Simulation of Network Attacks on SCADA Systems

Rohan Chabukswar[1], Bruno Sinopoli[1], Gabor Karsai[2], Annarita Giani[3], Himanshu Neema[2], Andrew Davis[2]

[1]Carnegie Mellon University, [2]Vanderbilt University, [3]University of California Berkeley

TRUST
Team for Research in Ubiquitous Secure Technology

First Workshop on Secure Control Systems
April 12, 2010
Stockholm, Sweden

Carnegie Mellon

Electrical & Computer ENGINEERING

Outline

Legacy SCADA Systems

- Supervisory Control and Data Acquisition Systems
- Designed to have long life spans, decades
- Currently used SCADA systems designed when security wasn't a big issue
- Internet connection exposes the systems to external security attacks

Upgrading Legacy SCADA Systems

SCADA systems are cumbersome to upgrade

1. Upgrading security implies downtime, not desirable in critical systems like power plants and traffic control
2. Legacy SCADA devices are too limited to be upgraded
3. SCADA networks are customized for the systems and their security properties cannot be generalized

Legacy and future SCADA systems require assessment and elimination of security vulnerabilities

Simulation of SCADA Systems

- It is essential to model and simulate communication networks to study mission critical situations
- SCADA system is composed of units in domains like dynamic systems, networks and physical environments
- Each of these units can be modeled using a variety of available simulators and/or emulators
- Simulation of such system needs underlying software infrastructure for a logically and temporally coherent framework

C2WindTunnel

- Enables various simulation engines to interact and transmit data, log and analyze real time simulation results
- Uses discrete event model of computation for the precise integration of a range of simulation engines
- Requires integration on two levels for each simulation model:
  1. API Level: Provides basic services like message passing and shared object management
  2. Interaction Level: Synchronization and coordination.

High Level Architecture (HLA)

- Basis of C2WindTunnel
- Initially designed by US Department of Defense (DoD) to ensure interoperability and reusability of models and simulation components
- Components of the HLA:
  1. HLA rules to ensure proper interaction among federates and to delineate the respective responsibilities
  2. Object Model Template (OMT) to prescribe format and syntax for recording and communicating information

Run Time Infrastructure (RTI)

- Run Time Infrastructure (RTI) is the software implementation of HLA
- A collection of software that provides a set of HLA required services to multiple simulation systems
- Several commercial and open-source RTIs available in the market, some of which have been verified by the US Defense Modeling and Simulation Office.
- RTI handles Federation, Object, Time, and Event Management

Time and Event Management

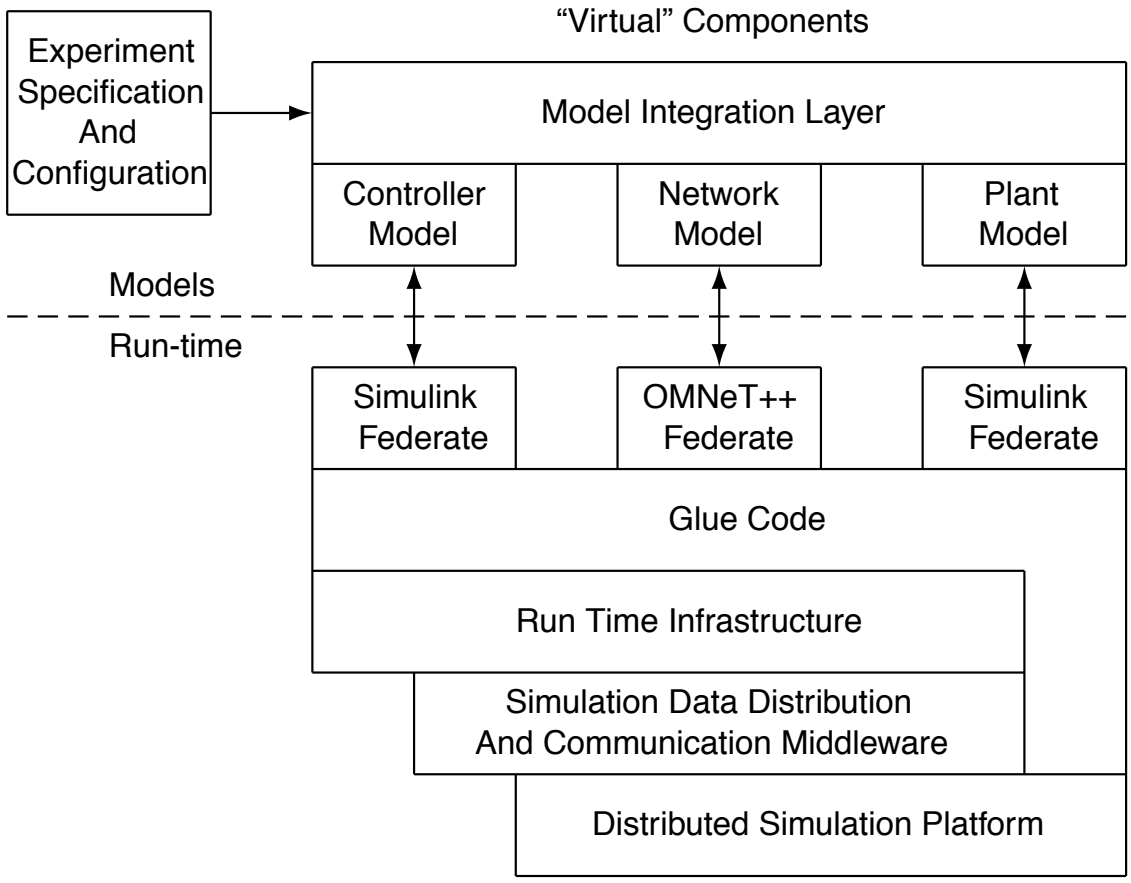
Time Management:

- Federate manager uses HLA-specified synchronization points to guarantee that all federates are ready to proceed with the simulation
- Simulation proceeds for a small time step, after which each federate needs permission from the RTI to proceed

Event and Data Interaction

- A publish and subscribe mechanism is used by the HLA
- Each federate declares to the federation which events it is interested in

C2WindTunnel Simulation Architecture



The Plant

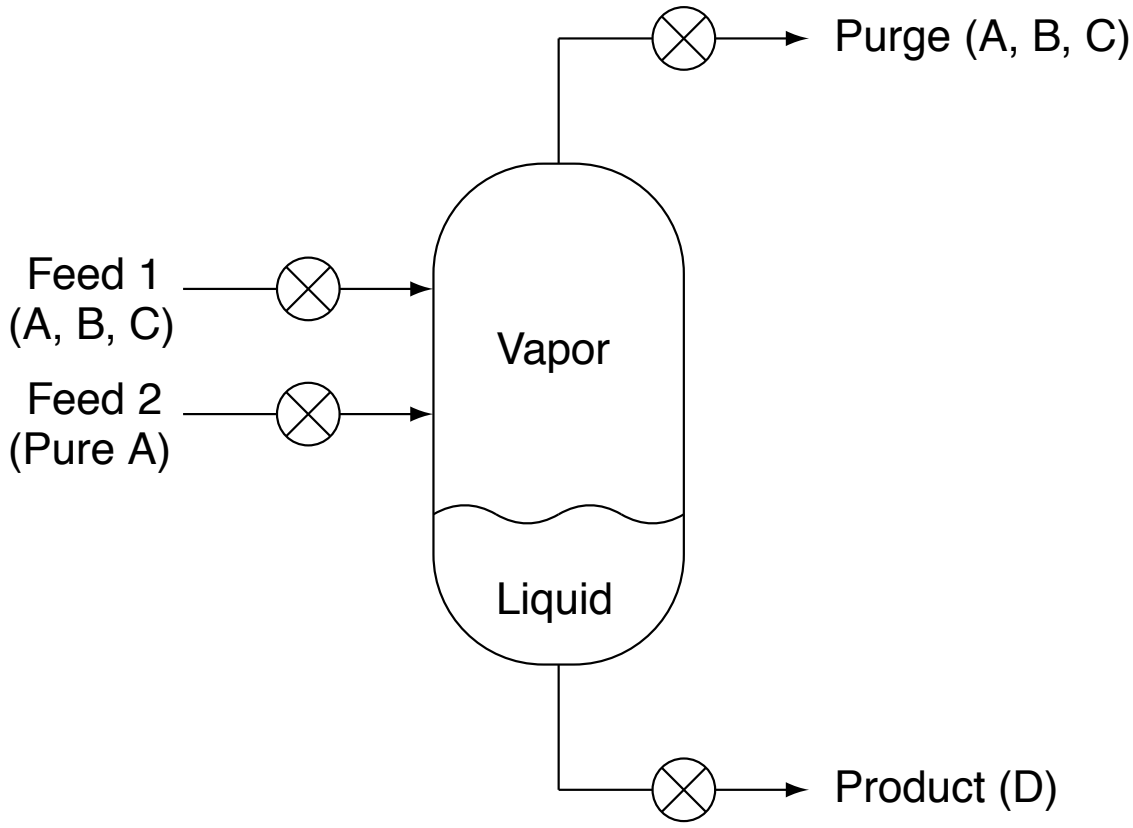


Figure: Chemical Plant ($A + C \rightarrow D$)

Control Problem

Objectives:

- Maintain production rate by controlling valves
- Minimize operating cost (function of purge loss of A and C)

Restrictions:

- Operating pressure below shutdown limit of 3 MPa
- Flows have a maximum at their saturation points

The Controller

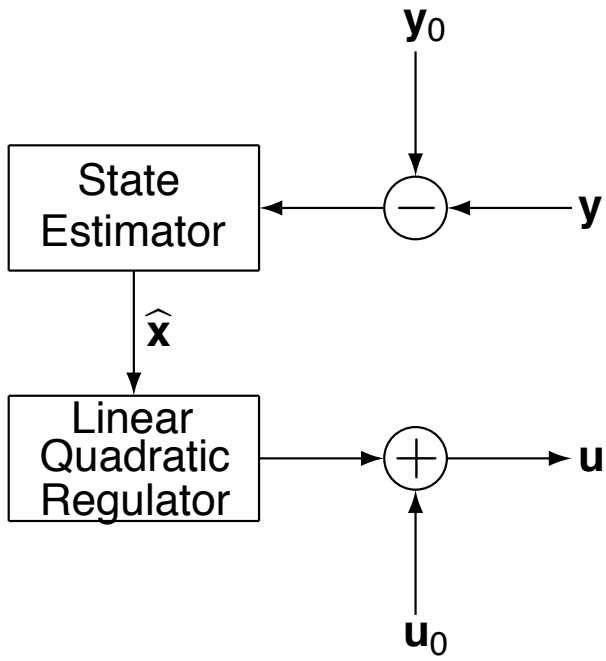


Figure: The Controller (Simulated in Simulink)

Network Map

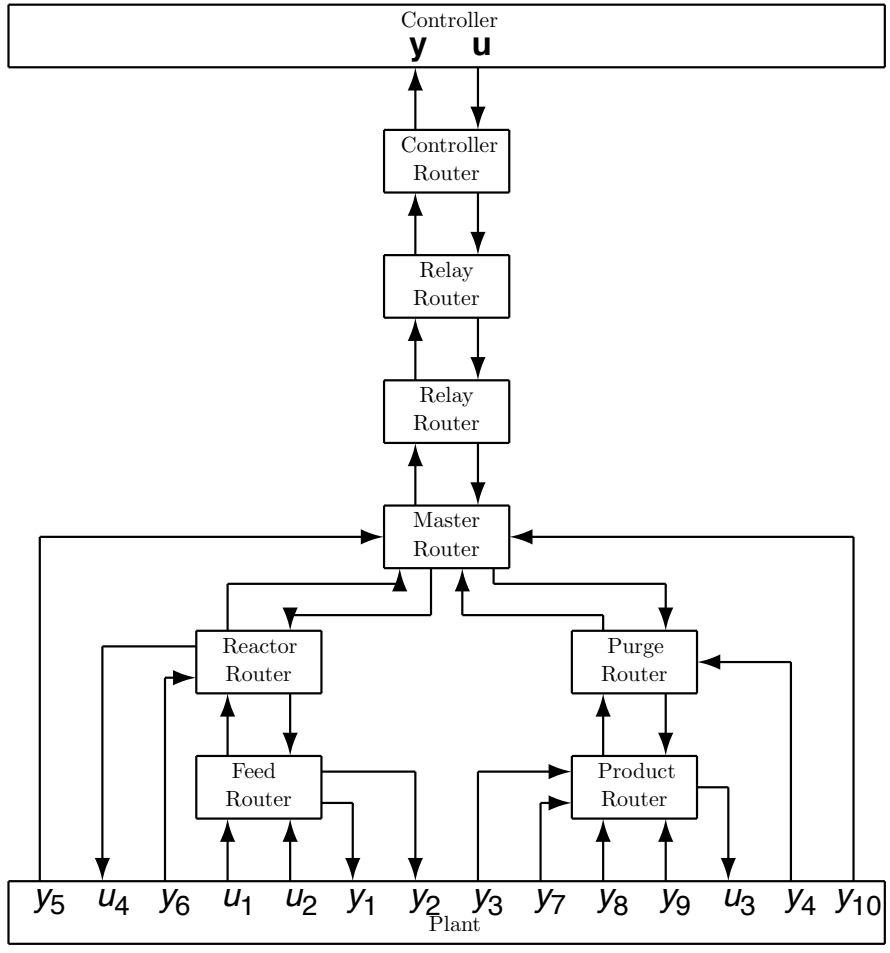


Figure: Network Map (Simulated in OMNeT++)

OMNeT++

- Interpreter traverses the integration model and understands which interactions may be sent or received
- Synthesizes glue code for each router in the system that needs to communicate data to other federates
- OMNeT++ internal simulation clock is synchronized with the RTI
- If a message timestamp is outside the current simulation interval, OMNeT++ requests the RTI for permission to proceed to the next time step

Simulink

- Interpreter generates code to integrate Simulink model with C2WindTunnel
- S-function block in each model for each interaction
- Synthesized integration code synchronizes simulation time
- Performance penalties must be weighed against timing errors to decide on time-steps

Attacks

- DDOS-like attacks are simulated on system, targeting various routers
- Saturated with external communication requests from large number of zombie nodes
- Rendered slow, effectively unavailable legitimate data
- Controller, feed and product routers are attacked from 30-second mark to 60-second mark out of simulation time of 150 seconds

Attack on Controller Router

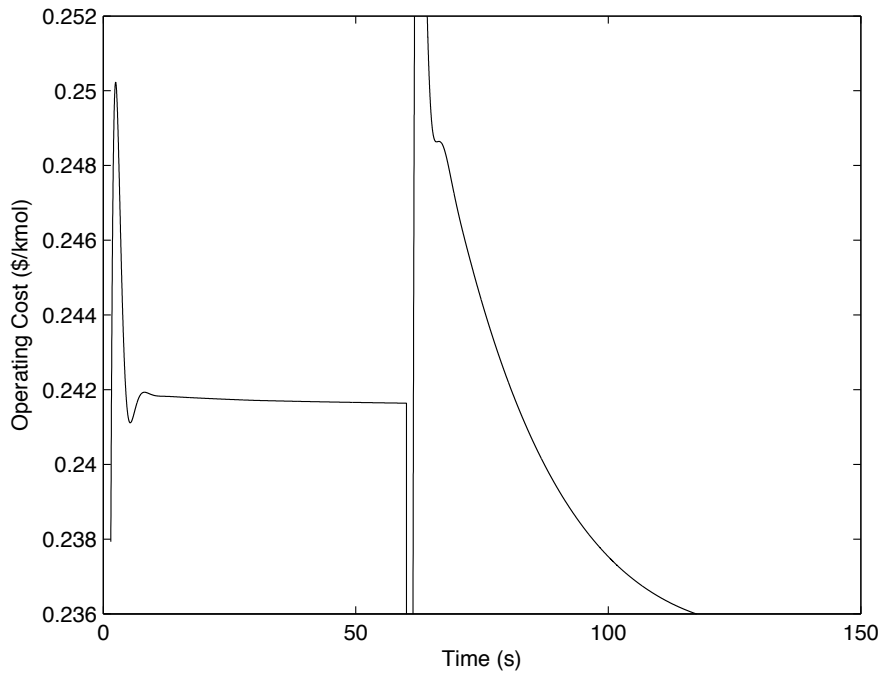


Figure: All sensors, valve controls blocked, plant resets and resumes normal operation after attack.

Attack on Feed Router

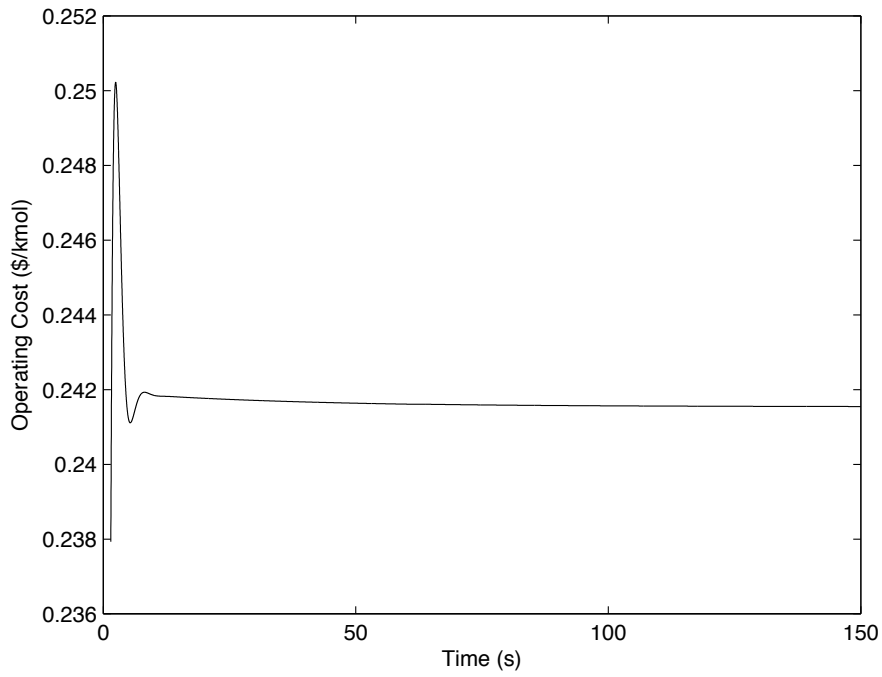


Figure: Feed 1 and feed 2 sensors, valve controls blocked, no effect on plant

Attack on Product Router

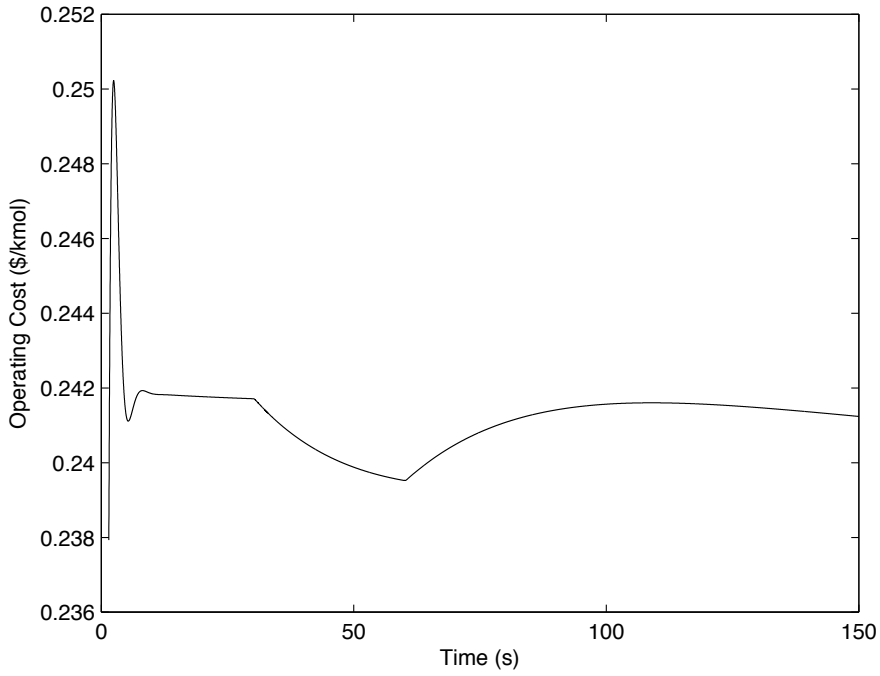


Figure: Several sensors, purge valve controller blocked, plant is uncontrolled for duration of attack, recovers after attack has ceased

Conclusions

- Effects of each individual attack are hard to predict and compare analytically
- For a complicated system, calculating effects would require intensive analytical computations, could be intractable
- Simulation is the best way to estimate effects, to implement and compare network configurations and redundancies
- In proof-of-concept implementation of SCADA system, C2WindTunnel facilitated interaction and data transfer between environments and monitoring response to attacks

Future Work

- Simulation can be used to analyze the current network and controller and develop more robust control algorithms and improve the network
- Expanding the SCADA system itself to employ a fault detection and isolation and/or an intrusion detection system
- Observing the effect of other common network security attacks on integrity and confidentiality of the data
- Simulation of systems including hardware-in-the-loop.

Acknowledgements

This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, DoCoMo USA Labs, EADS, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, TCS, Telecom Italia and United Technologies.

References I

N. Lawrence Ricker, *Model predictive control of a continuous, nonlinear, two-phase reactor*. Journal of Process Control, Volume 3, Issue 2, May 1993, Pages 109-123.

J. O. Calvin, R. Weatherly, *An introduction to the high level architecture (HLA) runtime infrastructure (RTI)*. Proceedings of the 14th Workshop on Standards for the Interoperability of Defence Simulations, Orlando, FL, March 1996, pp. 705-715.

References II

- G. Hemingway, H. Neema, H. Nine, J. Sztipanovits, G. Karsai, *Rapid Synthesis of HLA-Based Heterogeneous Simulation: A Model-Based Integration Approach*. in review for Simulation.
- R. Crosbie, J. Zenor, *High Level Architecture*. `http://www.ecst.csuchico.edu/~hla/`.
- *HLA standard - IEEE standard for modeling and simulation (M&S) high-level architecture (HLA) — framework and rules*. IEEE Std. 1516-2000, pp.i-22, 2000
- *OMNeT++ Simulation Package*. `http://www.omnetpp.org/`