TCIPG

Modeling Methodologies for Power Grid Control System Evaluation

David Nicol, Dong (Kevin) Jin, Yuhao Zheng

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 tradeoff 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.
    - S3F simulation engine: the next generation of the Scalable Simulation Framework (SSF).
    - S3FNet: network simulator based on S3F.
- Design & implement virtual time systems on virtualization platforms.
    - Virtualization yields high functional fidelity.
        - Runs unmodified application code.
    - Virtual time system yields high temporal fidelity.
        - Guest OSes perceive time as if they were running concurrently in real world.

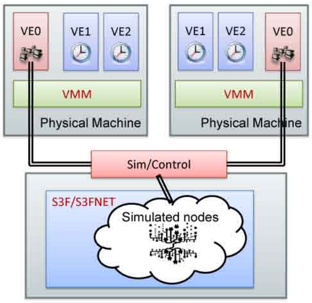


Figure 1: Architecture of testbed

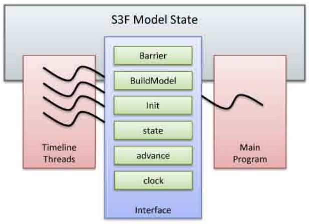


Figure 2: Logical organization of S3F Simulation Program

- Connect virtualization platforms to S3F/S3FNet.
    - S3F controls the emulation progress, to guarantee temporal accuracy and causal correctness.
    - S3FNet simulates low-level network layers and background traffic.
    - Distributed system design that allows simulation/emulation to run across multiple physical machines, and supports heterogeneous virtualization platforms.

Research Results

- Implemented a virtual time system on OpenVZ (single machine version).
    - High functional & temporal fidelity.
        - VEs perceive time as if they were running concurrently.
        - Temporal fidelity subject to scheduler granularity, which is tunable; can be as small as 30 μs.
    - Good scalability: 320 VEs/single machine.
- Developed the first version of S3F/S3FNet.

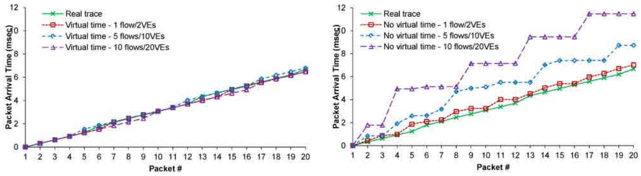
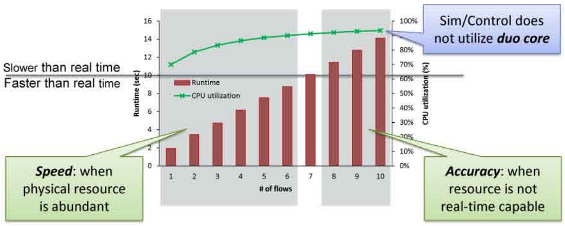


Figure 3: Comparison between virtual time and no virtual time



Sim/Control does not utilize ***duo core***

Speed: when physical resource is abundant

Accuracy: when resource is not real-time capable

Figure 4: Emulation runtime under different load

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, e.g., Trilliant, RDTS, etc.

Future Efforts

- Experimental design
    - Develop power-grid-specific methodologies that specify what to measure, what set of experiments to run, how to interpret results.
- Scalability
    - Connect the virtual time system to the S3F engine.
    - Distributed Sim/Control.
- Fidelity
    - Support more virtualization platforms, e.g., Xen, QEMU.
    - Support more low-level models, e.g., c12.22, ZigBee, ...

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