Integrated Simulation and Emulation Platform for Cyber-Physical System Security Experimentation

Wei Yan, Yuan Xue, Xiaowei Li, Jiannian Weng, Timothy Busch, Janos Sztipanovits

Vanderbilt University

HiCoNS 2012
Security Issues of CPS

• Trustworthiness of software and hardware for cyber-physical systems is an essential concern.

• Existing systems are built without sufficiently formalized and analyzed properties and guarantees.
  – Such inadequacies in the system design phase can lead to catastrophic consequences in operations.

• As CPS become more complex it becomes more challenging to formally analyze the performance, stability, safety and security properties of their behaviors.

• There is a pressing need to evaluate both cyber- and physical systems together and holistically
Security Assessment Tool and Experiment Environment

- Evaluation of CPS security requires a sophisticated modeling and simulation, experiment infrastructure that allows for the concurrent modeling, simulation and evaluation of
  - the CPS system architecture (advanced system-of-systems modeling)
  - Running environment (scenario modeling and generation)
  - Attack scenario (threat modeling and generation)

- This requires the integration at two levels
  - Run-time: integration of multiple tools/environment
    - Simulation, emulation, real testbed so that they can interact in a coordinated way
  - Modeling: model integration
    - Rapid configuration/deployment
## Current Solutions

<table>
<thead>
<tr>
<th>Tool</th>
<th>Type</th>
<th>Capacity</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truetime in Matlab/Simulink, Modelica, Ptolemy</td>
<td>Control system modeling and simulation environment</td>
<td>Model complex control algorithms</td>
<td>Limited support for network simulation</td>
</tr>
<tr>
<td>Ns-2, OMNet++</td>
<td>Network simulation environment</td>
<td>Packet-level simulation of network protocol stack</td>
<td>Limited in control system modeling and design</td>
</tr>
<tr>
<td>PiccSIM, ModelSim, NCSWT[HSCC’12]</td>
<td>Integrated modeling and simulation environment of both control and network systems</td>
<td>Model control system dynamics and simulate network behavior simultaneously</td>
<td>Lack of realistic network accuracy and operating system level details.</td>
</tr>
</tbody>
</table>
Our Approach: iSEE

• Integrating network emulation environment with control system simulation environment
  
  – Greater realism and accuracy with truthful protocol implementation and real network traffic delivery

  – Providing a computing platform where prototypes of software components can be deployed
Our Approach: iSEE

• Two major components
  – The modeling environment for system specification and experiment configuration.
    • System model of CPS
    • Security experiment scenario configuration
  – Run-time environment that supports experiment execution:
    • Network emulation platform: DETERlab: large number of tools available for emulate network attacks
iSEE Overall Framework

Modeling Environment

- Network Interaction Model
- Deployment Model
- Topology Model

Model Interpreter

Run-Time Environment

- NCSWT Simulation Environment
  - RTI
  - Federates Involving network communication

  - EmuGateway Federate
  - Tap Server
  - Simulink Federate

- Host Assignment

  - Tap Client
  - Tap Client
  - Tap Client

- Network Application Code
  - Network File System

- TCL script

Configuration/Control Environment

DETERlab Emulation Environment
Network Deployment Model

Meta-Model

Model
Network Interaction Model

**Meta-Model**

- **InteractionProxy**
  - `0..*`
  - `Delivery: enum`
  - `Order: enum`

- **NetworkInteraction**
  - `<<Model>>`
  - `Timestamp: field`
  - `ProcName: field`
  - `NodeName: field`

- **NetworkInteractionWithPeerInfo**
  - `<<Model>>`
  - `*: PeerProcPort: field`
  - `*: PeerNodeName: field`

**Model**

- `RecvCommandFromNetwork`
  - `NodeName: TBD (UAV1)`
  - `ProcName: RecvCommand`
  - `Timestamp: TBD`
  - `PeerNodeName: TBD (ControlStation)`
  - `PeerProcPort: TBD`
  - `Parameter: Command (String)`

- `SendImageToNetwork`
  - `NodeName: TBD (UAV1)`
  - `ProcName: SendImage`
  - `Timestamp: TBD`
  - `Parameter: ImageURL (String)`

- `RecvImageFromNetwork`
  - `NodeName: TBD (ControlStation)`
  - `ProcName: RecvImage`
  - `Timestamp: TBD`
  - `PeerNodeName: TBD (UAV1)`
  - `PeerProcPort: TBD`
  - `Parameter: PacketDelay (double)`

- `SendCommandToNetwork`
  - `NodeName: TBD (ControlStation)`
  - `ProcName: SendCommand`
  - `Timestamp: TBD`
  - `Parameter: Command (String)`
Network Topology Model

Meta-Model

Model
iSEE Run-time Environment

Emulation Host

Emulation Environment

- Time Synchronization
- Data Communication

Simulation Environment

Emulation Gateway Federate

Matlab/Simulink Federate

RTI
set ns [new Simulator]
source tb_compat.tcl

# Nodes
set EmuGatewayHost [$ns node]
set PlantEmuHost [$ns node]
set ControllerEmuHost [$ns node]

# os
tb-set-node-os EmuGatewayHost EmuGateway

# Links
set link0 [$ns duplex-link $EmuGatewayHost $PlantEmuHost 100Mb 0ms DropTail]
set link1 [$ns duplex-link $EmuGatewayHost $ControllerEmuHost 100Mb 0ms DropTail]
set link2 [$ns duplex-link $PlantEmuHost $ControllerEmuHost 100Mb 0ms DropTail]
set lan0 [$ns make-lan "$PlantEmuHost $ControllerEmuHost" 54Mb 0ms]
tb-set-lan-setting $lan0 "mode" "adhoc"

$ns rtproto Static
$ns run
Accuracy: comparison with NCSWT

Reference

NCSWT

iSEE
NCS WindTunnel [HSCC 2012]

Code/demo: http://vanets.vuse.vanderbilt.edu/dokuwiki/doku.php?id=research:cps
Impact of Security Attacks

Plots of UAV trajectory for various packet loss rate

10%  
20%  
30%
Summary and Demo

- iSEE: an integrated simulation and emulation platform for cyber-physical system security experimentation

For more info: http://vanets.vuse.vanderbilt.edu/dokuwiki/doku.php?id=research:isee

Acknowledgments
- U.S. Army Research Office and Lockheed Martin (W911NF-10-1-0005)
- NSF TRUST Science and Technology Center (CCF-0424422)
- National Science Foundation (NSF) Grants OCI-1127396
- Air Force Research Lab