GridStat Middleware Communication Framework: Application Requirements

Cyber-Physical Co-Simulation for Analyzing Impact of Cyber Events on the Power Grid

R. Liu, C. B. Vellaithurai, and A. K. Srivastava

GOALS

- Utilize developed cyber-physical test-bed for analyzing cyber-power interdependencies and impact of cyber events on the electric power transmission system.
- Develop high-level system analysis for cyber-physical vulnerability analysis.

FUNDAMENTAL QUESTIONS/CHALLENGES

- How to model and simulate end-to-end systems in real-time or near real-time with physical industrial hardware in the loop.
- How to model real-time dynamic unbalanced physical system simulation with the cyber system model.
- How to explore cyber-power system vulnerabilities in a comprehensive and truly integrated manner using a test-bed.

RESEARCH PLAN

- Identify possible cyber-physical vulnerabilities of wide area network (WAN) applications.
- Explore realistic cyber attacks that can be simulated and analyzed on the developed cyber-physical test-bed.
- Conduct integrated cyber-physical vulnerability and security analysis using the developed cyber-physical test-bed.

RESEARCH RESULTS

- Four different layers have been modeled in the developed test-bed, including (i) the power systems layer, (ii) the sensors and control layer, (iii) the communication layer, and (iv) the application layer. The data flow and the interaction among different layers are shown in Fig. 1.

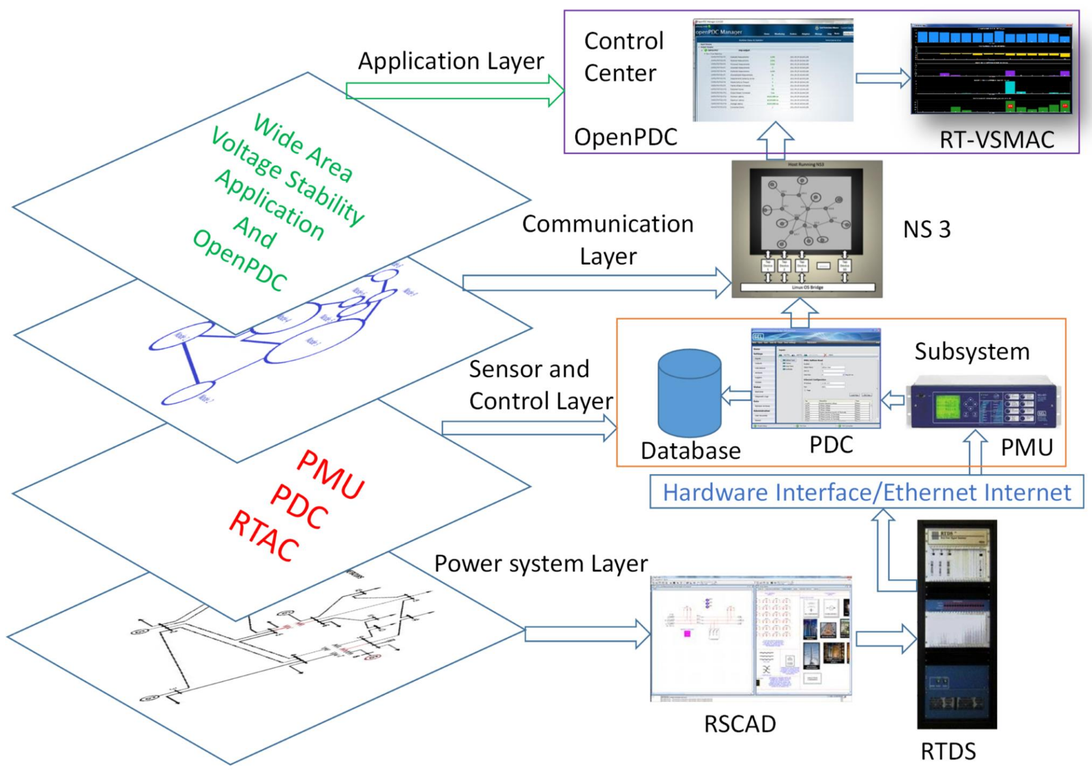

Fig. 1: Cyber-Physical Test-Bed Architecture

- The developed test-bed is used to demonstrate the impact of three different possible kinds of cyber-attacks on the power system, including communication line outage attacks, denial-of-service attacks, and man-in-the-middle (MITM) attacks.
- Communication line outage attacks are simulated by changing the routing table in the network simulator 3 (NS 3) to induce a communication delay on the packets to the destination.
- In a denial-of-service attack, the attacker crashes the service on a specific node by changing the error rate, which means that all the packets that go through a specific node are considered bad data and get dropped.
- Figure 2 shows the architecture of an MITM attack. Under normal operating conditions, the local PDC sends the synchrophasor data directly to the control center, but during an attack, it is assumed that the attacker uses ARP spoofing to poison the two communication endpoints in such a way that the local PDC sends data, which was originally intended for the control center, to the attacker's computer. Thus, the attacker can silently sit between the local PDC and the control center. The attacker could also use an MITM attack to corrupt information, including control commands, measurement values, price signals, etc., in the transmitted packets.
- Results demonstrate that the real-time, end-to-end comprehensive system model is necessary in order to analyze the impact of cyber events on the power grid dynamics and performance.

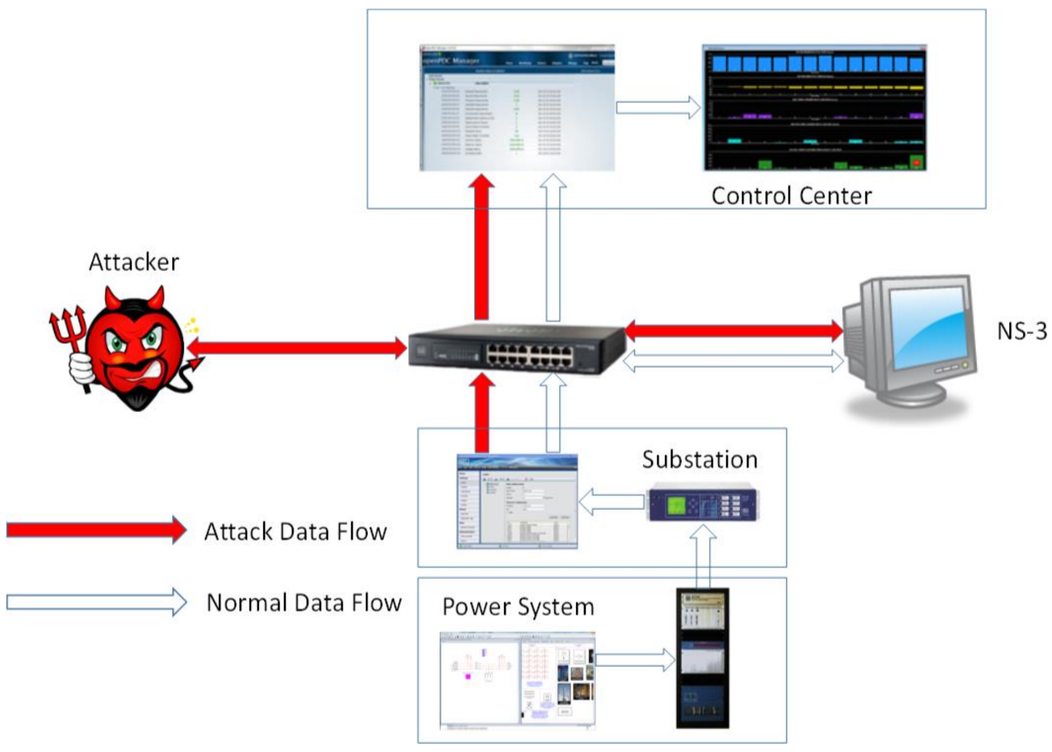

Fig. 2: Man-in-the-Middle Attack using the Developed Testbed

- DeterLab has already been integrated into the developed test-bed to replace NS-3 to emulate the communication network. The new architecture of the test-bed is shown in Fig. 3. With the communication features supported by DeterLab, we are able to observe and interact with real malicious software, operating in realistic network environments at scales found in the real world. More cyber attacks could be tested, and different cyber defense mechanisms could be integrated into the test-bed.

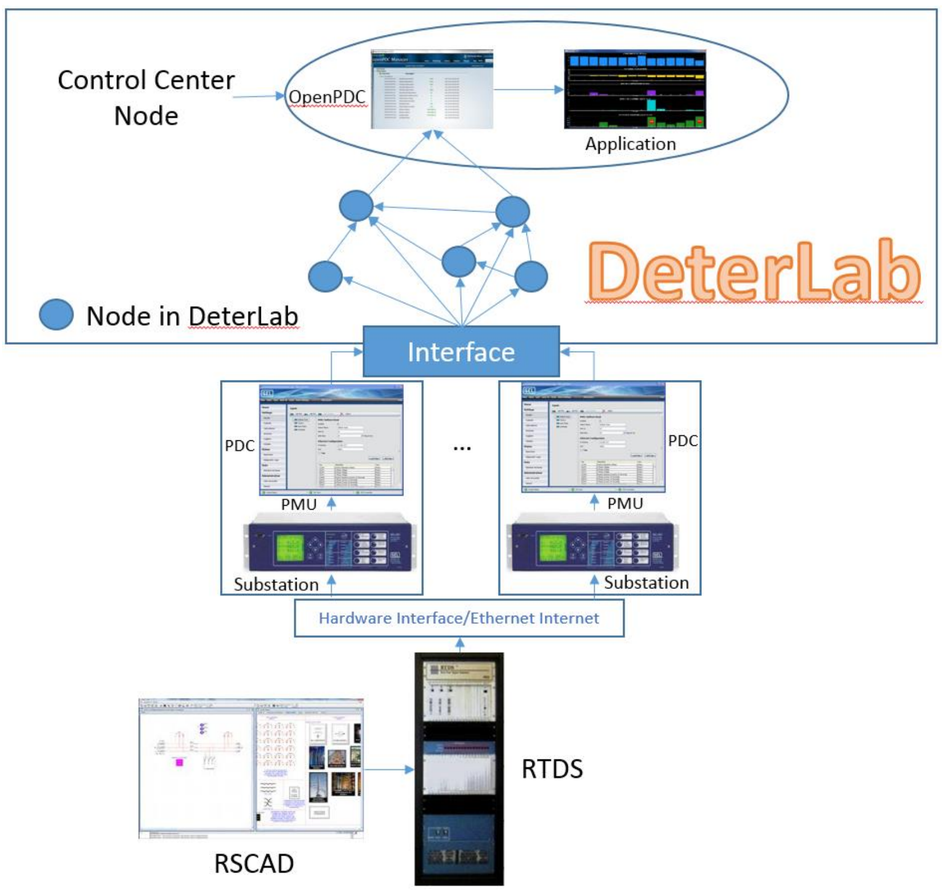

Fig. 3: Architecture of Cyber-Physical Test-bed with Integration of DeterLab

BROADER IMPACT

- Development of integrated cyber-physical system test cases will enable comparative analysis of several different algorithms and provide researchers with a common platform.
- Will provide analytical framework to analyze impact of a coordinated cyber-physical attack on the reliability of the power grid.
- Will build understanding of the complex relationship between power systems and cyber systems, as well as educational opportunities.

INTERACTION WITH OTHER PROJECTS

- Exploring option of using GridStat as a communication interface with RTDS to develop an integrated cyber-physical test-bed.

FUTURE EFFORTS

- Integrate GridStat in the cyber-physical test-bed.
- Utilize the developed cyber-physical test-bed to model additional cyber-power system test cases.
- Develop more realistic smart grid applications and analyze the impact of cyber-physical attacks.

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T