TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

SPECIFICATION-BASED IDS FOR THE DNP3 PROTOCOL

NOVEMBER, 12TH, 2014

HUI LIN

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

PROBLEM DEFINITION

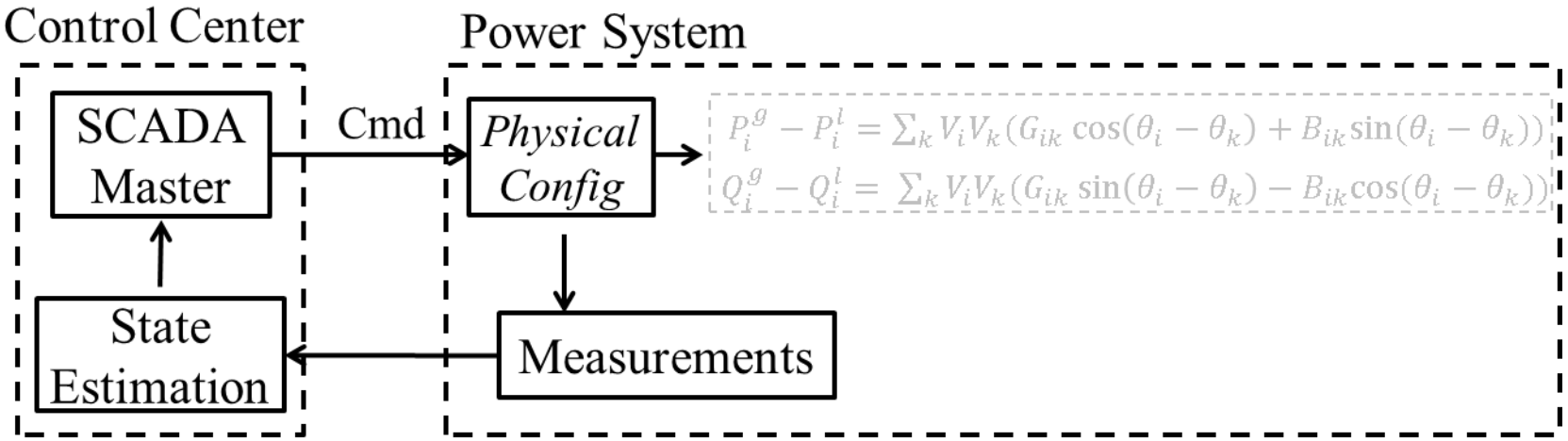
- ***Threat model*:** *control commands*, if maliciously crafted, can directly change system's physical state

PROBLEM DEFINITION

- ***Threat model*:** *control commands*, if maliciously crafted, can directly change system's physical state
- ***Control-related attack*:** a sophisticated attacker can exploit system vulnerabilities and use a few maliciously crafted commands to put the system into insecure electrical states

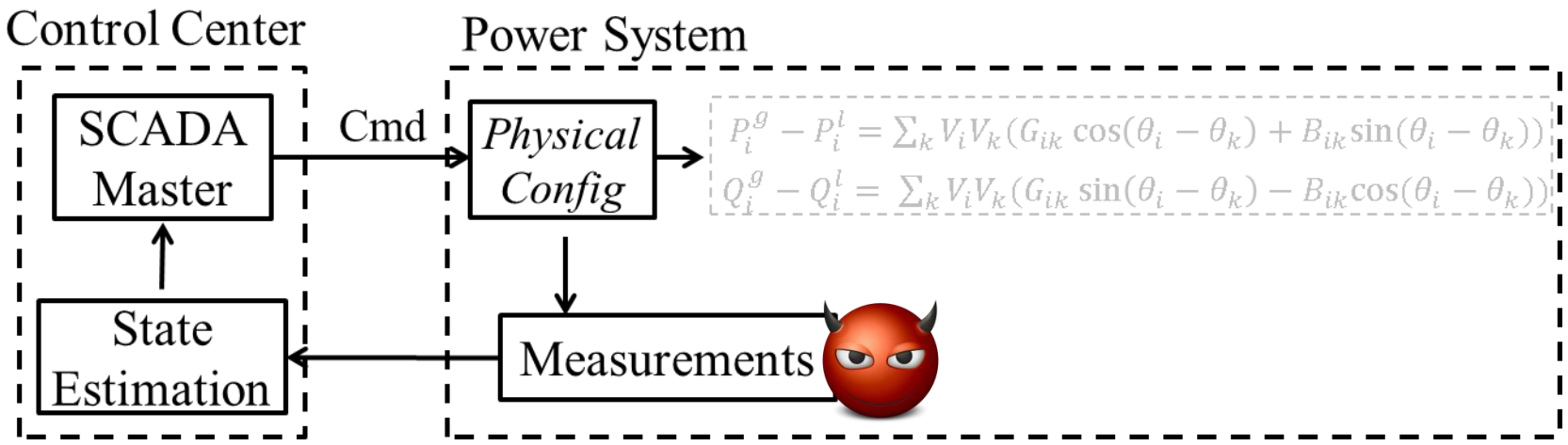
PROBLEM DEFINITION

- ***Threat model***: *control commands*, if maliciously crafted, can directly change system's physical state
- ***Control-related attacks***: a sophisticated attacker can exploit system vulnerabilities and use a few maliciously crafted commands to put the system into insecure electrical states



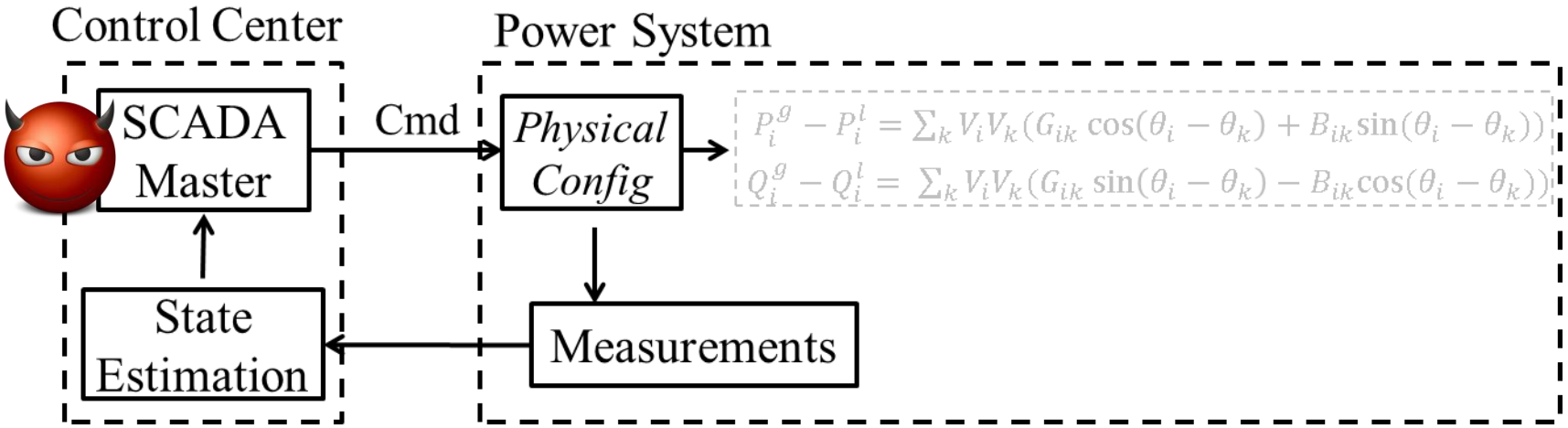
PROBLEM DEFINITION

- ***Threat model***: *control commands*, if maliciously crafted, can directly change system's physical state
- ***Control-related attacks***: a sophisticated attacker can exploit system vulnerabilities and use a few maliciously crafted commands to put the system into insecure electrical states



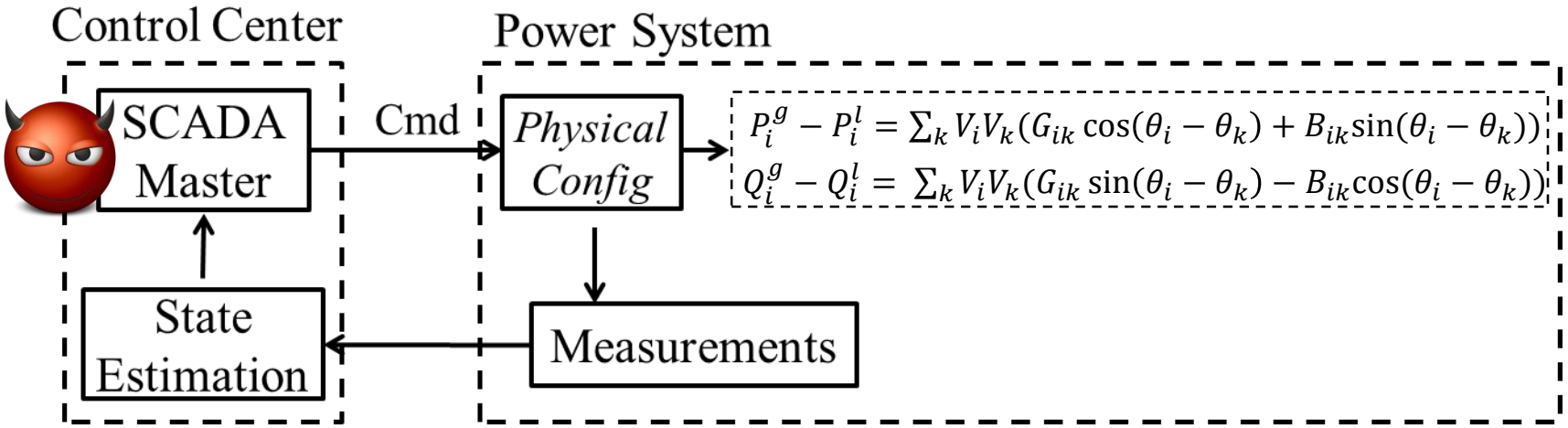
PROBLEM DEFINITION

- ***Threat model***: *control commands*, if maliciously crafted, can directly change system's physical state
- ***Control-related attacks***: a sophisticated attacker can exploit system vulnerabilities and use a few maliciously crafted commands to put the system into insecure electrical states



PROBLEM DEFINITION

- ***Threat model***: *control commands*, if maliciously crafted, can directly change system's physical state
- ***Control-related attacks***: a sophisticated attacker can exploit system vulnerabilities and use a few maliciously crafted commands to put the system into insecure electrical states



WHY DETECTION IS A CHALLENGE?

- Hard to detect based solely on power systems' electrical states
  - Traditional contingency analysis considers low-order incidents, i.e., the "*N-1*" contingency
  - Traditional state estimation is performed periodically, detecting attacks after physical damage
  - Measurements may be compromised

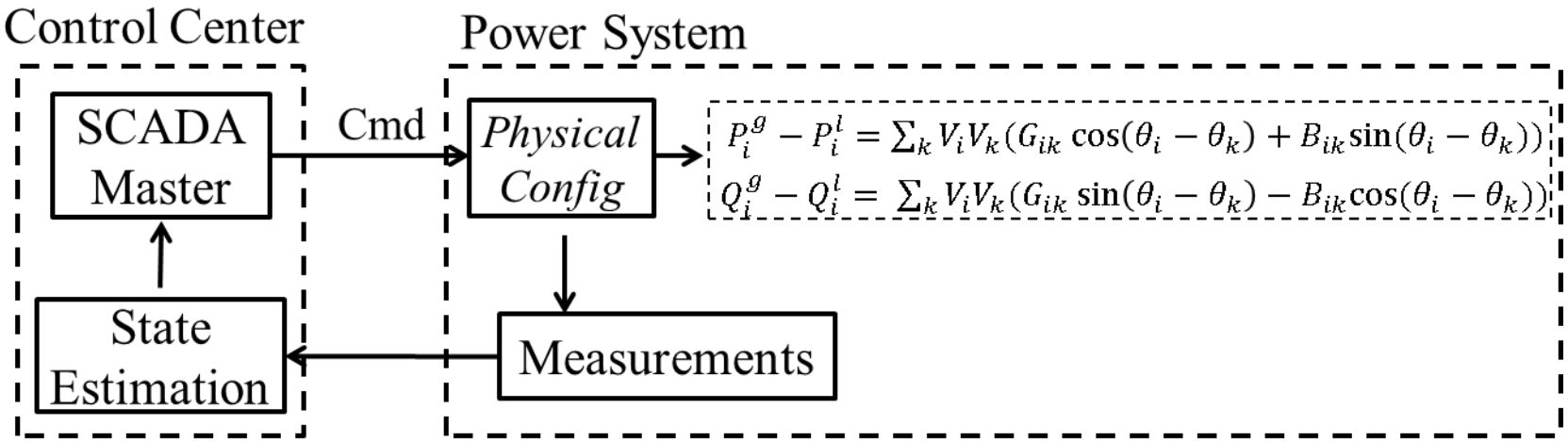
WHY DETECTION IS A CHALLENGE?

- Hard to detect based solely on power systems' electrical states
  - Traditional contingency analysis considers low-order incidents, i.e., the "*N-1*" contingency
  - Traditional state estimation is performed periodically, detecting attacks after physical damage
  - Measurements may be compromised
- Hard to detect based solely on the network intrusion detection systems
  - Commands can be encoded in correct syntax
  - Not detectable by traditional network intrusion detection systems (IDS)

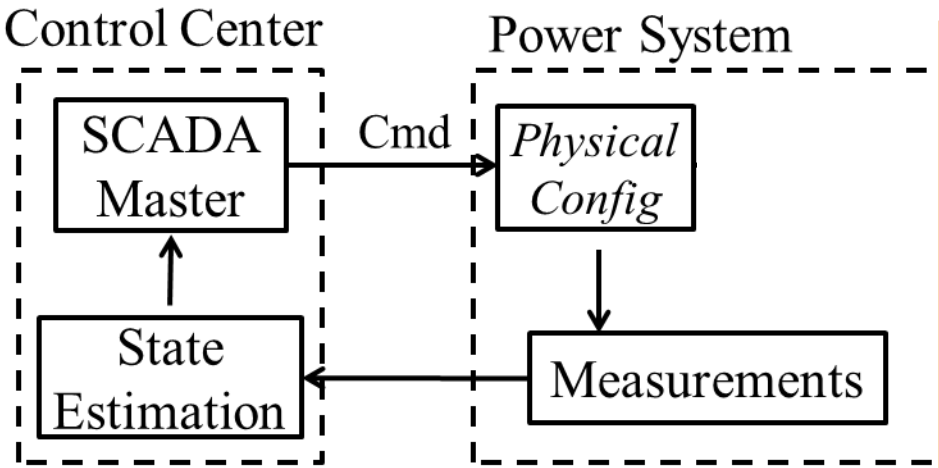
DETECTION DESIGN

- Combine system knowledge of both cyber and physical infrastructure in the power grid
  - Integrate network monitoring with look-ahead power flow analysis
- Detect malicious commands at their *first appearances*, instead of identifying power system's physical damage after the fact

APPROACH

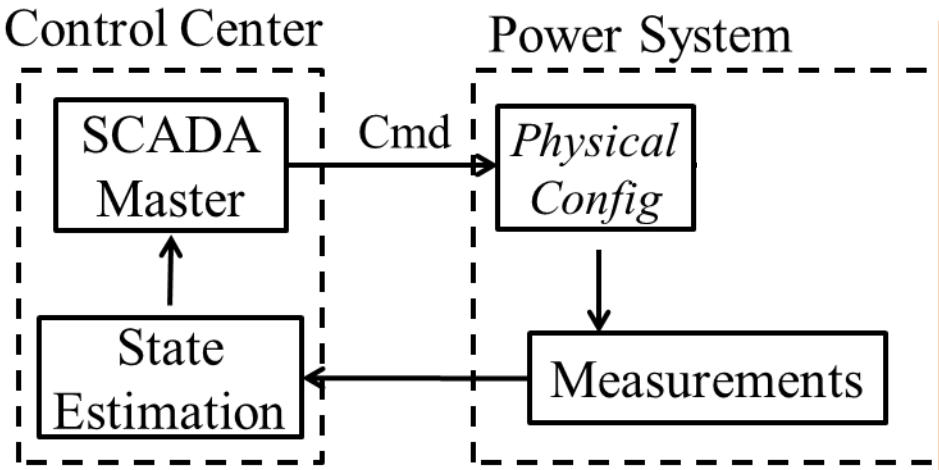

Control Center
Power System
SCADA Master
Cmd
Physical Config
$P_i^g - P_i^l = \sum_k V_i V_k (G_{ik} \cos(\theta_i - \theta_k) + B_{ik} \sin(\theta_i - \theta_k))$
$Q_i^g - Q_i^l = \sum_k V_i V_k (G_{ik} \sin(\theta_i - \theta_k) - B_{ik} \cos(\theta_i - \theta_k))$
State Estimation
Measurements

APPROACH



Cyber Infrastructure

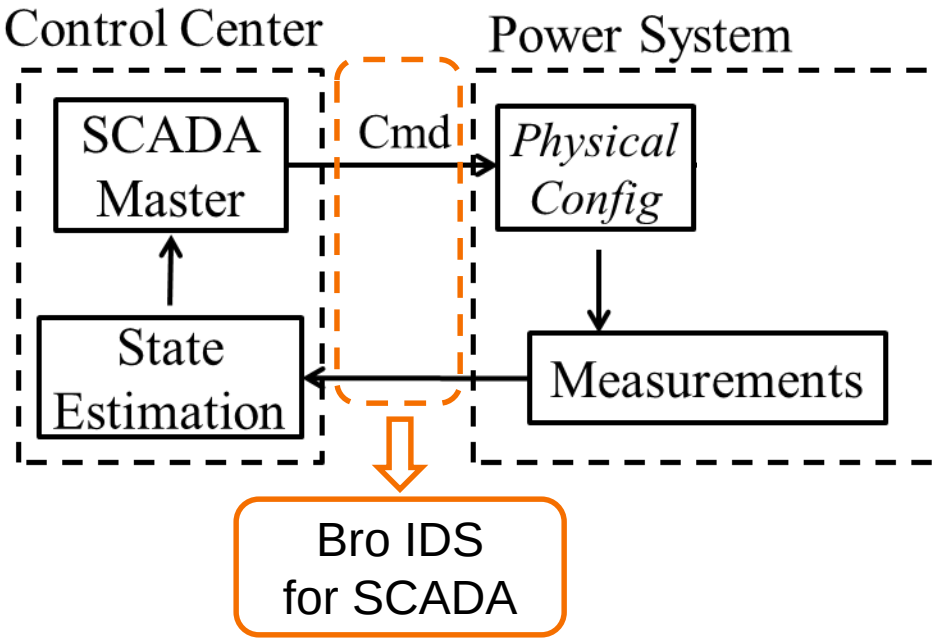
APPROACH



Cyber Infrastructure

- Adapt specification-based IDS for SCADA systems
  - Detect unexpected network activities based on predefined security specifications

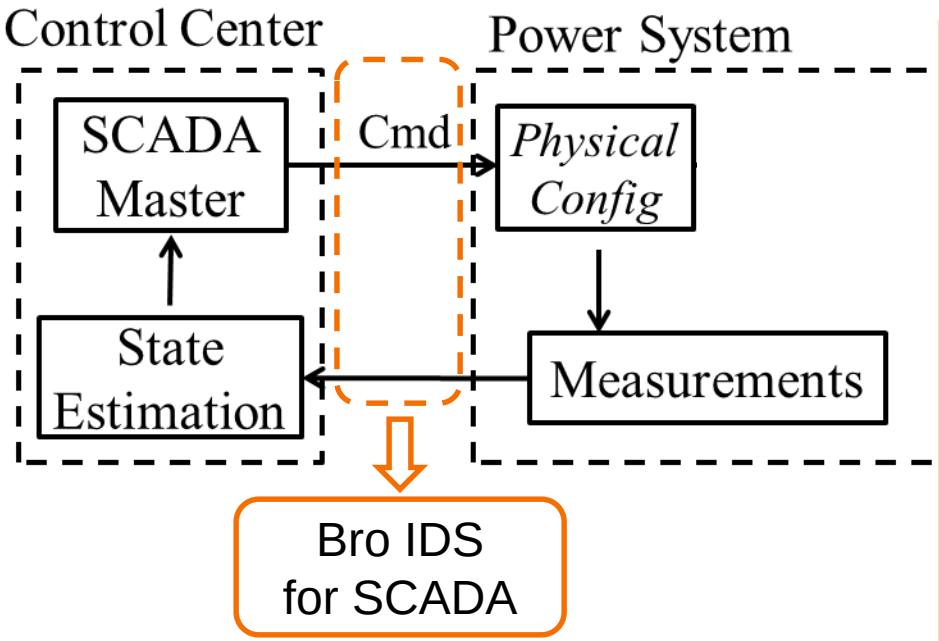
APPROACH



Cyber Infrastructure

- Adapt specification-based IDS for SCADA systems
  - Detect unexpected network activities based on predefined security specifications
- Adapt Bro to support SCADA protocols
  - Develop DNP3 & Modbus analyzers in Bro's distribution
  - Collaborate with industry, i.e., Ameren, Abbot Lab
    - Use real network traffic from substations in Ameren to test the developed tools

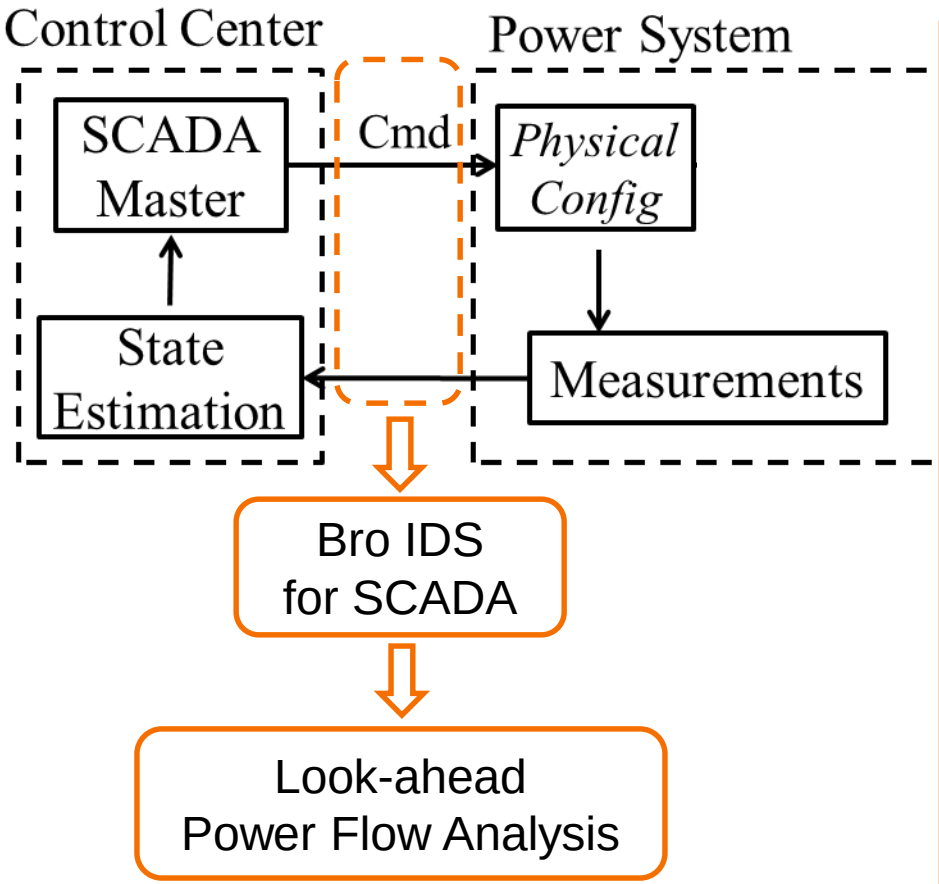
APPROACH



Physical Infrastructure

- Develop semantic analysis framework
  - Augment network IDS with power flow analysis

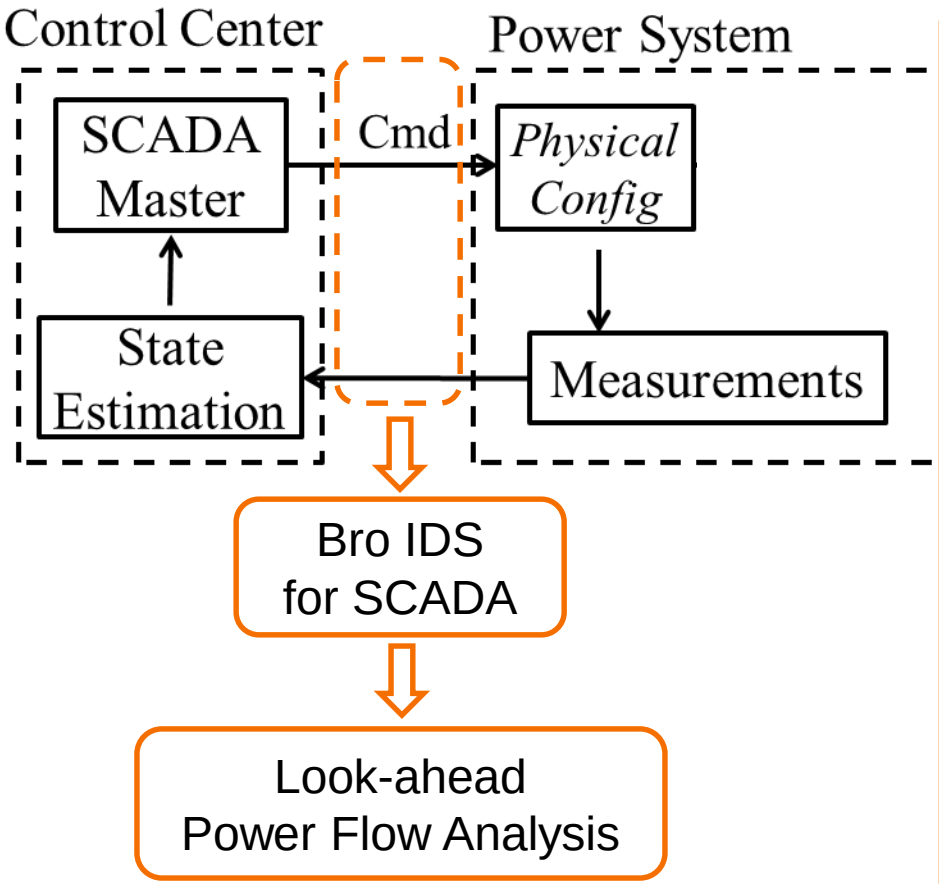
APPROACH



Physical Infrastructure

- Develop semantic analysis framework
  - Augment network IDS with power flow analysis
  - Monitor network payloads to identify control commands
  - Invoke look-ahead power flow analysis to evaluate the physical consequence of a command's execution

APPROACH



Physical Infrastructure

- Develop semantic analysis framework
  - Augment network IDS with power flow analysis
  - Monitor network payloads to identify control commands
  - Invoke look-ahead power flow analysis to evaluate the physical consequence of a command's execution
  - Monitor sensor measurements to identify corruptions

LOW LATENCY DETECTION

- Classical AC power flow analysis calculates accurate system states with long latency

LOW LATENCY DETECTION

- Classical AC power flow analysis calculates accurate system states with long latency
- DC power flow analysis introduces very little latency, but calculates very inaccurate system states

LOW LATENCY DETECTION

- Classical AC power flow analysis calculates accurate system states with long latency
- DC power flow analysis introduces very little latency, but calculates very inaccurate system states
- Adapt AC power flow analysis to balance detection latency and accuracy
  - Allow timely responses before system-wide propagation of malicious damage

LOW LATENCY DETECTION

- Classical AC power flow analysis calculates accurate system states with long latency
- DC power flow analysis introduces very little latency, but calculates very inaccurate system states
- Adapt AC power flow analysis to balance detection latency and accuracy
  - Allow timely responses before system-wide propagation of malicious damage
- Adapt Newton-Raphson algorithm
  - Intelligently reduce the *number of iteration* for different control commands
    - Meet the trade-off between detection accuracy and latency

EVALUATION: DETECTION ACCURACY

- The test-bed configuration
  - Use the case files of IEEE 24-bus, 30-bus, 39-bus, and a 2736-bus system in *Matpower* to evaluate the adapted power flow analysis algorithm
  - Malicious changes: line outage, generation and load modification

EVALUATION: DETECTION ACCURACY

- The test-bed configuration
  - Use the case files of IEEE 24-bus, 30-bus, 39-bus, and a 2736-bus system in *Matpower* to evaluate the adapted power flow analysis algorithm
  - Malicious changes: line outage, generation and load modification
- Compare the detection accuracy in terms of false positive (*FP)* and false negative (*FN*) detection
  - Adapted algorithm ("*Adapted*") and DC power flow analysis ("*DC*")

		24-bus	30-bus	39-bus	2736-bus
Adapted	FP	0.0005%	0.78%	0	0
	FN	0.01%	0.01%	0.01%	0.0005%
DC	FP	7.6%	2.6%	6.7%	5.3%
	FN	1.3%	20%	0.3%	1.9%

EVALUATION: DETECTION ACCURACY

- The test-bed configuration
  - Use the case files of IEEE 24-bus, 30-bus, 39-bus, and a 2736-bus system in *Matpower* to evaluate the adapted power flow analysis algorithm
  - Malicious changes: line outage, generation and load modification
- Compare the detection accuracy in terms of false positive (*FP)* and false negative (*FN*) detection
  - Adapted algorithm ("*Adapted*") and DC power flow analysis ("*DC*")

		24-bus	30-bus	39-bus	2736-bus
Adapted	FP	0.0005%	0.78%	0	0
	FN	0.01%	0.01%	0.01%	0.0005%
DC	FP	7.6%	2.6%	6.7%	5.3%
	FN	1.3%	20%	0.3%	1.9%

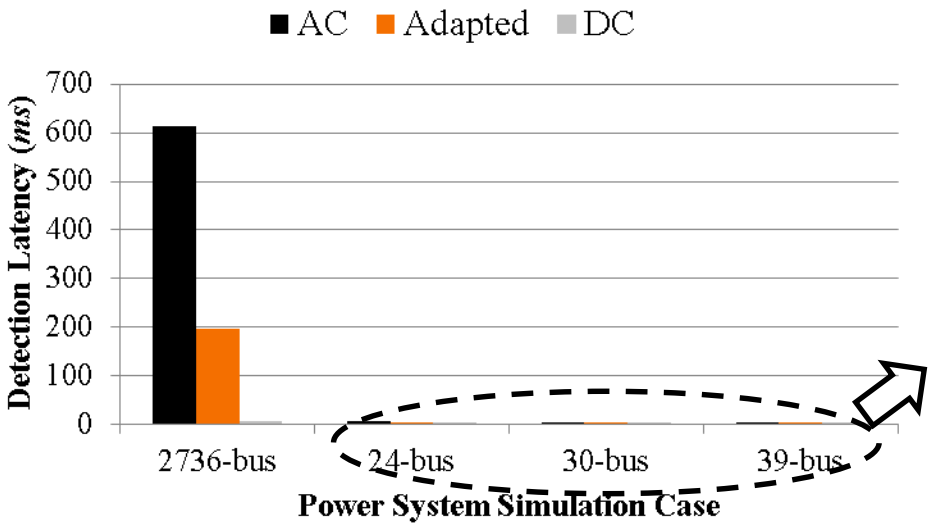
EVALUATION: DETECTION ACCURACY

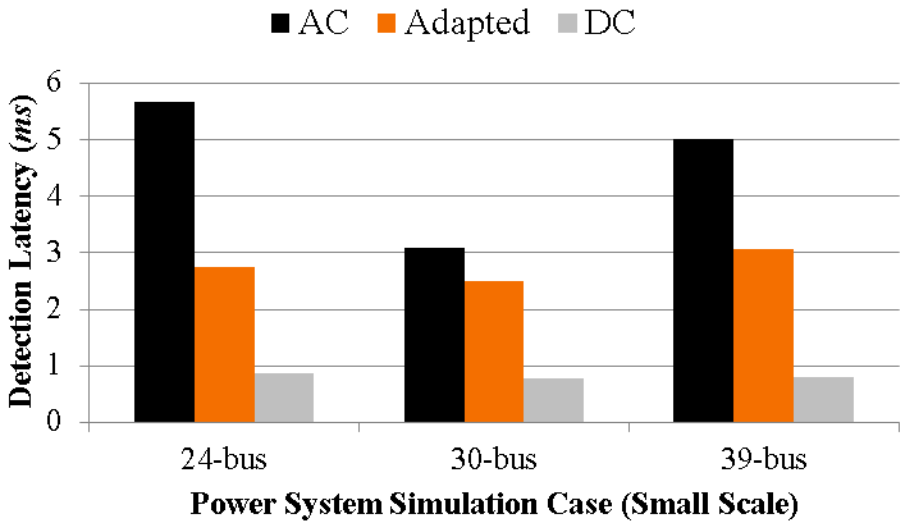
- The test-bed configuration
  - Use the case files of IEEE 24-bus, 30-bus, 39-bus, and a 2736-bus system in *Matpower* to evaluate the adapted power flow analysis algorithm
  - Malicious changes: line outage, generation and load modification
- Compare the detection accuracy in terms of false positive (*FP)* and false negative (*FN*) detection
  - Adapted algorithm ("*Adapted*") and DC power flow analysis ("*DC*")

		24-bus	30-bus	39-bus	2736-bus
Adapted	FP	0.0005%	0.78%	0	0
	FN	0.01%	0.01%	0.01%	0.0005%
DC	FP	7.6%	2.6%	6.7%	5.3%
	FN	1.3%	20%	0.3%	1.9%

EVALUATION: DETECTION LATENCY

- Compare detection latency
  - Classical AC power flow analysis ("*AC*"), the adapted algorithm ("*Adapted*"), and the DC power flow analysis ("*DC*")
  - Reduce the detection latency by up to 60% as compared with AC power flow analysis





CONCLUSION

- Combine system knowledge of both cyber and physical infrastructure in power grid to detect control-related attacks

CONCLUSION

- Combine system knowledge of both cyber and physical infrastructure in power grid to detect control-related attacks
- Develop network IDS for proprietary protocols used in power grid

CONCLUSION

- Combine system knowledge of both cyber and physical infrastructure in power grid to detect control-related attacks
- Develop network IDS for proprietary protocols used in power grid
- Augment network IDS with semantic analysis to estimate the physical consequence of command's execution

CONCLUSION

- Combine system knowledge of both cyber and physical infrastructure in power grid to detect control-related attacks
- Develop network IDS for proprietary protocols used in power grid
- Augment network IDS with semantic analysis to estimate the physical consequence of command's execution
- Adapt AC power flow analysis algorithm specifically used for the semantic analysis
  - Balance the detection latency and accuracy

THANKS

- The DNP3 and Modbus analyzer are included in Bro's standard distribution (bro.org/download)
- Contacts:
  - Hui Lin: hlin33@illinois.edu
  - Zbigniew Kalbarczyk, kalbarcz@illinois.edu
  - Ravishankar Iyer, rkiyer@illinois.edu
  - Adam Slagell, slagell@illinois.edu
- For further discussion, please stop at our poster "Specification-based IDS for the DNP3 Protocol"