TCIPG

Modeling Methodologies for Power Grid Control System Evaluation

David Nicol, Dong (Kevin) Jin, Yuhao Zheng, Huaiyu Zhu, Lenhard Winterrowd

Goals

- To develop a high-fidelity, highly scalable simulation/emulation platform for security evaluation in power grid control networks.
  - To create a backbone at the core of the Smart Grid testbed at Illinois that connects various components.
  - To create models that support security assessment in a realistic large-scale setting.
  - To create experimental designs and output analysis.

Fundamental Questions/Challenges

- How do we make simulation/emulation run sufficiently fast in large-scale scenarios? How does one balance the trade-off between execution speed and behavioral accuracy?
- How do we mitigate the temporal error introduced by emulations running real application code?
- How can we seamlessly connect the testbed to various virtual and real power/network systems in the TCIPG lab?
- How do we approach experimental design in the “security for power grid context”? What are the metrics? How best do we explore the design space?

Research Plan

- Develop S3F/S3FNet parallel network simulator.
- Implement virtual time systems on virtualization platforms.
  - Virtualization yields high functional fidelity.
  - Virtual time system yields high temporal fidelity.
- Integrate virtualization platforms to S3F/S3FNet. (Figure 1)
  - Simulation: models an extensive ensemble of background computation and communication
  - Emulation: represents execution of critical software.
- Ongoing and remaining work
  - Performance:
    - Acceleration: emulation lookahead.
    - Distributed version: run across multiple machines to support experiments of larger scale.
  - Features: support software-defined networking (OpenFlow) simulation and emulation.
  - Applications: security assessment in the smart grid context (e.g., defense mechanism against DDoS attack in AMI networks).

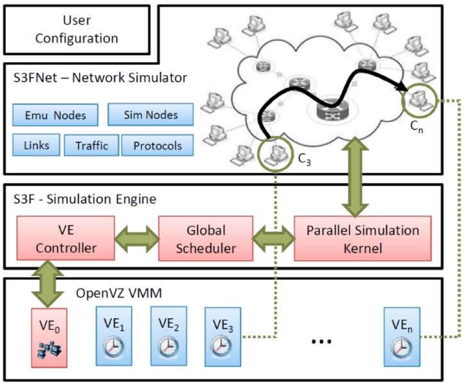


Figure 1: System Design Architecture

Research Results

- Developed and validated our testbed (S3F/S3FNet + OpenVZ).
  - Global synchronization algorithm: integrate simulation & emulation.
  - System temporal error: bounded by one timeslice (100us). (Figure 2)
  - Evaluation of application behavior:
    - Network-intensive (e.g., FTP, browser) / CPU-intensive applications.
    - Introduced error: virtual time system < OpenVZ platform.
- Demonstrated the usability of our testbed. (Figure 3)
  - Model/simulate a DDoS attack on C12.22 protocol in AMI networks.
  - Evaluate the existence and effectiveness of the attack. (Figure 4)

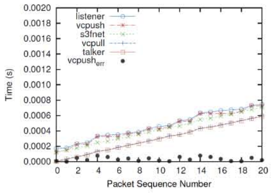


Figure 2: Packet Timestamps Through System Interfaces

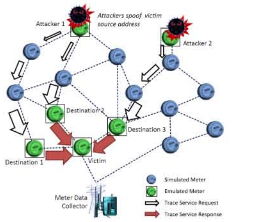
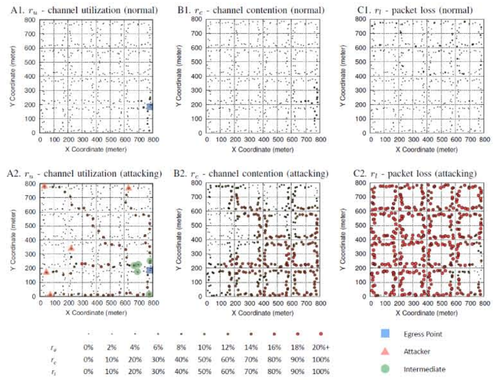


Figure 3: C12.12 Trace Service DDoS Attack in AMI Network



r_u	0%	2%	4%	6%	8%	10%	12%	14%	16%	18%	20%+
r_c	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
r_l	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Figure 4: Experimental Results on the C12.22 Trace Service DDoS Attack

Broader Impact

- Provide platform for assessing security vulnerabilities and proposed countermeasures in a realistic large-scale setting.
- Interact with other research/industrial resources that provide medium-scale real-device testbed and industrial power data.

Interaction with Other Projects

- Support use of testbed for security evaluations for other TCIPG projects.
- Connect our testbed with other systems in the TCIPG lab (e.g., Trilliant, RDTS, the smart meter testbed, etc.).

Future Efforts

- Develop power-grid-specific methodologies that specify what to measure, what set of experiments to run, and how to interpret results.

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org

University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University