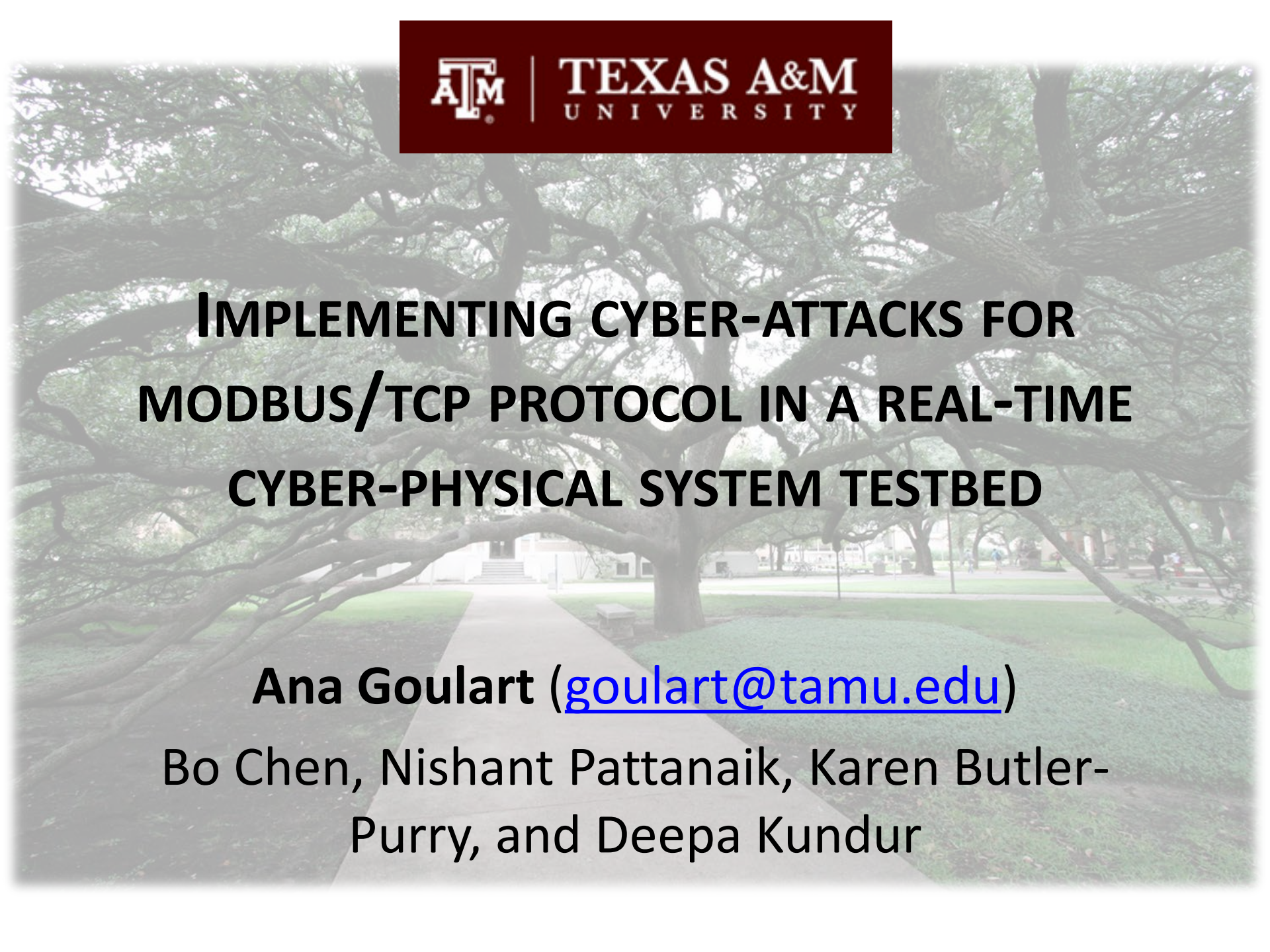


IMPLEMENTING CYBER-ATTACKS FOR MODBUS/TCP PROTOCOL IN A REAL-TIME CYBER-PHYSICAL SYSTEM TESTBED

Ana Goulart (goulart@tamu.edu)

Bo Chen, Nishant Pattanaik, Karen Butler-Purry, and Deepa Kundur

Outline

- Motivation for a Smartgrid testbed
- Existing testbeds
- Our testbed architecture
- Case studies:
  - Man-in-the-middle attack (MITM)
  - Denial of Service attack (DoS)
- Conclusions

Motivation

- What is SmartGrid?

  Monitoring and controlling power systems in communication networks

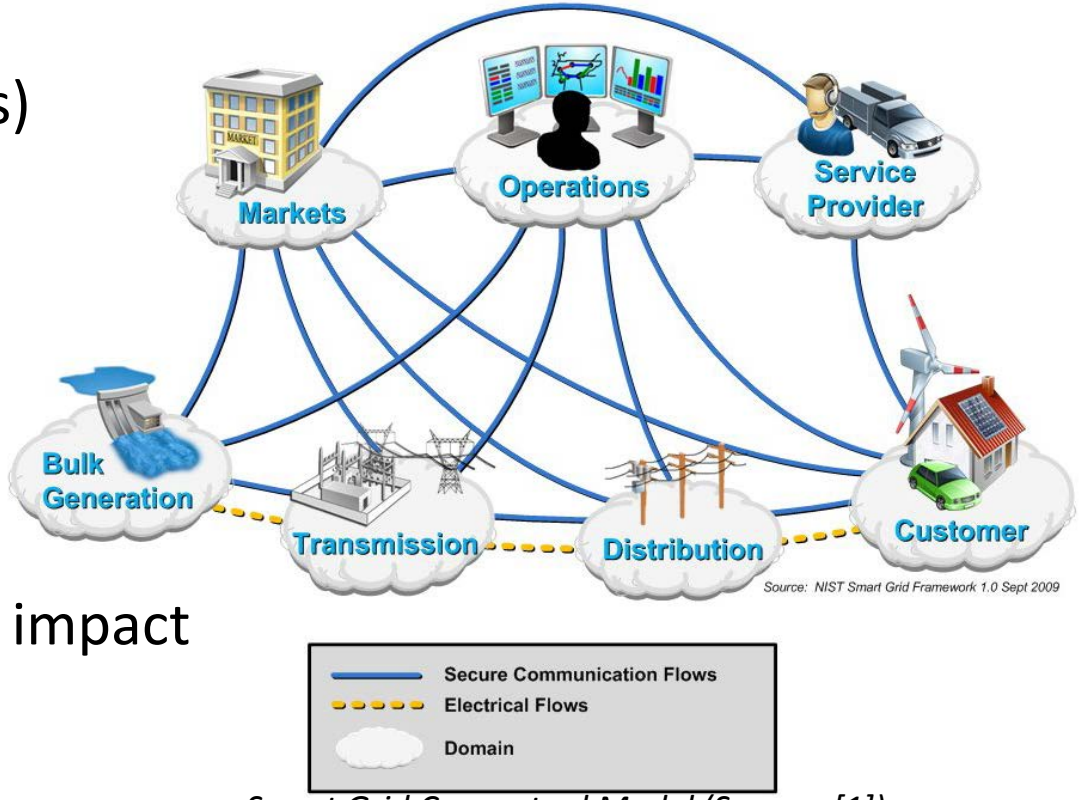
  – Many access points (IEDs)

  – Public networks

- Security in SmartGrid

  – Lack of cybersecurity awareness in early SCADA

  – Development of testbed to assess vulnerability and impact of cyber attacks.



Smart Grid Conceptual Model (Source: [1])

[1] "Report to NIST on the Smart Grid Interoperability Standards Roadmap," Electric Power Research Institute (EPRI), Palo Alto, CA, 2009.

Testbeds in the literature

Test Bed		Real Time	Smart Grid Protocol Supported	Components	
Name	*Year*			*Commercial*	*In-House*
[13]	2014	Yes	IEC 61850	RTDS, LabVIEW, OPNET	N/A
[14]	2013	Yes	DNP3, IEC 61850, MMS	RTDS, DIgSILENT	ISEAGE
[15]	2011	Yes	Modbus/TCP	PowerWorld, OPNET, Modbus RSim	N/A
[16]	2008	Yes	Modbus/TCP	OPNET, PXI, RTU	UMR
[17]	2006	Yes	Modbus/TCP	PowerWorld	RINSE

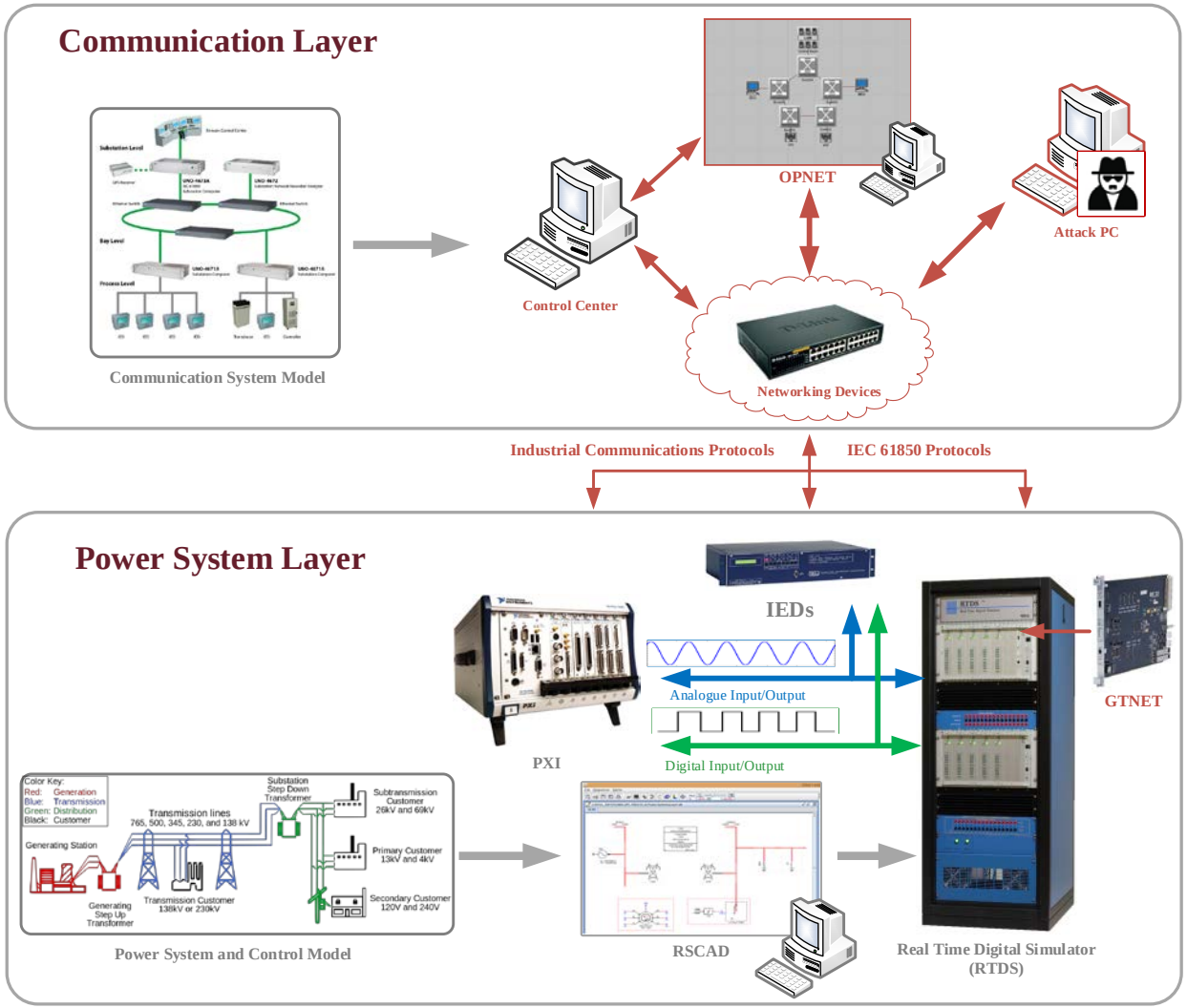
- In-house components are difficult to duplicate
- Support for multiple SmartGrid protocols is needed:
  - IEC61850 (LAN within a substation)
  - Modbus/TCP, DNP3 (control commands from/to SCADA system)

Goals of our cyber-physical testbed

- Capabilities
  - Cyber-physical system simulation
  - Data visualization
  - Interoperability *(use of commercial and open source tools)*
  - Scalability
- Applications
  - Testing and validation for advanced IEDs and control methods
  - Impact analysis (*in this paper, MITM and DoS*)
  - Vulnerability evaluation
  - Mitigation evaluation
  - Training and education

Testbed Architecture

- RTDS
  - Power system and control simulation
  - Data acquisition
- NI LabVIEW and PXI
  - Controller/Protection-in-loop
  - Data acquisition
- OPNET simulator
  - Communication system simulation
- Real World Devices
  - IEDs
  - Switches, routers
- Attack PC
  - Cyber attack software



Testbed Architecture of the Real-Time Cyber-Physical Testbed

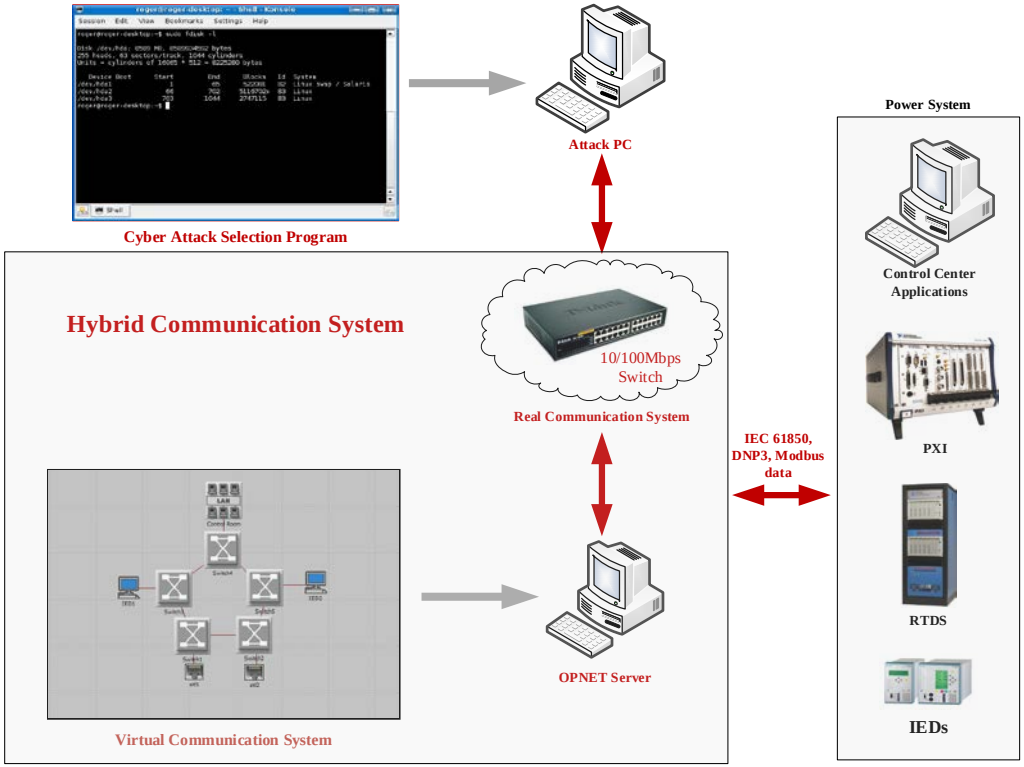
Communication System

OPNET

- System-In-The-Loop (SITL)
- Allows to develop a hybrid system by connecting to real networks
- Attack PC can connect to each real and simulated node

RTDS and NI PXI

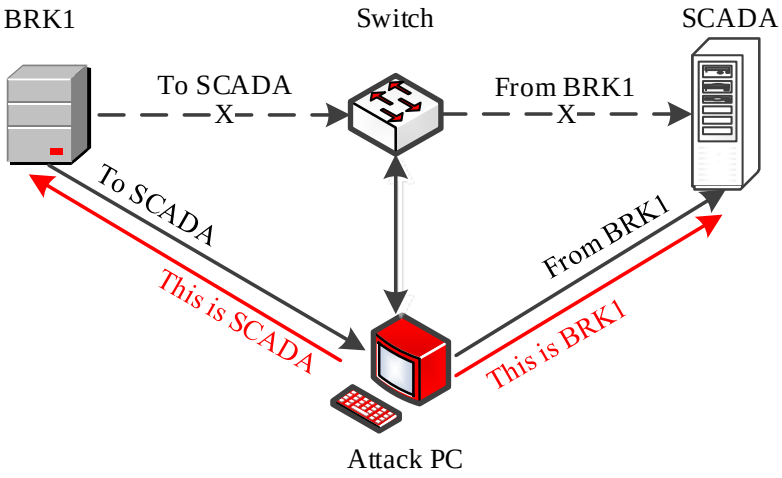
- GTNET (IEC 61850 Sampled Values)
- Industrial Communications Protocols (DNP3, Modbus TCP, etc.)



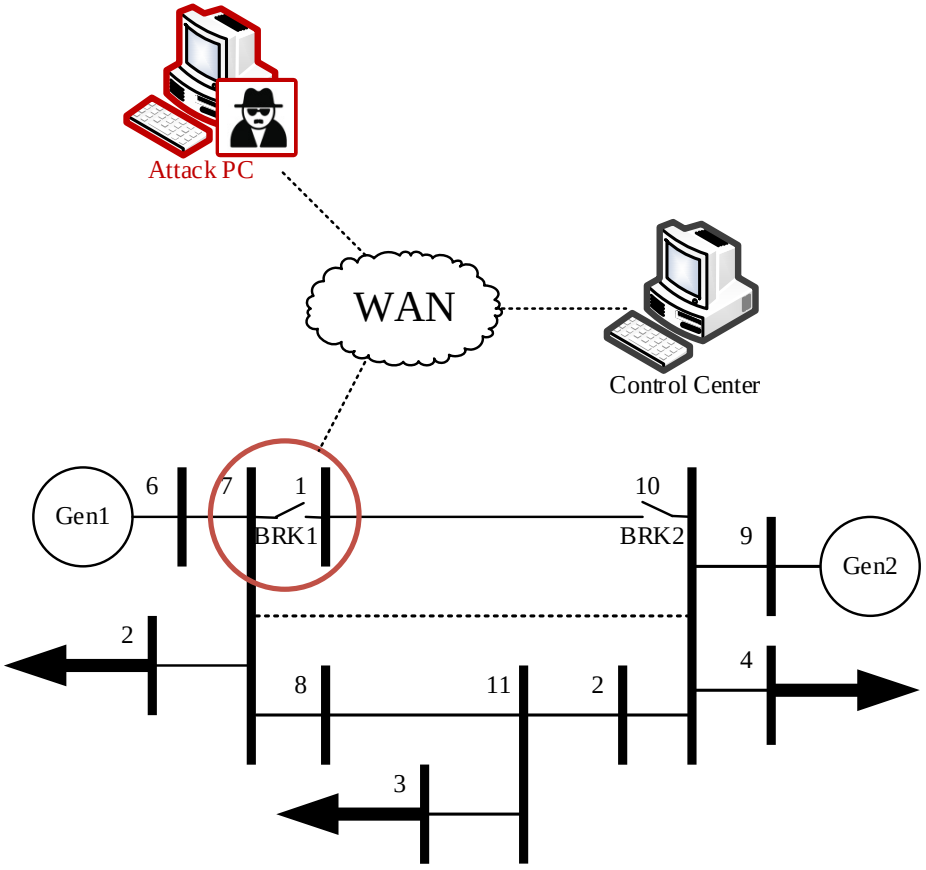
Modeling Communication Systems in the Real Time CPS Test Bed

Case Studies: Impact Analysis of Cyber Attacks

- MITM attack can disrupt the original link between an IED and the SCADA, and develop another link
- An attacker can eavesdrop, delay, or manipulate the packets
- In this case study, the attack PC will inject tripping signal to open BRK1

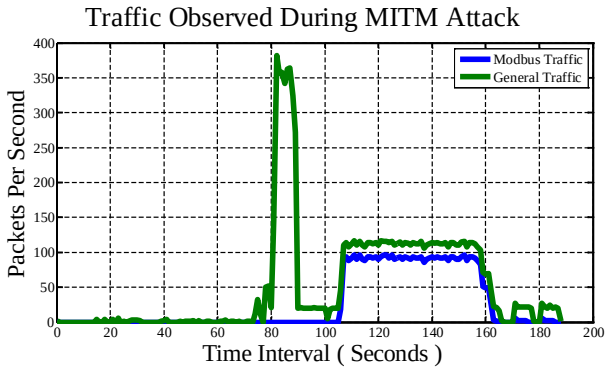


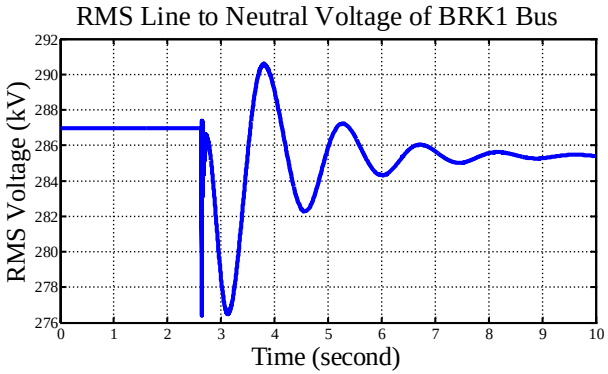
Man-In-The-Middle Attack

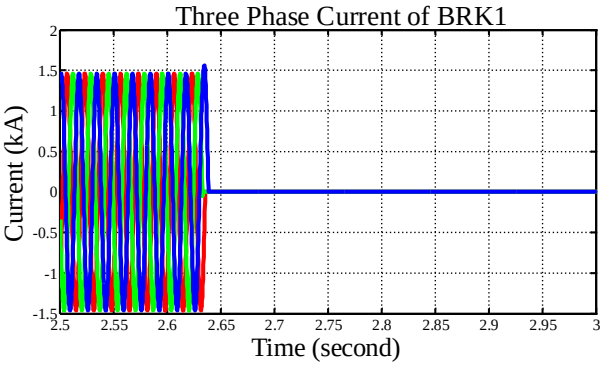


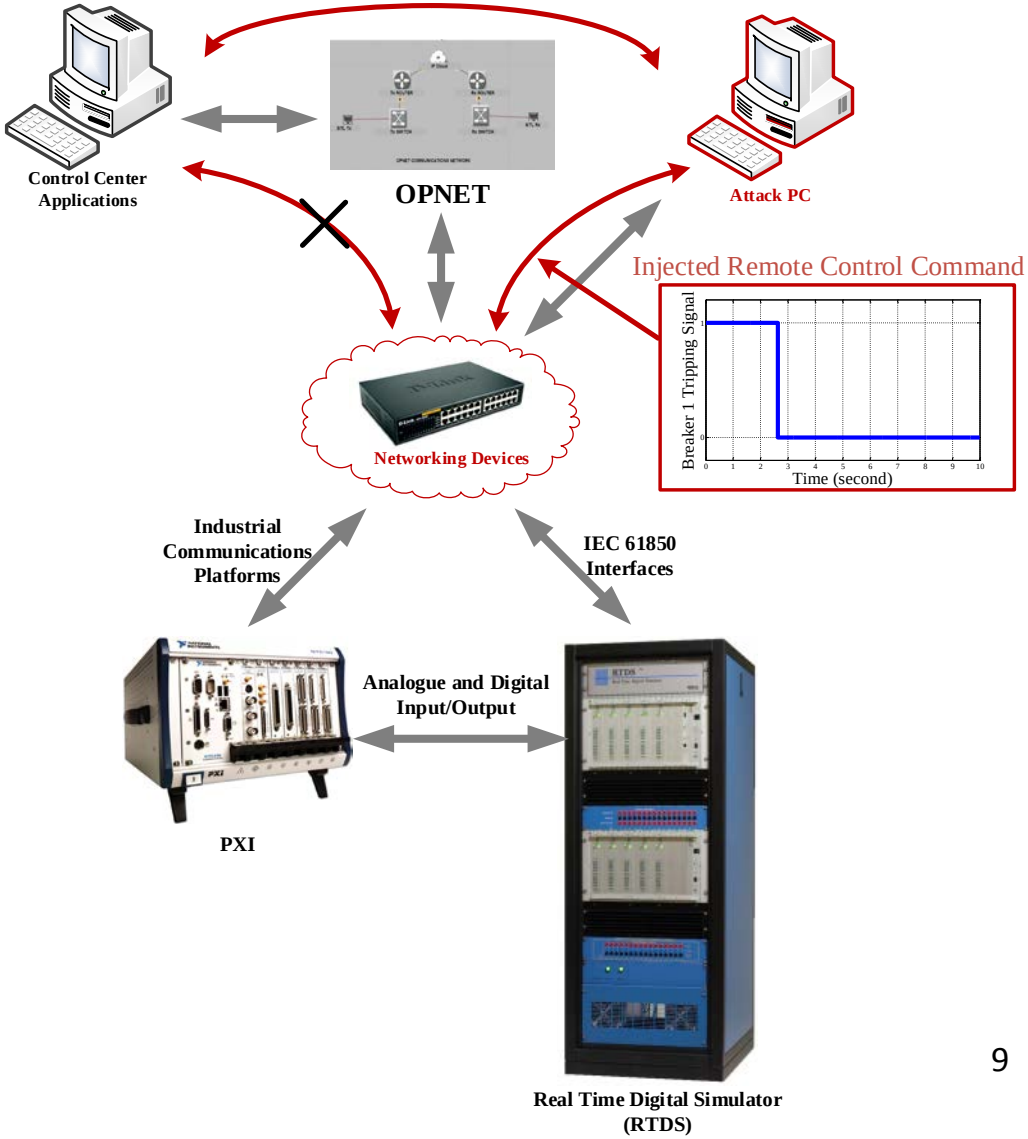
11 Bus Power Transmission System Modeled in the Test Bed

Case Study: Man-In-The-Middle Attack



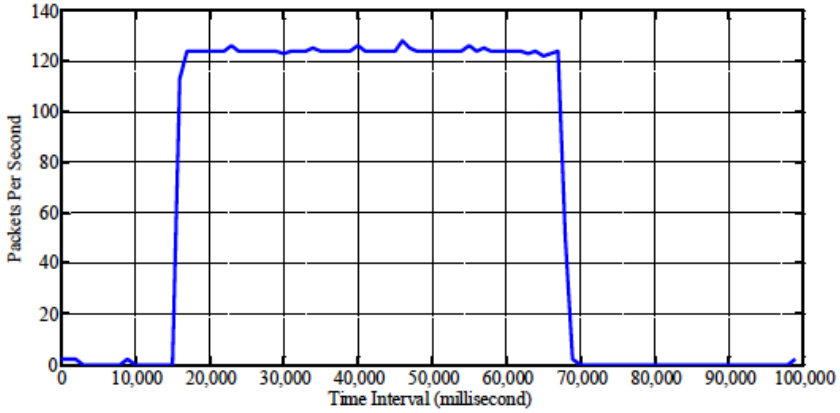


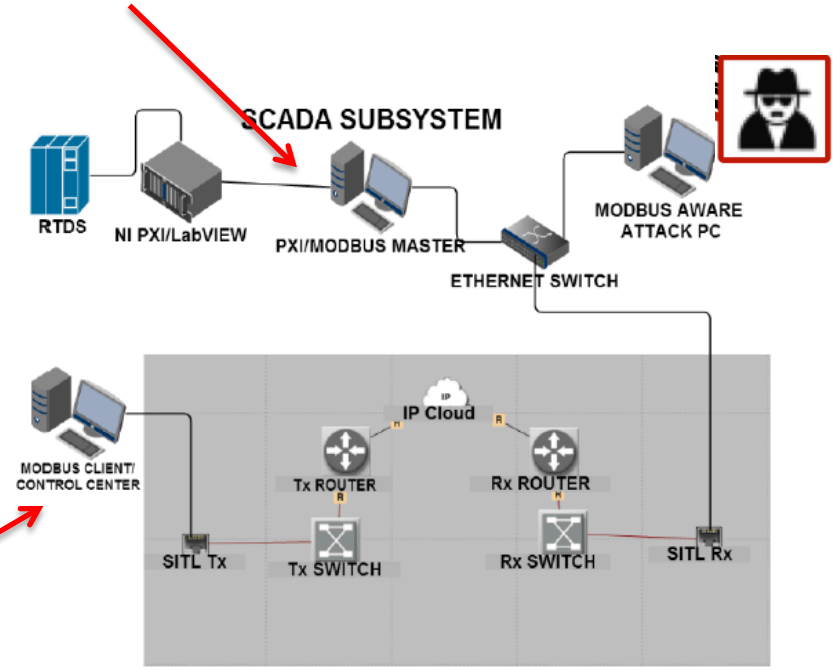




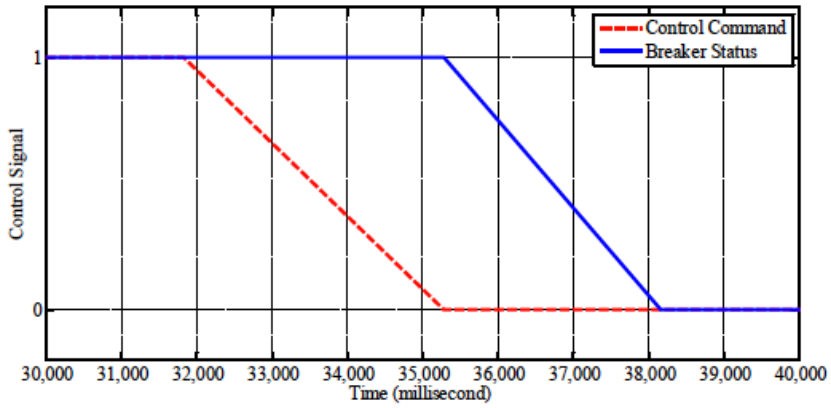
Case Study: SYN Flood

Spoofed TCP SYN packets received at the Modbus master

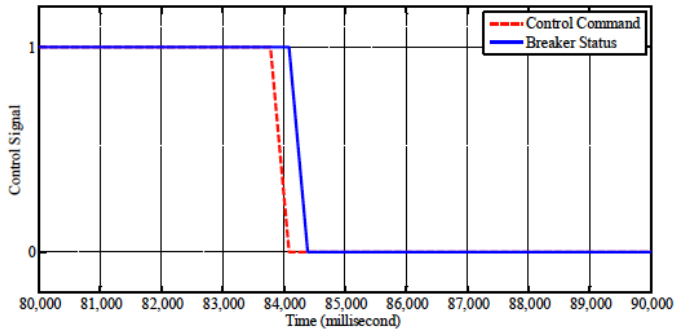




Delay between control and status messages at Modbus client during SYN flood



Delay - no SYN Flood



Conclusions

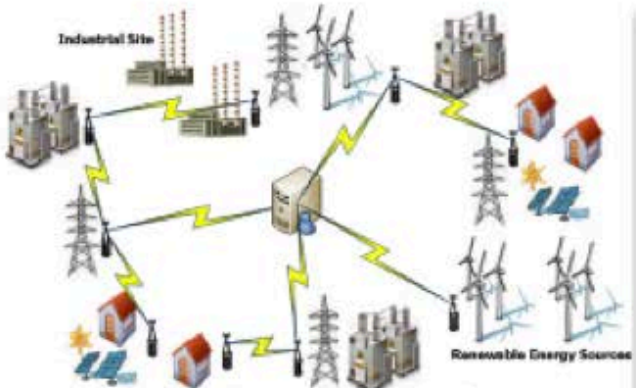
- Impact of cyber-attacks
  - MITM
    - affected stability of the system
    - if multiple transmission lines are tripped by the attacker, we can have power outage
  - SYN flood (DoS attack)
    - Delayed commands or status messages
    - SCADA control center may not have accurate picture of the system
    - Currently simulating different rates and duration of SYN floods

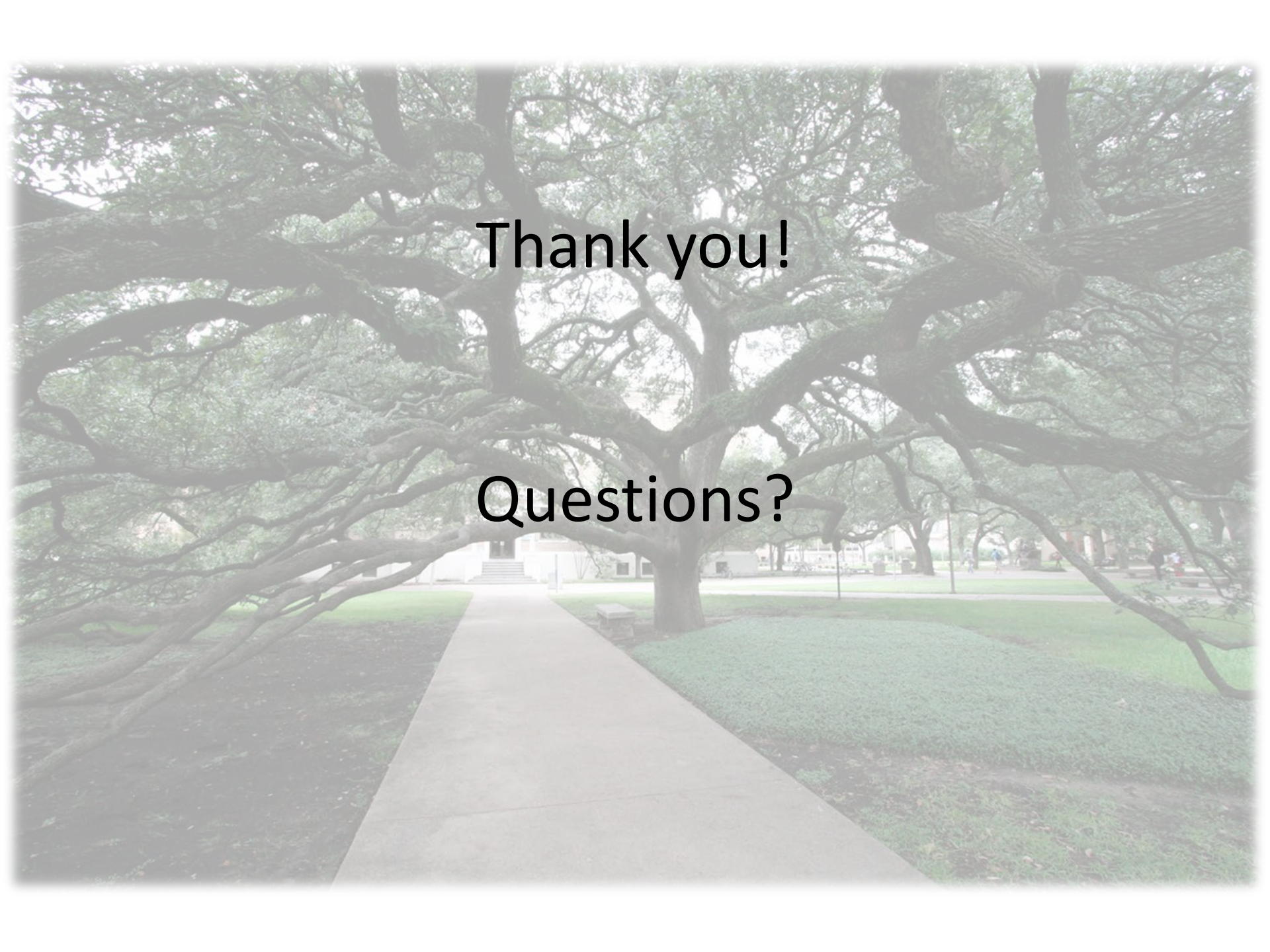
Future Work

- Adding Voltage/VAR control using ETAP
- Extending the testbed

  Modbus – add timestamps in Modbus packet to help detect delayed Modbus responses and spurious Modbus messages

  Ipsec – adding Layer3 encryption




Thank you!
Questions?