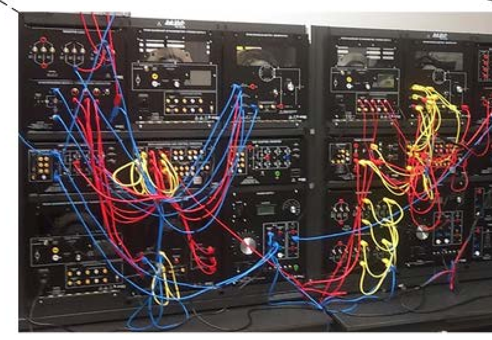
❖ Optimal Load Shedding:
- ➢ Objective: To determine where and how many load needed to be shed due to coordinated cyber-physical attacks for minimizing the expected cost of load shedding.

❖ Attacker vs. Defender:
- ➢ Model: A Non-cooperative game.
- ➢ Utility: Expected cost of load shedding.
- ➢ Strategy: Distribution of finite attacks (defense mechanisms) on transmission lines.
- ➢ Object: Nash Equilibrium.

❖ Learning Algorithm:
- ➢ Minimax Q-learning vs Proposed Algorithm

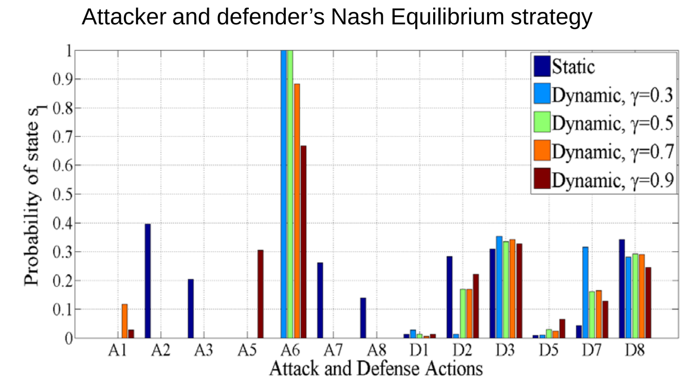
Layered architecture of Proposed Testbed at FIU



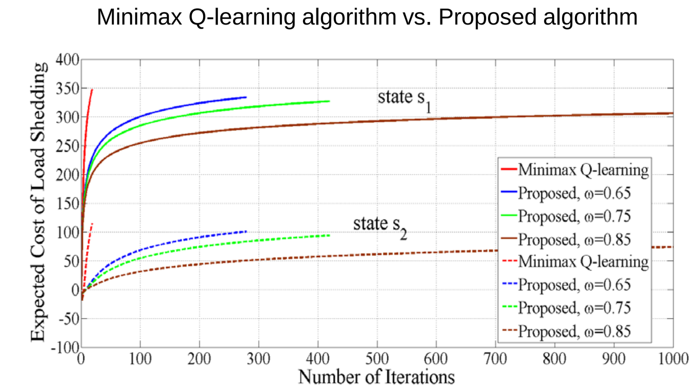


Main Result

Attacker and defender's Nash Equilibrium strategy



Minimax Q-learning algorithm vs. Proposed algorithm



Identifying Cyber Vulnerabilities in Automatic Generation Control Systems

❖ Data injection attack in AGC loop.
- ➢ AGC is an integral part of Energy Management System
- ➢ AGC processes grid data received from SCADA
- ➢ False data injection through multiple entry points: frequency sensor, tie line flow, and load change command data.
- ➢ Attacker's objective: Set generators into transients and instability

❖ Identify the most vulnerable entry point in AGC
- ➢ Objective: Determine the entry port that may induce the largest transients in the grid due to a data attack

❖ Approach: Stochastic stability analysis
- ➢ Model: Simplify IEEE 9-Bus system to a two-area control system
- ➢ Stochastic dynamic model with embedded control and noise
- ➢ Determine ball of convergence of state error

❖ Main result
- ➢ Tie line flow data and load change data ports are most sensitive.
- ➢ Induces large transients due to relatively small data attacks (figure)
- ➢ Possible defense: Fast acting AGC controller and large AEC time constant.