TCIPG

Specification-based IDS for the DNP3 Protocol

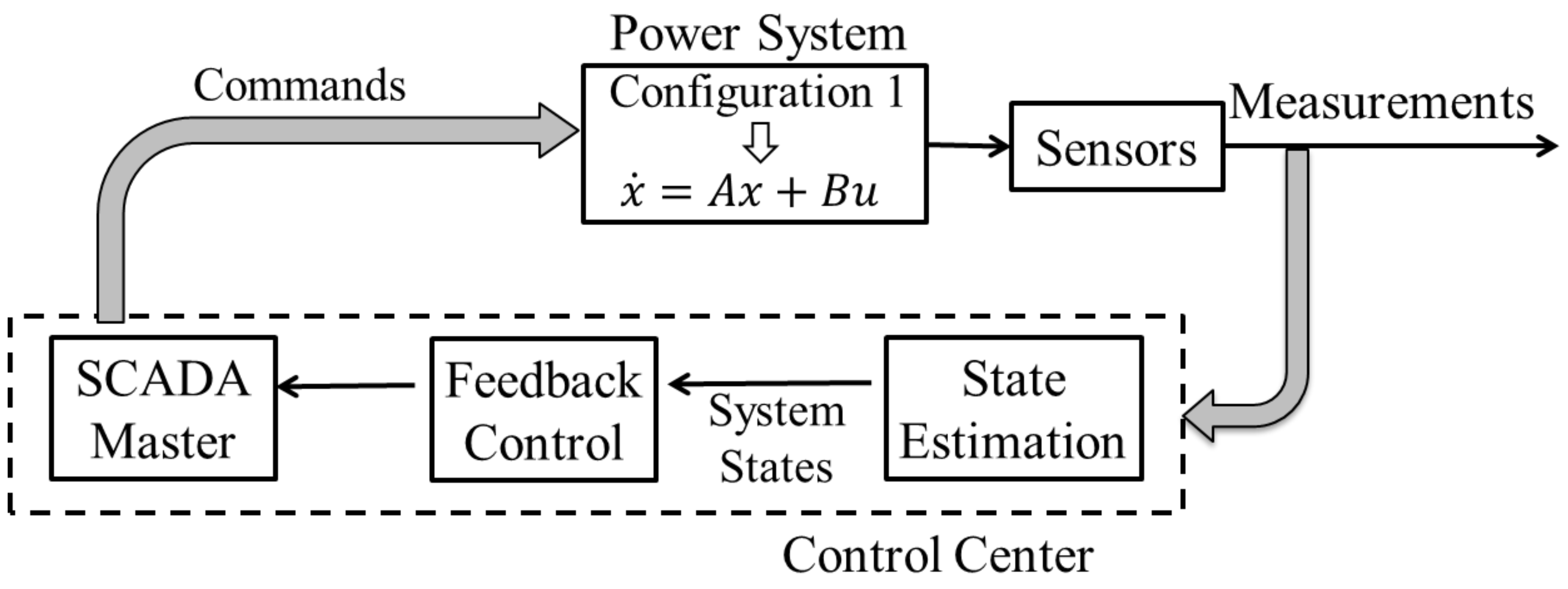
Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, and Ravi K. Iyer

GOALS

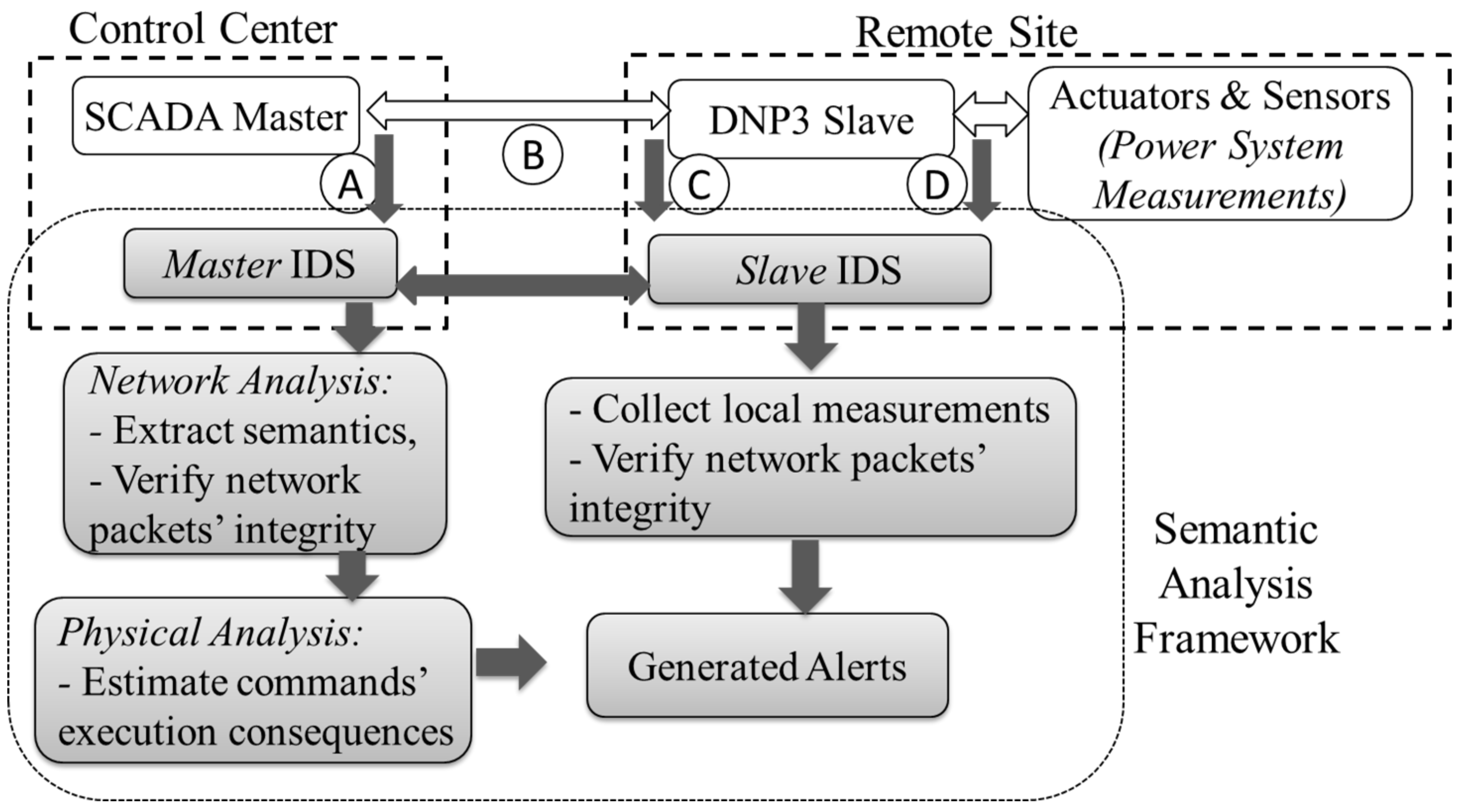
- Overall:
  - Detect control-related attacks that modify a power grid's physical configurations without exhibiting obvious network anomalies.
  - Combine system knowledge of both cyber and physical infrastructure in power grids to estimate the execution consequences of maliciously crafted control commands.
- Specifically:
  - Augment Bro IDS with DNP3 analyzer to monitor control commands and measurement data exchanged between SCADA master and substations.
  - Achieve rapid detections by adapting power flow analysis algorithm based on the observed control commands.

FUNDAMENTAL QUESTIONS/CHALLENGES

- A sophisticated attacker can exploit system vulnerabilities and use seemingly legitimate commands to cause a wide range of system changes.
- The attack modifies the power system's open loop configurations.
  - System's steady states can be significantly changed.
  - System operator can lose control over some system states.
  - Measurements related to some states can become unobservable.


Power System
Configuration 1
⇩
$\dot{x} = Ax + Bu$
Commands
Sensors
Measurements
SCADA Master
Feedback Control
System States
State Estimation
Control Center

RESEARCH PLAN


Control Center
Remote Site
SCADA Master
DNP3 Slave
Actuators & Sensors
(Power System Measurements)
A
B
C
D
Master IDS
Slave IDS
Network Analysis:
- Extract semantics,
- Verify network packets' integrity
- Collect local measurements
- Verify network packets' integrity
Physical Analysis:
- Estimate commands' execution consequences
Generated Alerts
Semantic Analysis Framework

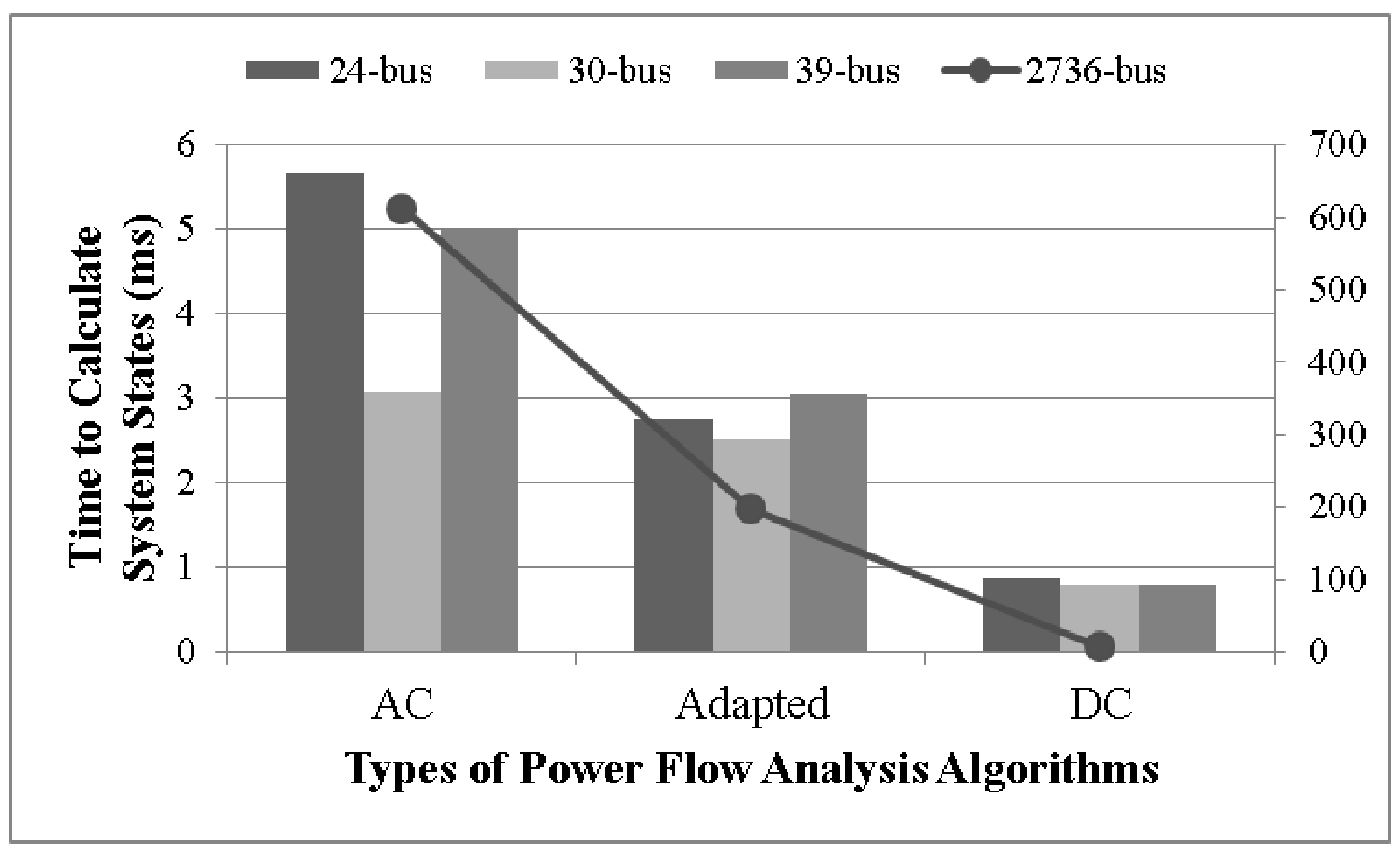
- Master IDS at the control center:
  - Distinguish critical commands from noncritical ones.
  - Collect measurements from multiple substations.
  - Include state estimation & contingency analysis components to estimate consequences of executing a given command.
- Slave IDS at the remote site.
  - Use local IDS to obtain trusted measurements directly from sensors.
    - Assume that concurrent physical tampering with a large number of distributed sensors is not practical for the attacker.
  - Validate absence of corrupted measurements at other locations.
- Adapt the parameters of the iterative algorithm, e.g., Newton-Raphson algorithm, used in power flow analysis.
  - As an *initial* solution, when a malicious command is issued, use the most recent known system state.
  - The *convergence threshold* is set such that the estimated system state is accurate.
  - Change the *number of iterations* to calculate system states for different control commands.

RESEARCH RESULTS

- Compare the detection accuracies of the adapted algorithm ("*Adapted*") and the DC power flow analysis ("*DC*").
  - False negative (FN) rate is around 0.01%; false positive rate is 0.78% at most.

		24-bus	30-bus	39-bus	2736-bus
Adapted	*FP*	4.9×10^{-6}	7.8×10^{-3}	0	0
	FN	1.2×10^{-4}	1.3×10^{-4}	1.2×10^{-4}	4.8×10^{-6}
DC	*FP*	0.076	0.026	0.067	0.053
	FN	0.013	0.20	0.003	0.019

- Compare the execution time by using three different algorithms: the classical AC power flow analysis ("*AC*"), the adapted algorithm ("*Adapted*"), and the DC power flow analysis ("*DC*").
  - With the help of the adapted algorithm, the detection latency is reduced as much as 60%.



BROADER IMPACT

- The adapted power flow analysis algorithm significantly reduces the detection latency.
  - The semantic analysis does not inject network traffic or modify normal operation of the power grid.
  - The semantic analysis can be extended to support appropriate remediation mechanisms to prevent physical damage from the attack.
  - The method and implementation of semantic analysis can be extended to other industrial control environments.
- The implemented network IDS can be equipped with other scenario-specific policies in different operational contexts.

INTERACTION WITH OTHER PROJECTS

- Collaborate with International Computer Science Institute (ICSI) and the University of Illinois' National Center for Supercomputing Applications (NCSA).
  - The extension made on Bro to support the DNP3 protocol is included in Bro's current source code release (version 2.2).
  - New NSF award is being used to support further work.
- Collaborate with Ameren Technology Application Center (TAC).
  - Use Bro's DNP3 analyzer to analyze traffic data collected from real substations.
  - Develop appropriate security policies to deploy in the utility.

FUTURE EFFORTS

- Study possible response mechanisms to attacks.
  - Exploit protection mechanisms for transient faults (e.g., the reclosing logic) deployed in intelligent relays as intrusion response mechanisms.
- Exploit control-theoretic approach to quantitatively study the impact of control-related attacks.

SELECTED PUBLICATIONS

1. Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter Sauer, and Ravishankar Iyer. "Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids." In *Proceedings of Smart Energy Grid Security Workshop, SEGS 2013.*
2. Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol." In *Proceedings of 8th Annual Cyber Security and Information Intelligence Research Workshop, CSIIRW 2012*. Top Three Paper Award.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T