Compromising Security of Economic Dispatch in Power System Operations

Devendra Shelar, MIT

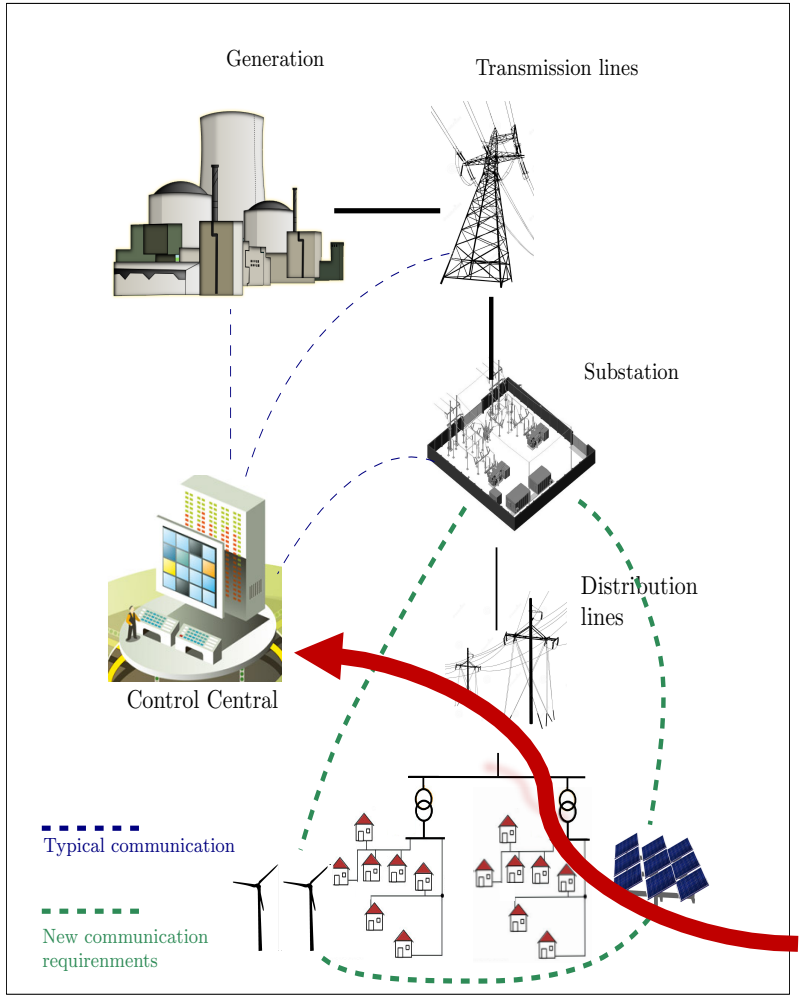
Dependable Systems and Networks, June 29th, 2017

Joint work with

Saurabh Amin, MIT

Pengfei Sun and Saman Zonouz, Rutgers

Focus of the talk



Economic dispatch

- United States - 4 Billion MWh of energy produced
- Around 400 Billion $ revenues per annum
- Day-ahead market, real-time operations

Question - Cybersecurity of economic dispatch software (in the control center) in the wake of semantics-aware memory data compromises

Security failures (attacks): post Stuxnet

Cyberspies: hacking into US electric grid (2009)

Dragonfly: DERs give backdoor entry (2013)

Sniper attack: PG&E's Metcalf substation (2013)

Ukraine: Outages & equipment damage (2016)

Motivation

Characteristics of previous attacks

- Not geographically diverse attack
- Control center node attacks
- Sub-optimal attacks
  - Did not fully exploit the physics of the underlying system
- In Ukraine attack, attacker had full control of the grid controller
  - Power was restored after 6 hours

Question

- Can there be a more damaging attack with lesser attacker control?

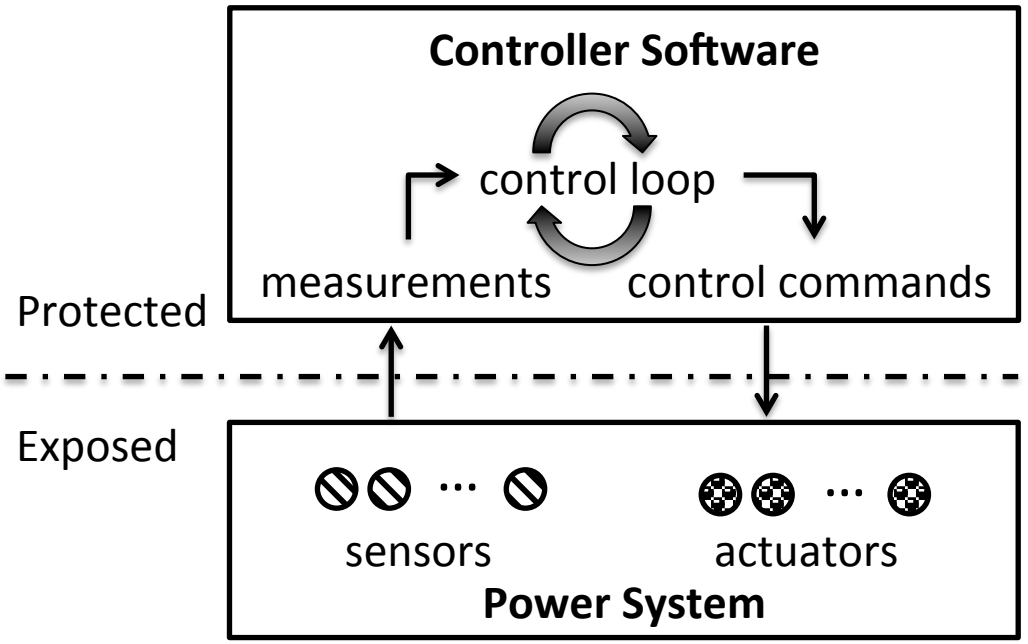
Our contributions

Semantic data attack on power grid controller software

- Attack on control algorithm – Economic Dispatch (ED)
  - Using network and power system knowledge
  - Game-theoretic framework for optimal attack strategy

- Implementation based on memory data corruption
  - Leverage logical memory invariants in the software
  - Implemented on widely used ED software

Overall approach



Attacker's 3-step plan

Memory pattern extraction using offline software analysis

Optimal attack generation for modifiable parameters

Run-time attack: Control-sensitive data location and corruption

Related Work

Cyber security issues of the power system

- M. Reiter et al. – False data injection attacks against state estimation
- Z. Zhang et al. – Bad data identification based on measurement
- Z. Kalbarczyk et al. – False data injection attacks against automatic generation control

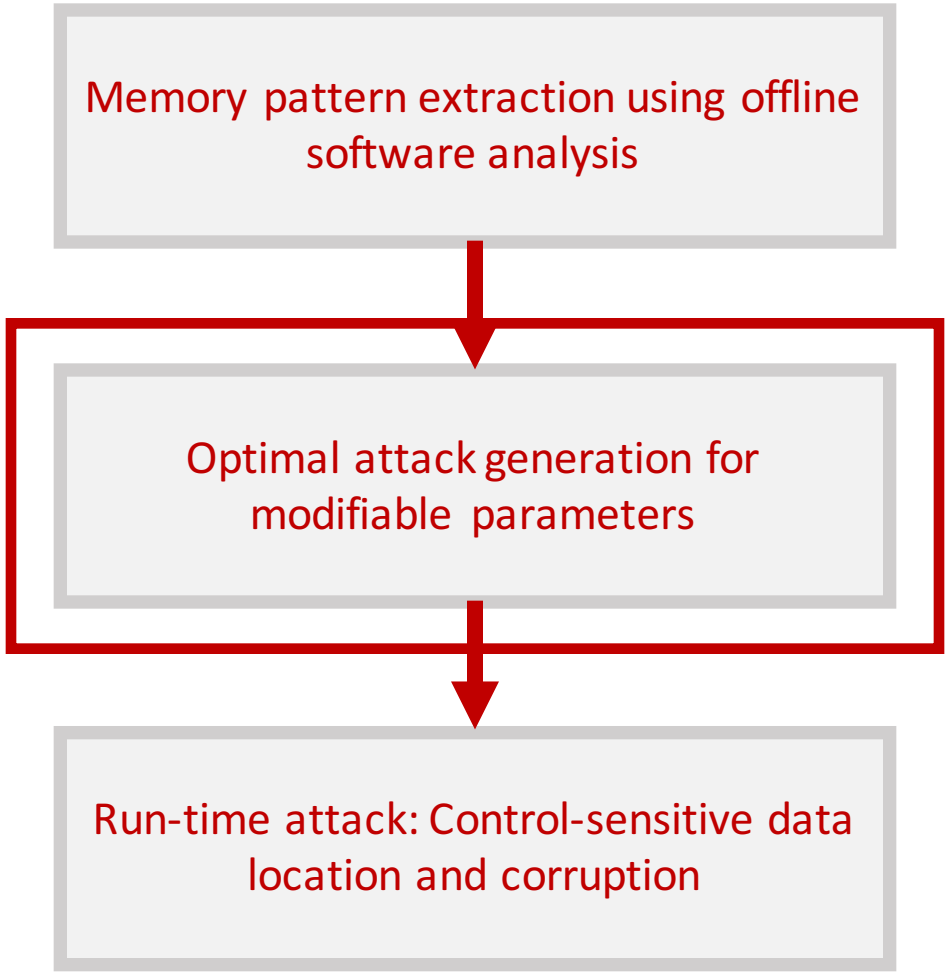
Physical vulnerabilities of the power system

- Bienstock et al. – N-k problem, cascades
- Kevin Wood et al. – Network interdiction problem

Comments

- Lack of integrated approach to implement optimal attack into the control algorithm
- Assume that the attacker can directly compromise distributed sensors or components
- Assume knowledge of network parameters that usually resides at the control center

Attacker’s 3-step plan



Optimal attack generation

A sequential game between attacker and defender (operator)

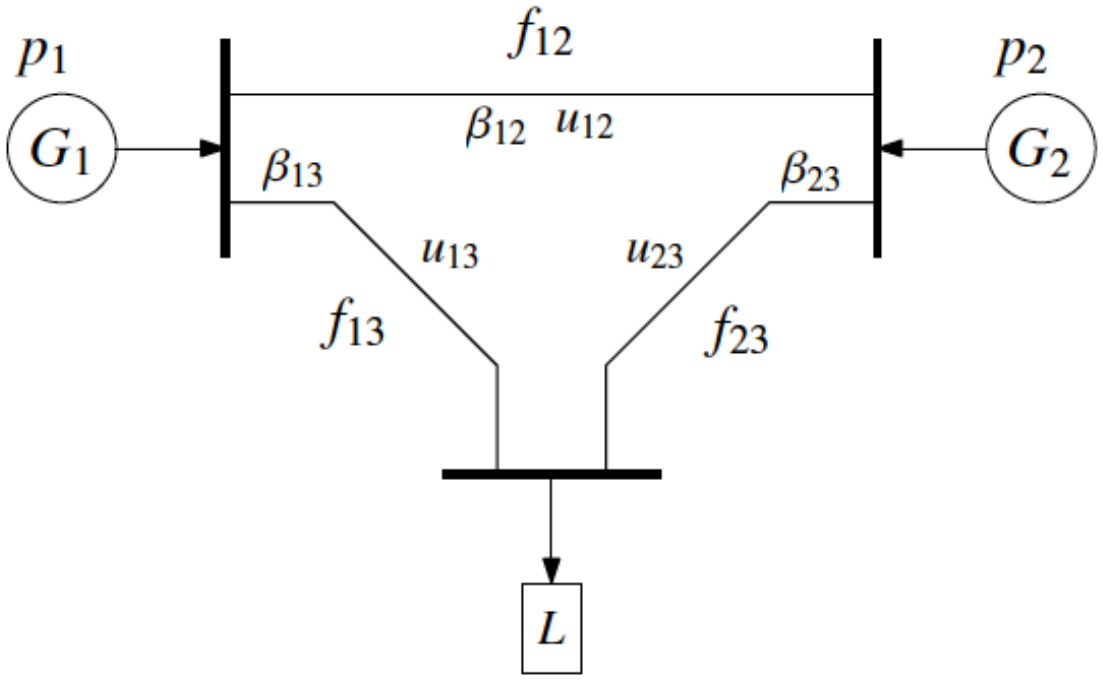
- Attacker moves first
  - Stealthily manipulates parameters of the economic dispatch
- Defender (operator) moves next
  - Computes economic dispatch

Problem statement:

- Determine optimal attack plan (i.e. parameter manipulation) to maximize power system violations
  - Assuming defender does economic dispatch with manipulated DLR values

Economic Dispatch

- Inputs
  - network topology
  - Generator / demand data
  - Network parameters
- Constraints
  - Device limits
  - Power flows
  - Supply-demand balance
- Output
  - Generation levels
- Objective
  - Minimize cost of generation



Economic Dispatch

$$\min_{p,\theta,f} C(p)$$

Minimize total cost of generation

subject to $\sum_{i \in G} p_i = \sum_{j \in V} d_j$

Total Supply = Total demand

$\forall \{i,j\} \in E$ $f_{ij} = \beta_{ij}(\theta_i - \theta_j)$

Ohm's law (DC power flow)

$\forall i \in V$ $\sum_{j:\{i,j\} \in \mathrm{E}} f_{ij} = \sum_{k \in G_i} p_k - d_i$

Power flow conservation

$\forall \{i,j\} \in E$ $|f_{ij}| \leq u_{ij}$

Line capacity limits

$\forall i \in G$ $p_i^{min} \leq p_i \leq p_i^{max}$

Generation bounds

$C(p) = \sum_{i \in G} a_i\, p_i^2 + b_i p_i + c_i$

Generation cost functions

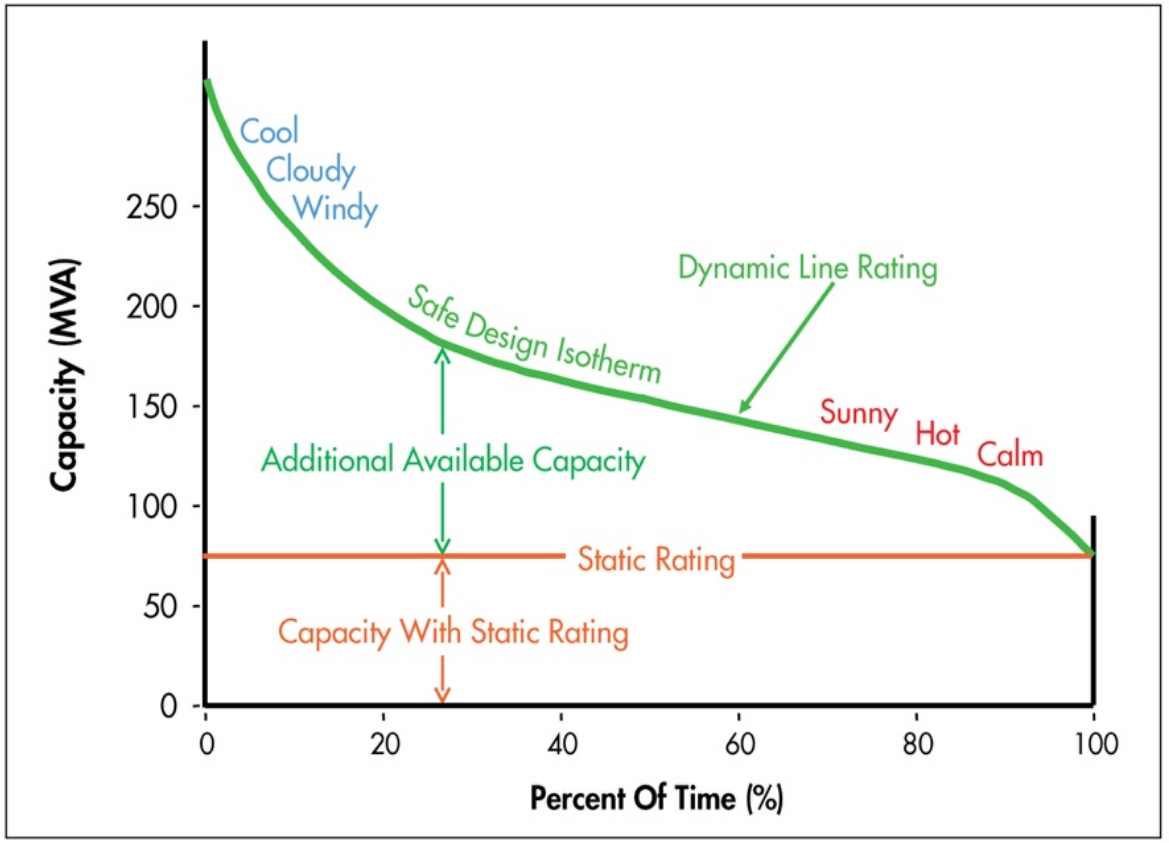
Dynamic Line Ratings (DLR)

$$u_{ij} = \begin{cases} u_{ij}^{s} \text{ if } \{i,j\} \in E^{S} & \text{(static)} \\ u_{ij}^{d} \text{ if } \{i,j\} \in E^{D} & \text{(DLR)} \end{cases}$$

Lower and upper bounds for DLR values

$$u_{ij}^{min} \leq u_{ij}^{d} \leq u_{ij}^{max}$$

Figure 1: Tapping into existing capacity above the static rating



Source: Valley Group

Economic dispatch

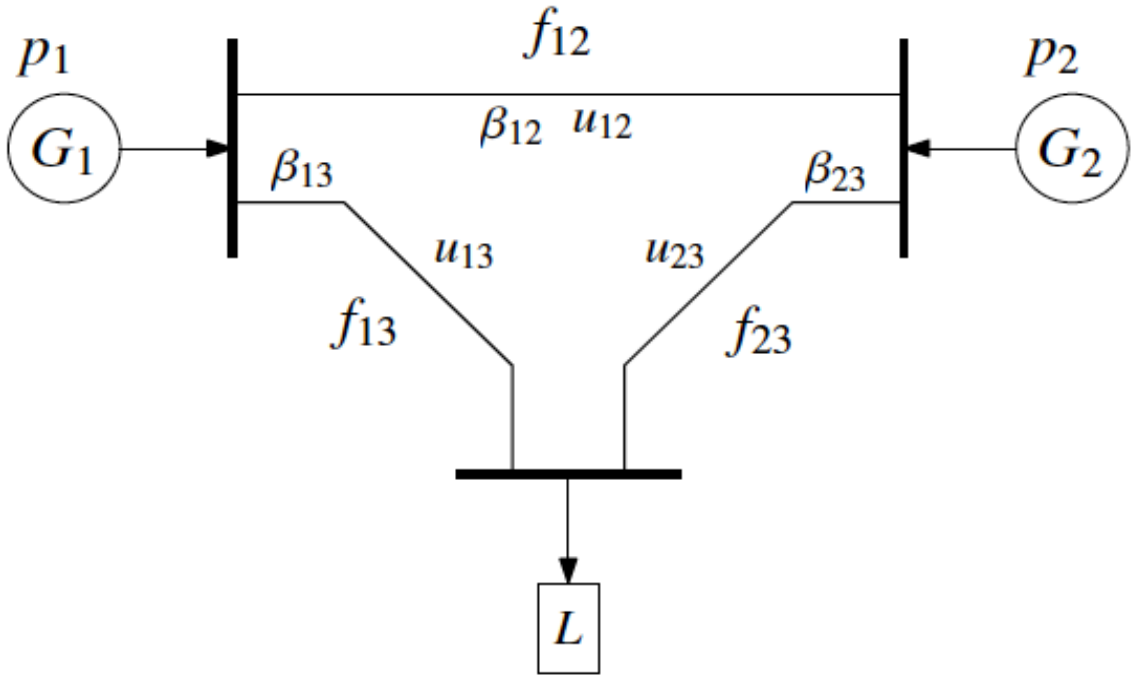
$$\left(y^{\star}(u^{d}), s^{\star}(u^{d})\right) \in \arg\min_{y,s} \ \frac{1}{2} y^{T} H y + h_1^{T} y + h_2$$

Subject to $\quad By + s = b$

$$s \geq 0$$

Illustration of DLR manipulation

- G2 has lower costs
- Load, $d_3 = 300$.
- If $u_{13}^d = u_{23}^d = 150$, then
  - $p_1 = p_2 = 150$
  - $f_{13} = f_{23} = 150$
- If $u_{13}^a = 100, u_{23}^a = 200$, then
  - $p_1 = 0, p_2 = 300$ MW
  - $f_{13} = 100$, $f_{23} = 200$, 33% violation



Sequential Game

Sequential interaction between the attacker and the defender (operator)

Attacker model

Action set – Compromise DLR values $u_{ij}^d = u_{ij}^a$

such that $u_{ij}^{min} \leq u_{ij}^a \leq u_{ij}^{max}$

Objective – Maximize the maximum line capacity violation over all DLR lines

Defender model

Assume the (possibly manipulated) DLR values

Compute the economic dispatch solution

$$\max_{u^a} U_{\text{cap}}\left(\hat{u}^d = u^a\right) \coloneqq \max_{\{i,j\} \in E^D} 100 \left(\frac{|f_{ij}^\star|}{u_{ij}^d} - 1 \right)_+$$

where $p^\star, \theta^\star, f^\star(\hat{u}^d) \in \arg\min_{p,\theta,f} C(p)$

s.t. economic dispatch constraints

KKT-based Mixed Integer Linear Program

$2|E^D|$ subproblems

Focus on one DLR line at a time

$$\max_x g^T y^\star$$

$$\text{s.t.} \quad Ax \le e$$

$$y^\star, s^\star \in \arg\min_y \frac{1}{2} y^T H y + h_1^T y + h_2$$

$$\text{s.t.} \quad By + s = b - Fx$$

$$s \ge 0$$

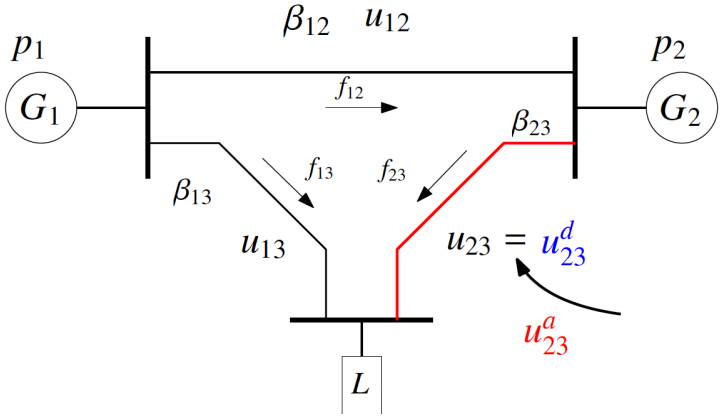
$$\max_{x,\, y^\star,\, s^\star} g^T y^\star$$

$$\text{s.t.} \quad Ax \le e$$

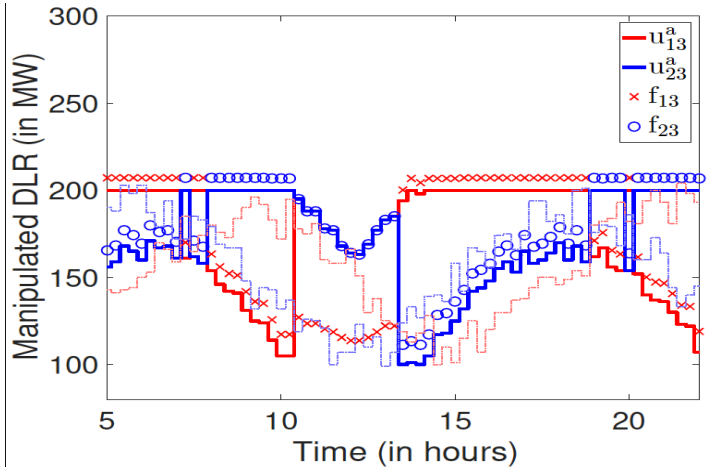
Primal feasibility	$\begin{cases} By^\star + s^\star = b - Fx \\ s^\star \ge 0 \end{cases}$
Dual feasibility	$\lambda^\star \ge 0$
Stationarity	$Hy^\star + h_1 + B^T\lambda^\star = 0$
Complementarity slackness	$\begin{cases} \lambda_i^\star \le \mathrm{M}(1-\mu_i) \\ s_i^\star \le \mathrm{M}\mu_i \\ \mu_i \in \{0,1\} \end{cases}$

M is an upper bound on dual and slack variables

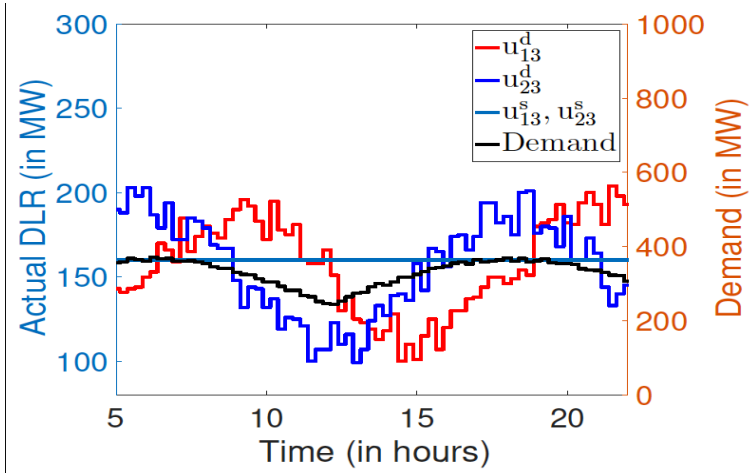
Optimal attack strategy on 3 node network



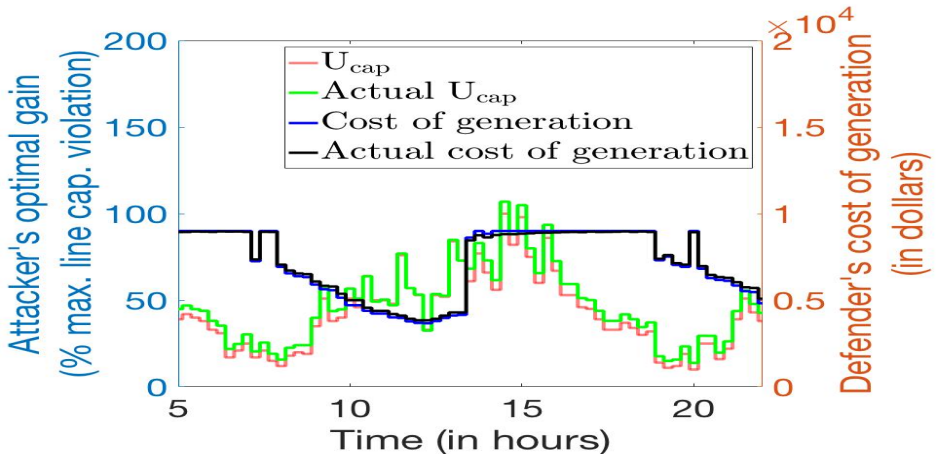
3-bus system



Attacker strategy (largely) exhibits a *bang-bang* policy.

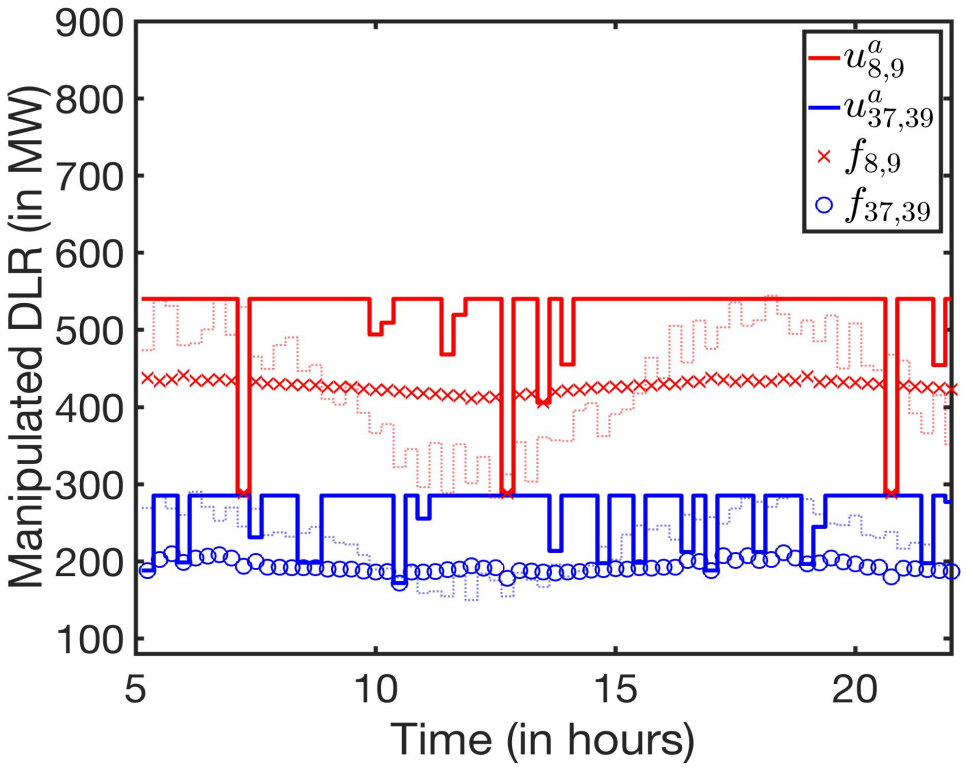


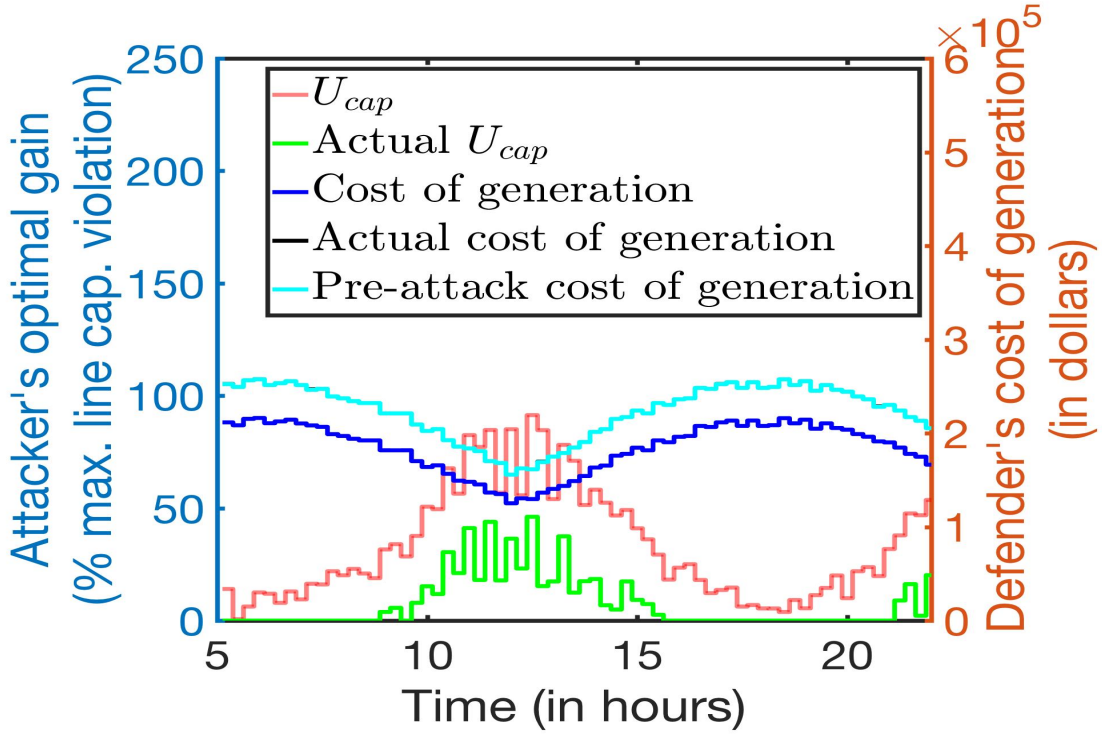
True line capacity ratings and demand over 24 hour horizon



Attacker's gain and operator's cost

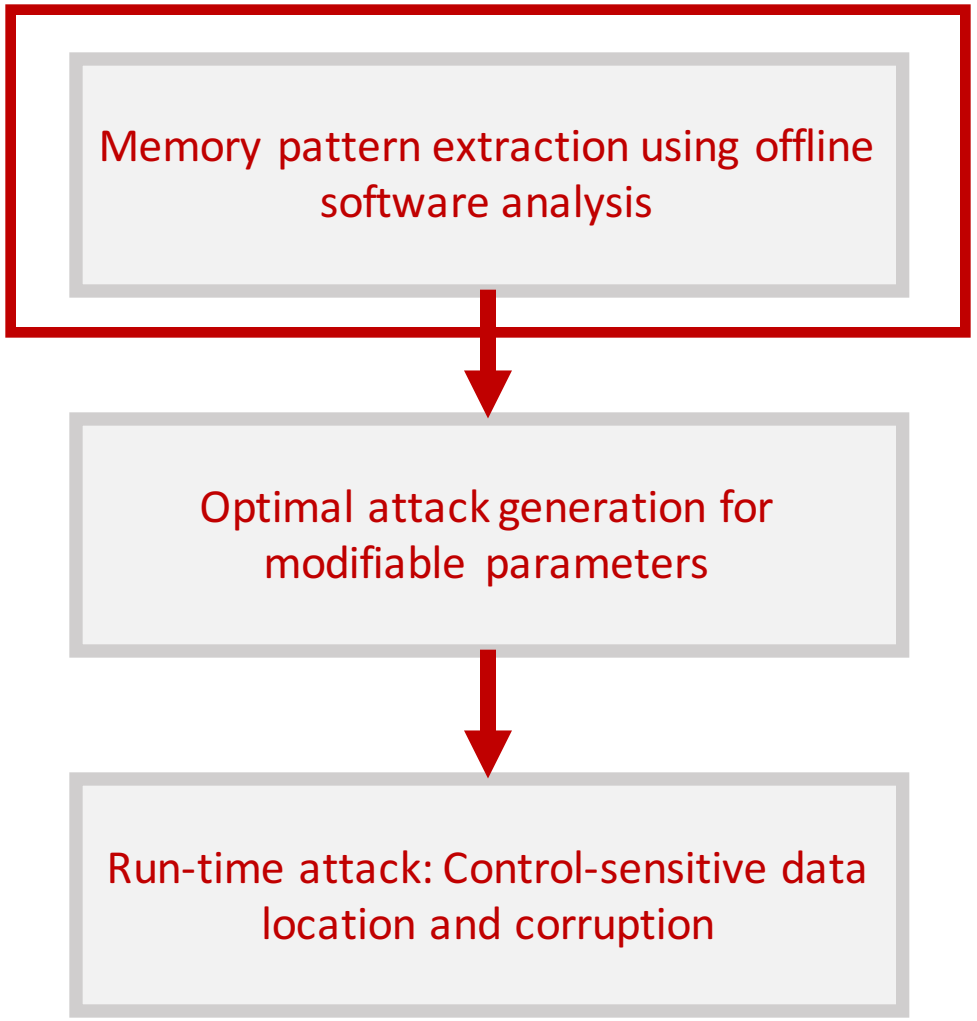
Optimal attack strategy on 118 node network



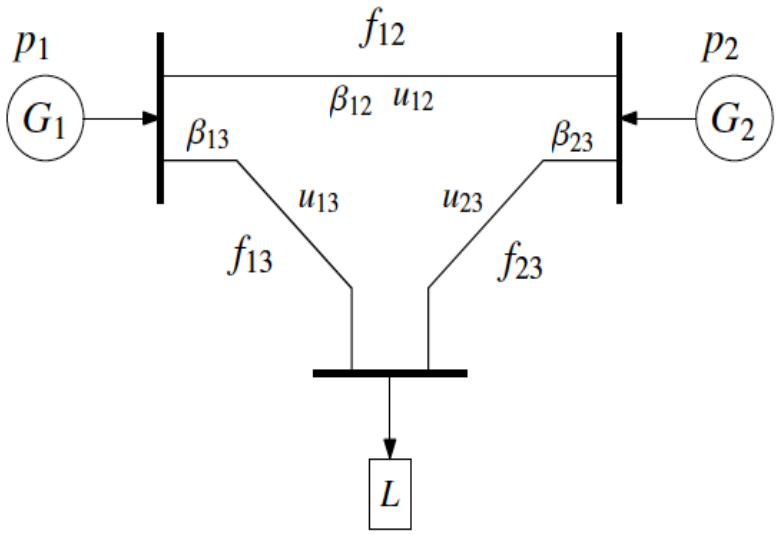


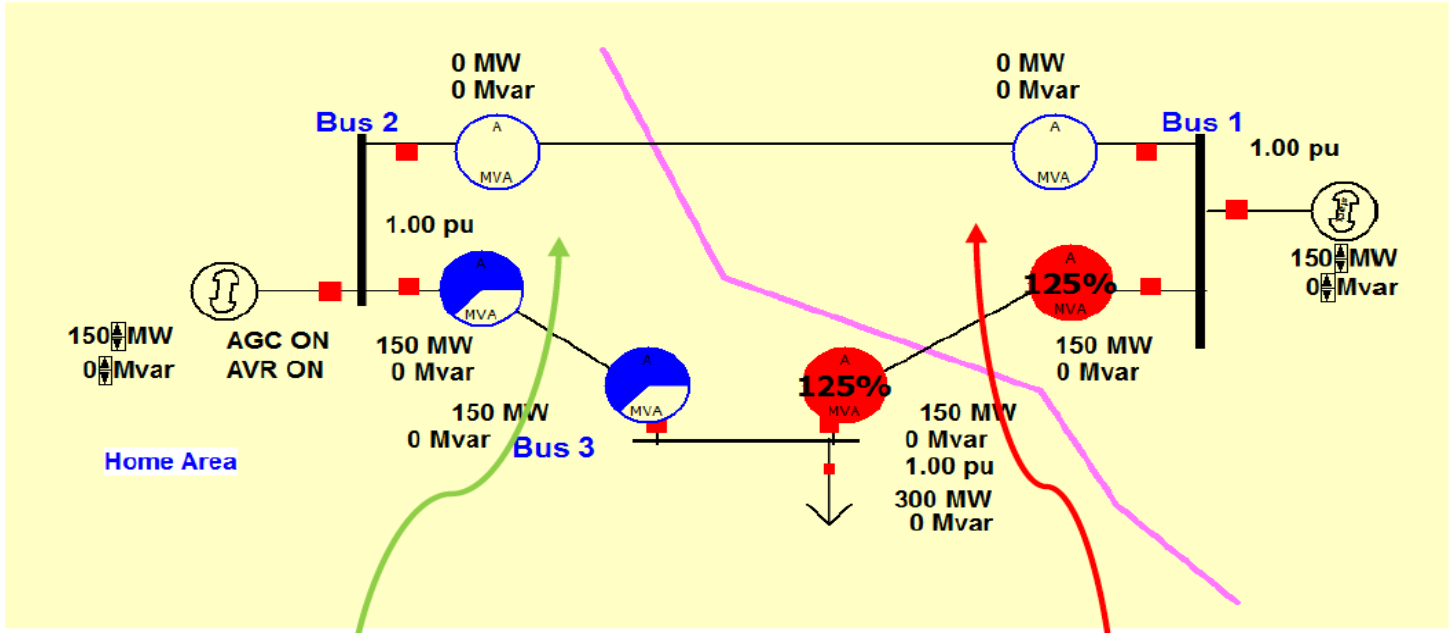
- Bang-bang policy holds for larger network.
- The line capacity violation under AC power flows can be smaller than those of DC power flows
  - Attacker's approximate model may overestimate the impact of the attack

Attacker’s 3-step plan



Semantics-aware memory attack



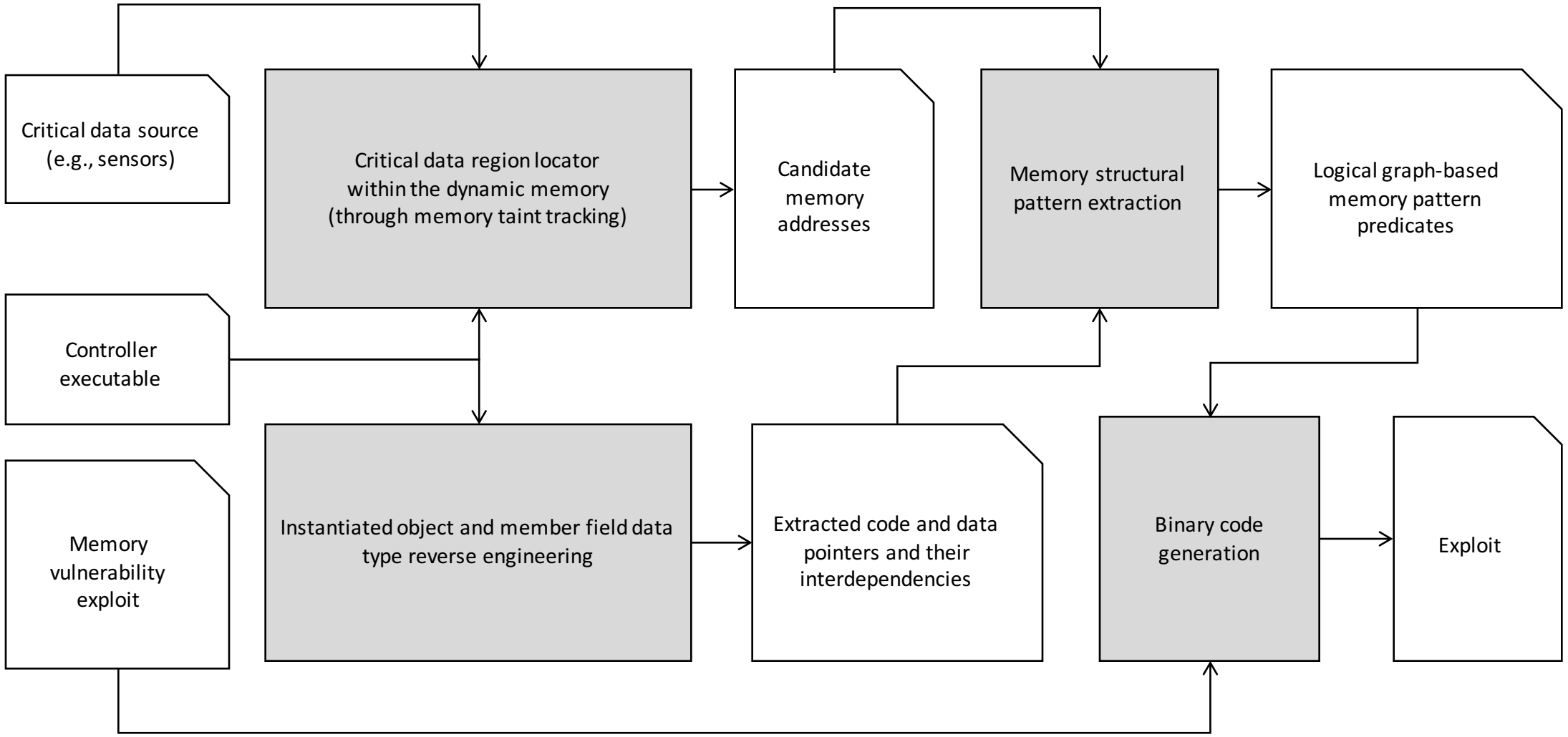


06410AE0 01 00 00 00 C0 65 49 09 00 00 00 00 00 00 00 00
06410AF0 00 00 00 00 00 00 00 00 00 00 00 00 FE 00 00
06410B00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
06410B10 00 00 00 00 9A 99 19 40 E1 FA C7 42 E1 FA C7 42

06410840 01 00 00 00 60 65 49 09 00 00 00 00 00 00 00 00
06410850 00 00 00 00 00 00 00 00 00 00 00 00 FE 00 00
06410860 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
06410870 00 00 00 00 9A 99 99 3F E1 FA C7 42 E1 FA C7 42

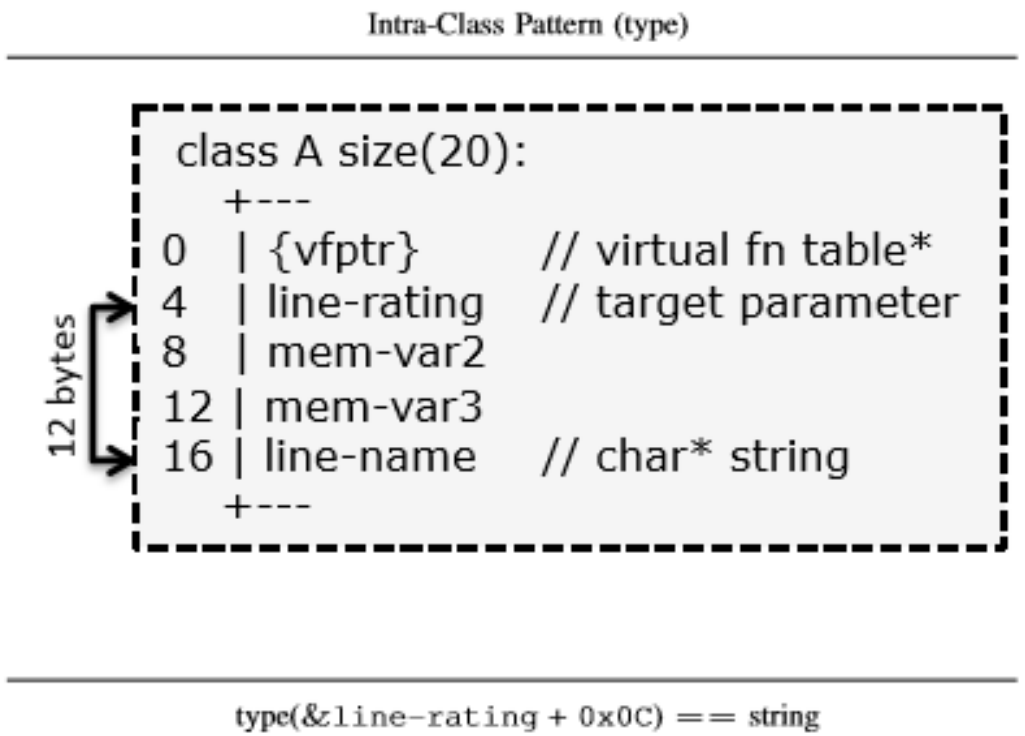
Post-attack power system state

Memory Data Manipulation Attack



Logical memory structural patterns

- Intra-class type patterns
- Code pointer-instruction patterns
- Data pointer-based patterns



- ➢Intra-class
- ➢Fixed offset
- ➢Data types and/or values

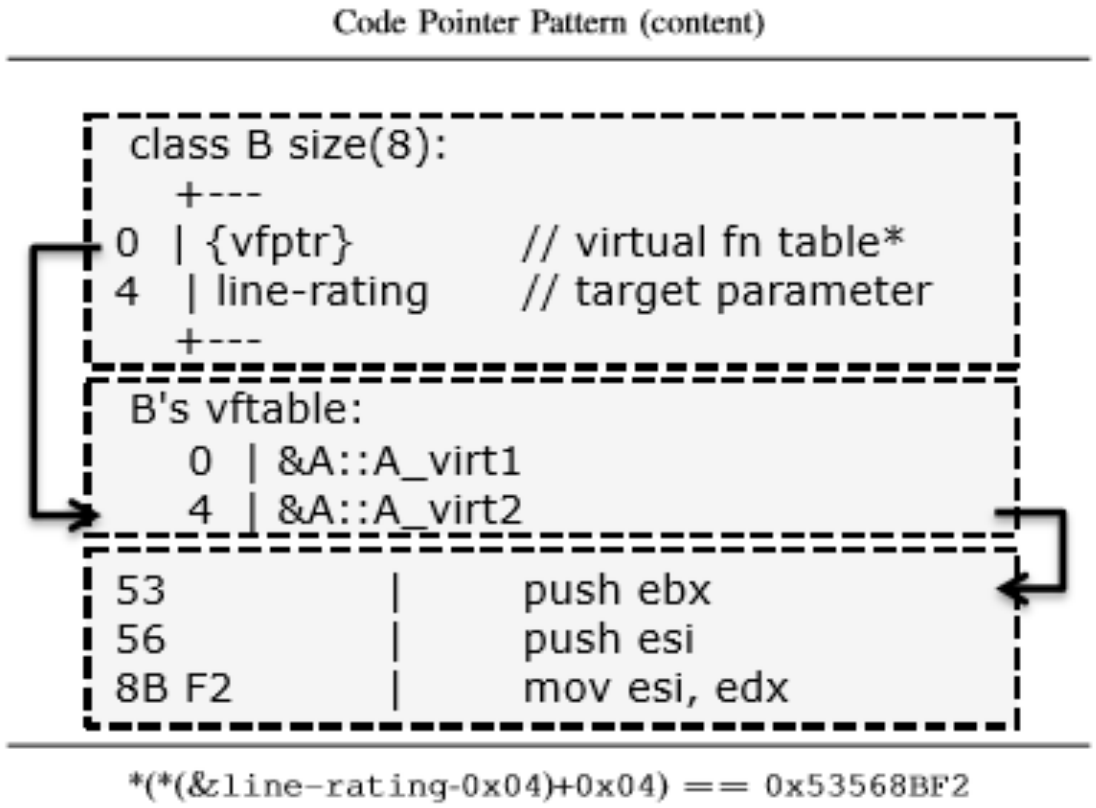
Logical memory structural patterns

- Intra-class type patterns
- Code pointer-instruction patterns
- Data pointer-based patterns

➢Code segments read-only

➢Virtual function table

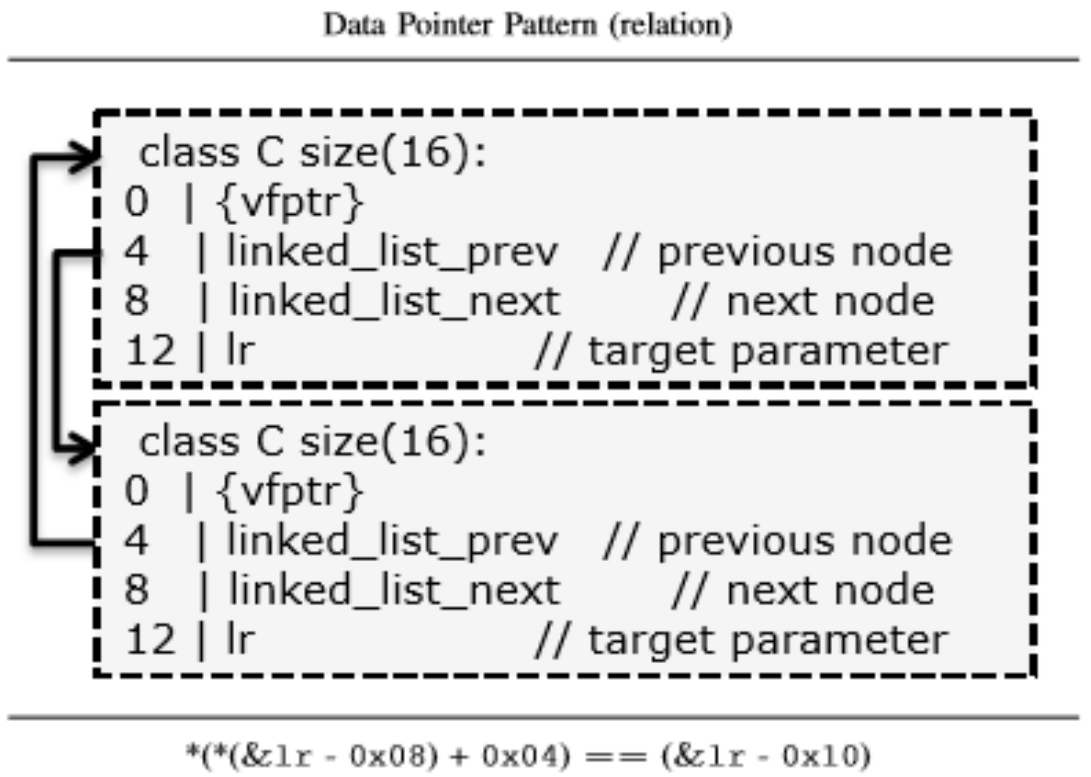
➢Virtual function prologue



Logical memory structural patterns

- Intra-class type patterns
- Code pointer-instruction patterns
- Data pointer-based patterns

  - ➢Inter-object dependencies
  - ➢Recursive pointer traversal
  - ➢Directed graph



ED Software - PowerWorld, NEPLAN, PowerFactory, PowerTools, SmartGridToolbox

Memory Forensics Accuracy

Sample result: PowerWorld memory for 3-bus power system

fbus	tbus	r	x	b	rateA	rateB	rateC	ratio	angle	status	angmin	angmax
1	3	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0
1	2	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0
2	3	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0

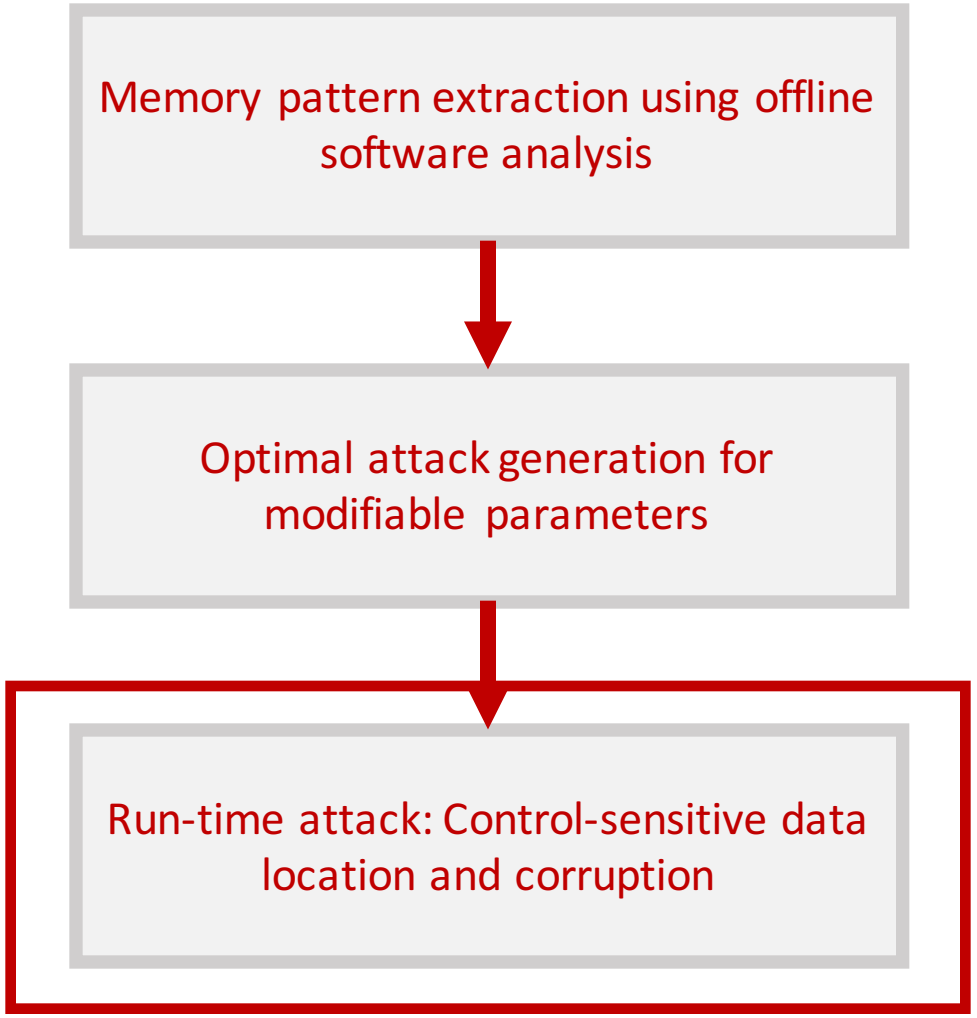
```
016B2AE0 0001 0000 0000 0000 2AC8 016B 0000 0000
016B2AF0 0000 0000 0000 3FF8 0000 0000 0000 0000
016B2B00 0000 0000 0000 3FF0 0000 0000 0000 0000
016B2B10 0000 0000 0000 0000 999A 9999 9999 3FA9
016B2B20 0000 0000 0000 0000 FFFF FFFF FFFF C033
016B2B30 0000 0000 0000 3FF0 0000 0000 0000 0000
```

```
016C0500 0003 0000 0000 0000 95B8 016B 0000 0000
016C0510 0000 0000 0000 3FF8 0000 0000 0000 0000
016C0520 0000 0000 0000 3FF0 0000 0000 0000 0000
016C0530 0000 0000 0000 0000 999A 9999 9999 3FA9
016C0540 0000 0000 0000 0000 FFFF FFFF FFFF C033
016C0550 0000 0000 0000 3FF0 0000 0000 0000 0000
```

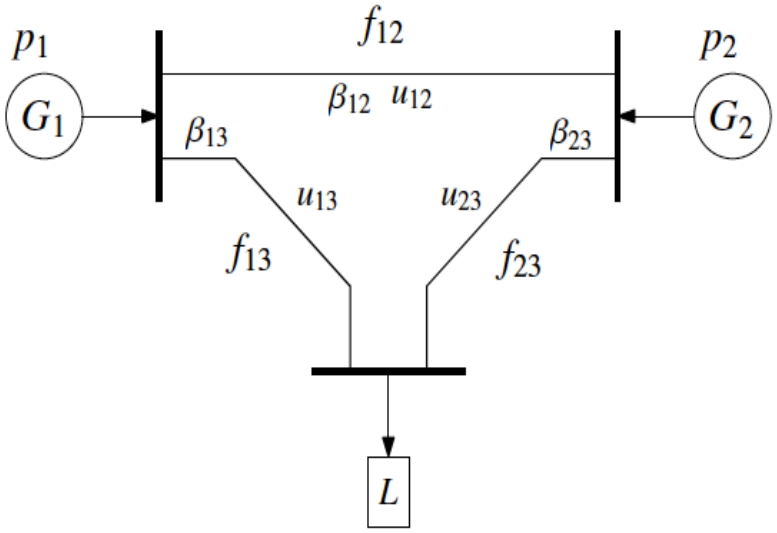
Forensics accuracy for five known EMS software modules

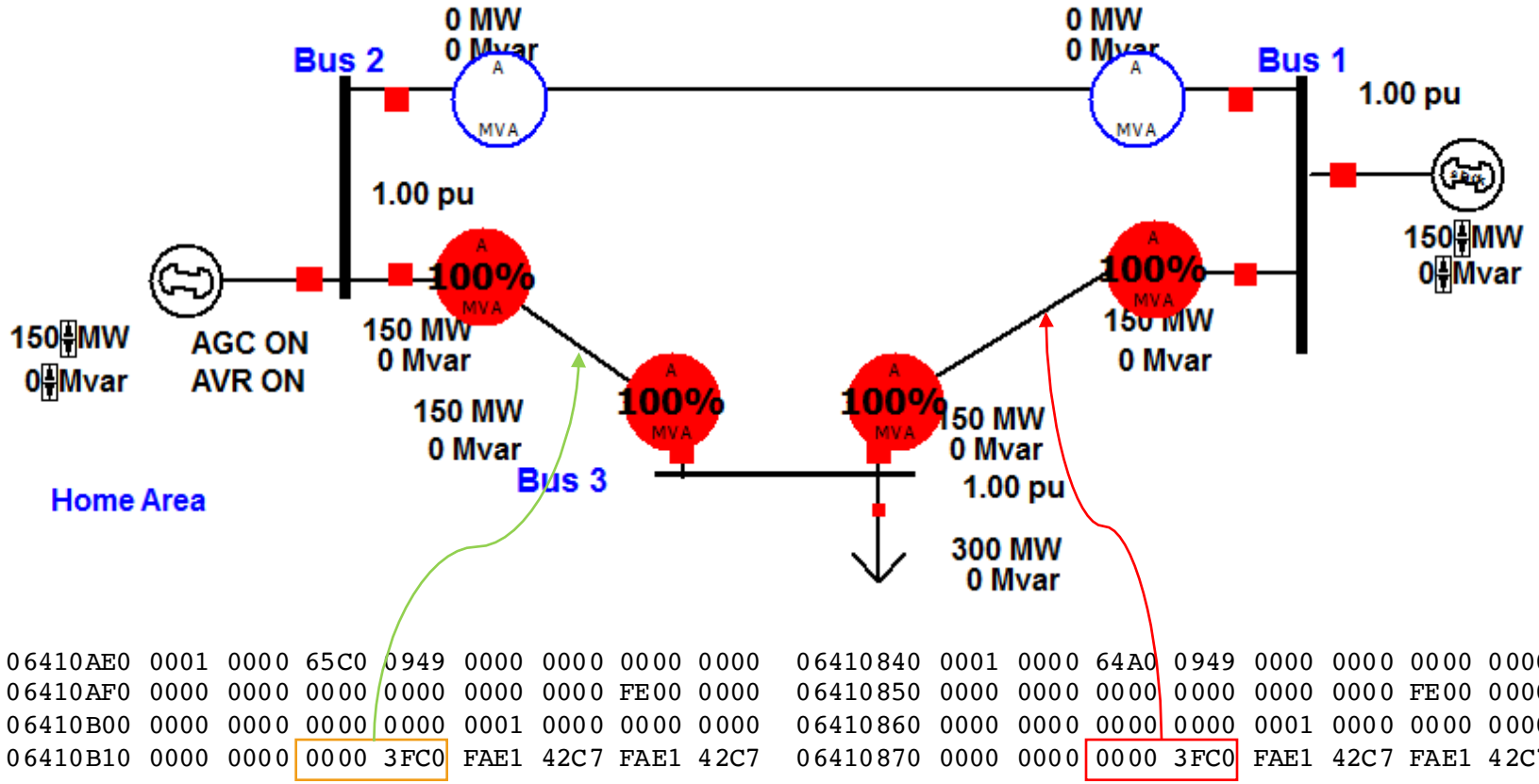
EMS Software	vfTable	Line	Bus	Gen.	Accuracy
PowerWorld	8527	3	3	2	100%
NEPLAN	6549	51	30	5	100%
PowerFactory	110	34	39	10	100%
Powertools	3	185	118	53	100%
SmartGridToolbox	194	79	57	4	100%

Attacker’s 3-step plan

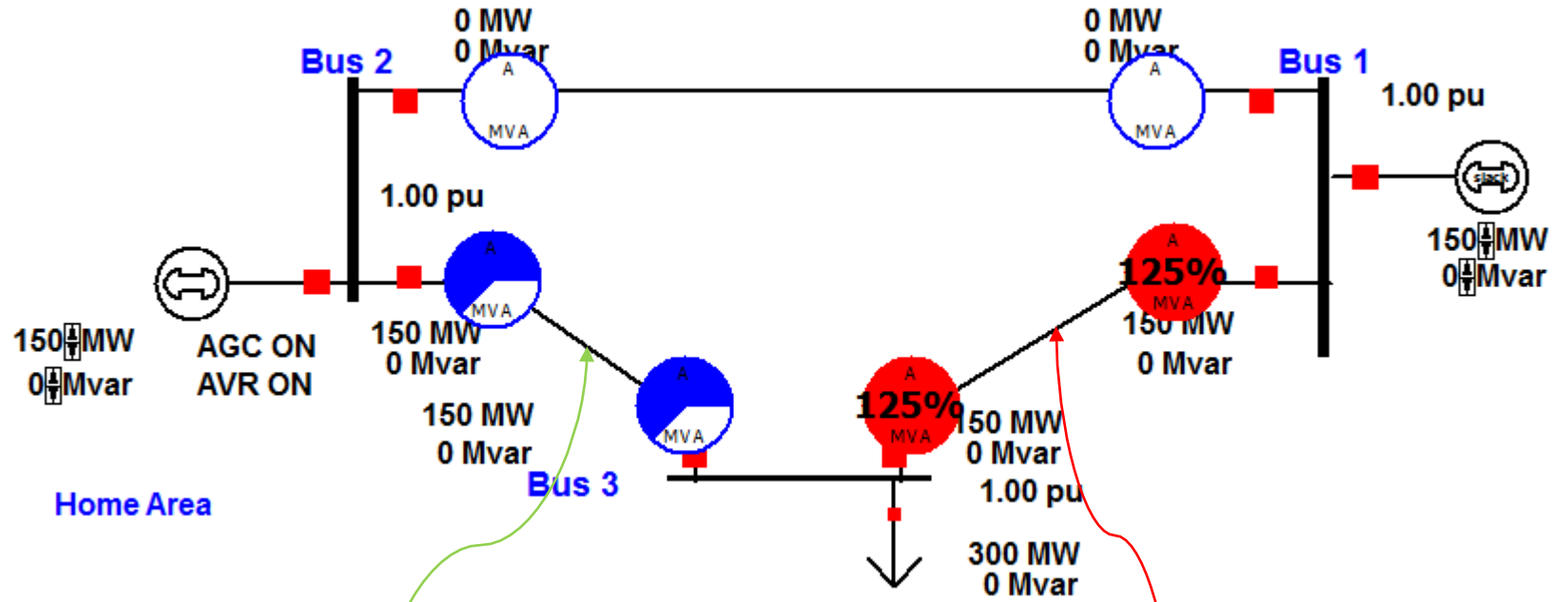


PowerWorld pre-attack system state





PowerWorld post-attack system state



Potential Mitigations

- Protection of sensitive data
  - Fine-grained data isolation (e.g. SGX)
- Control command verification
  - Controller output verification
- Intrusion-tolerant replication
  - Comparing with one replica controller result
- Algorithmic redundancy
  - Attack-aware optimal dispatch
- Memory vulnerability mitigation

Summary

Semantics-aware compromise of power grid controllers

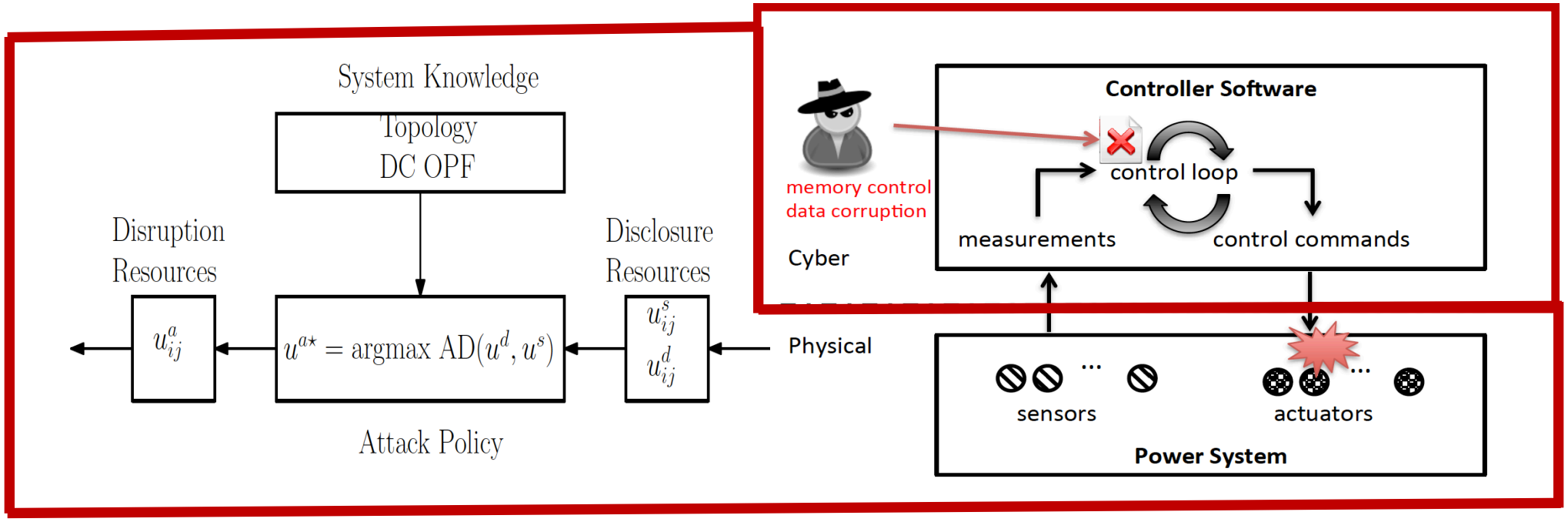
- Optimal attack on control algorithm
- Implementation by means of memory data corruption

Future Work

- Extension to other parameter violations
- Simultaneous line capacity violations of multiple lines
- Automation of critical parameter location and corruption

Thank You!

Cyber-physical security problem



Control systems security viewpoint ? Software systems security viewpoint