



Testing the Edge: Cyber Security Testing in the Smart Grid

David M Nicol

University of Illinois at Urbana-Champaign

Problem Considered

“Smart Grid” can mean a number of technologies

- Automation of
 - Topology
 - Voltage support
- Deployment and use of phasor measurement units
- Advanced Metering Infrastructure
 - “smart meters” at the home support
 - More economical data collection, set-up/take-down
 - Load control
 - Real-time pricing

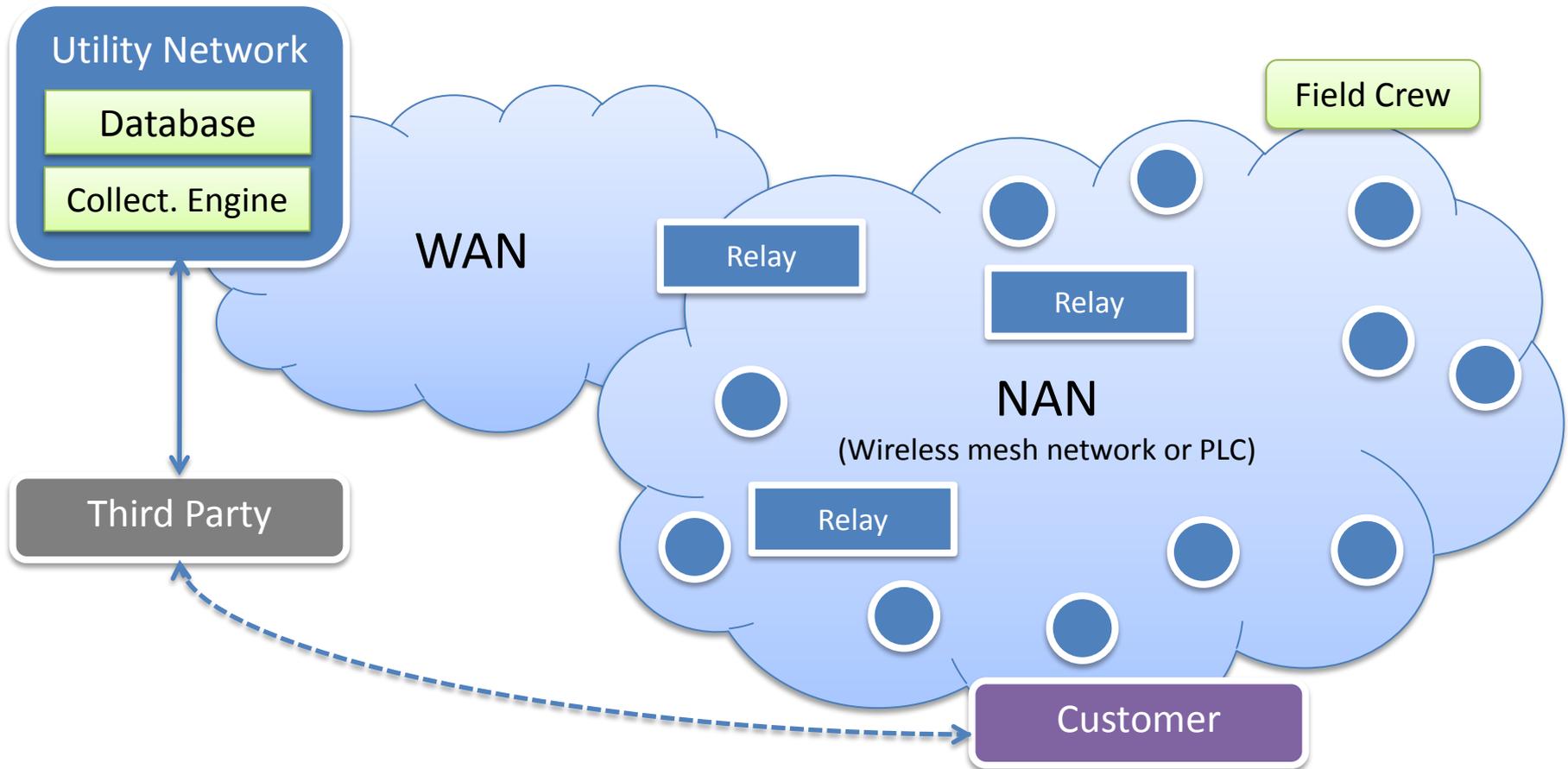
Problem Considered

“Smart Grid” can mean a number of technologies

- Automation of
 - Topology
 - Voltage support
- Deployment and use of phasor measurement units
- Advanced Metering Infrastructure
 - “smart meters” at the home support
 - More economical data collection, set-up/take-down
 - Load control
 - Real-time pricing

We look at AMI “at the edge”

AMI Architecture



WAN: Wide Area Net., **NAN:** Neighborhood Area Net.
PLC: Power Line Comm.

● Smart Meter

AMI Testbed

The top screenshot shows the 'AMI Security Monitoring' interface with a 'Meter' section containing various configuration fields like 'GlobalCurrentProtocol', 'GlobalAccessMethod', and 'PsmUserid'. The bottom screenshot shows the 'Specification-based IDS Console' with a network map and a list of connections.

IDS Management Console

Collection Engine
ITRON

Data Management
System (Oracle DB)

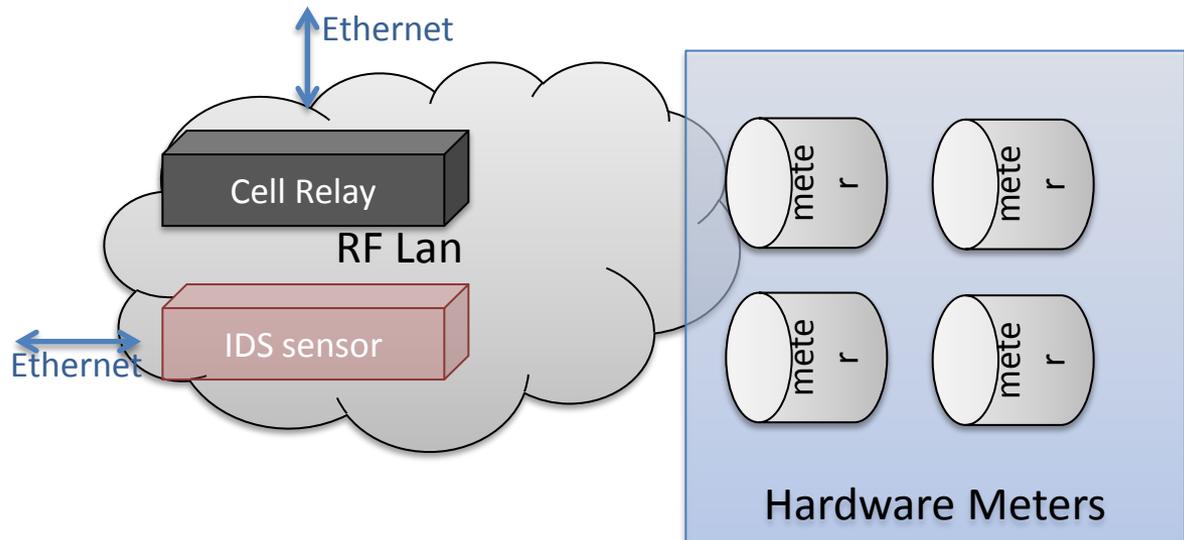
Virtual Machines



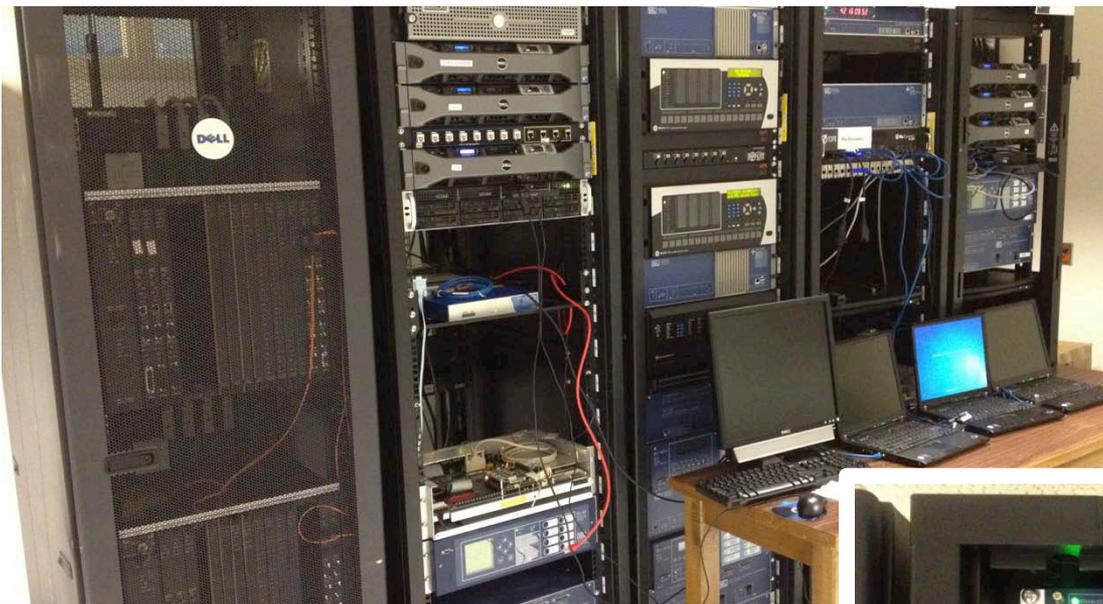
Trilliant Table TstBench
(software meter)

Trilliant Table TstBench
(software meter)

Virtual Meters



AMI Testbed (cont.)



Meters

- System characteristics:
 - OpenWay CENTRON
 - ANSI C12.22 and C12.19
 - Non-volatile memory (EEPROM)
 - RFLAN (unlicensed 900Mhz)
 - ZigBee radio
 - Remote service switch
 - Tamper detection (inversion, removal and reverse power flow)
- Load box (we built this)



Cell Relays

- System characteristics:
 - Designed for pole-mount
 - Backup Battery for power-outage
 - Self-configuring, self-healing 900 MHz RFLAN
 - Ethernet TCP/IP (for WAN)
 - GSM-3G
 - Two external wired interconnects
 - Wi-Fi radio for field service and
 - Embedded computer system - Linux OS
 - GPS receiver (optional)



Security Evaluation : The Challenge

- Production gear, not generally instrumented for deep testing
- Weak standards climate
- Security depends in part on implementation, vendor decisions
 - Variations in communication technology, routing, authentication
 - Means different entry points in security evaluation
- Standard tools often don't work
 - E.g., wireshark does not dissect C12.22 or C12.19 standards
- Such tools as exist are limited, and available only as .exe

Home-brew tools

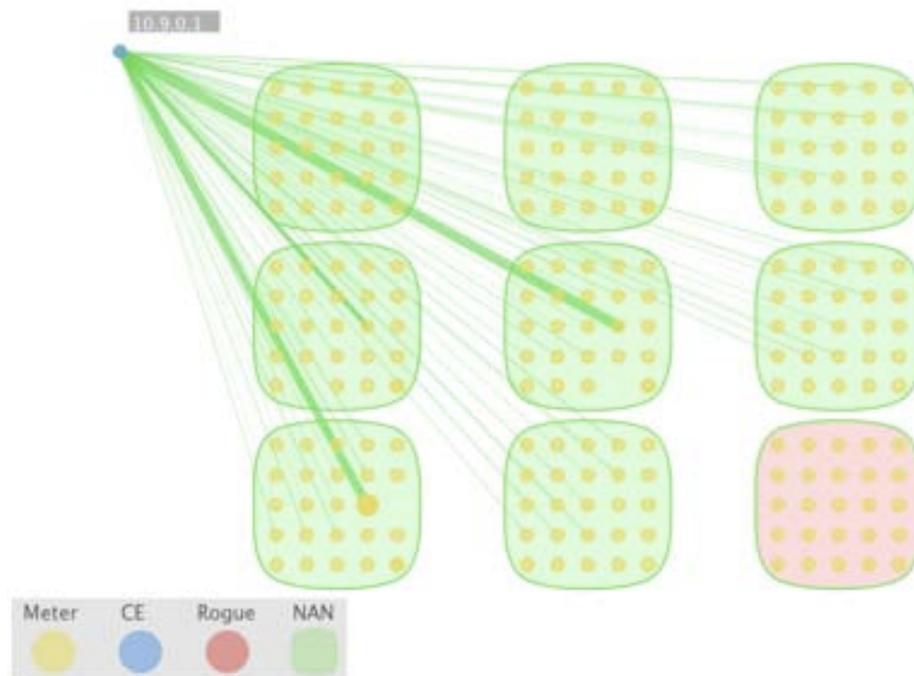
- Protocol dissector of c12.22 / c12.19
 - Libpcap interprets packet headers
 - Payload dissecting using BER decoder
 - State machine tracks c12.22 state over time
 - Tracks meter state transitions based on requests and replies
 - Alerts when behavior deviates from “specification”

Home-brew tools

Visualization

- Takes reports from protocol dissector
- Extracts node and flow information
 - Nodes are dots, flows are edges
 - Color coding

- Nodes detected: 226
- Connections analyzed: 83



Larger Systems

Added challenges in assessing systems too large for the lab

Addressed by our emulation/simulation test-bed

- OpenVZ emulation embedded in virtual time
 - Real c12.22 stacks run with traffic generators
- Integrated with wireless PHYS/MAC layer simulator
- Both emulated and simulated nodes run Zigbee
- Hundreds of nodes represented in effects evaluation of c12.22
Traceback vulnerability we discovered

A Parallel Network Simulation/Emulation Testbed

- A light-weighted virtual machine based emulation

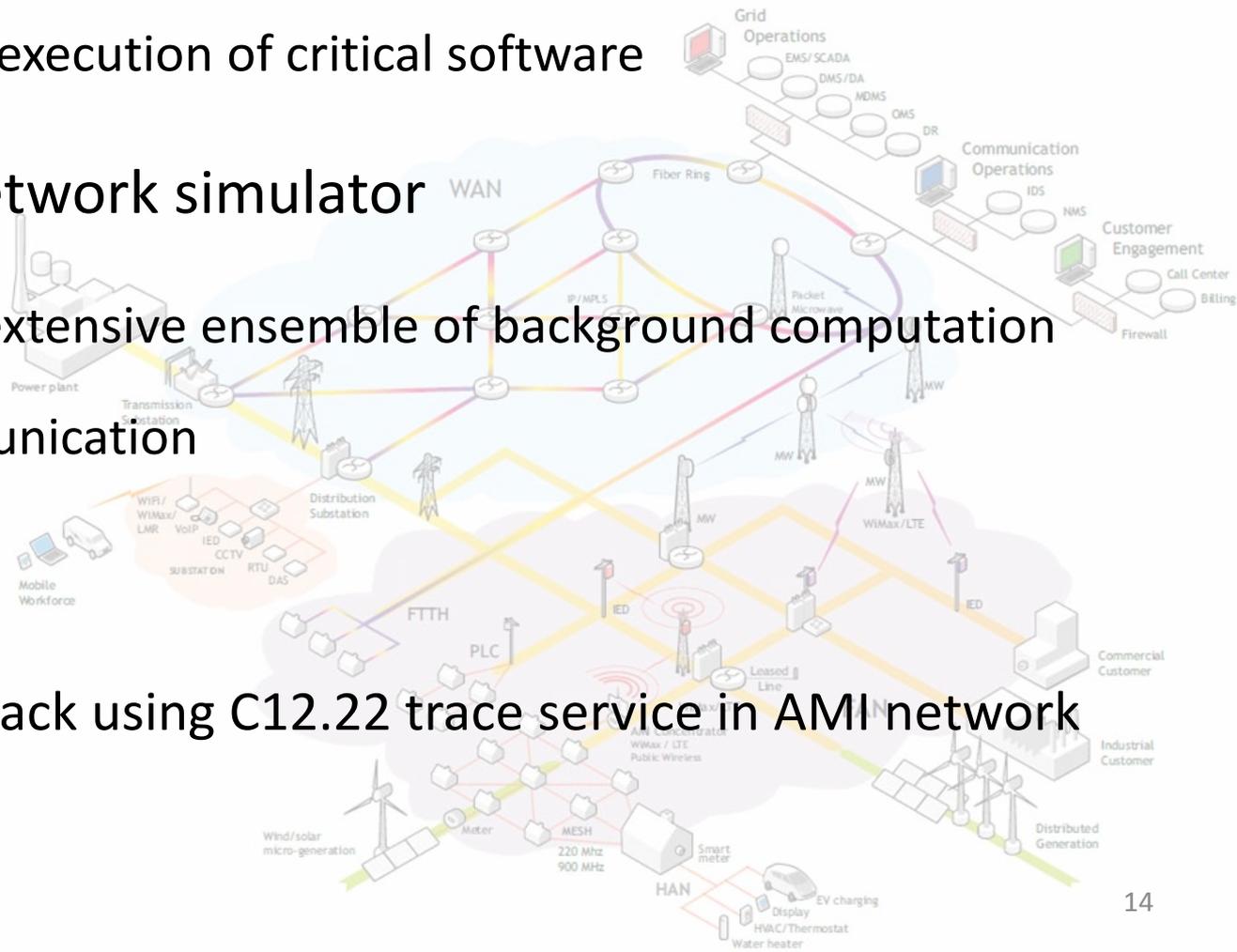
- model the execution of critical software

- A parallel network simulator

- model an extensive ensemble of background computation and communication

- Case study

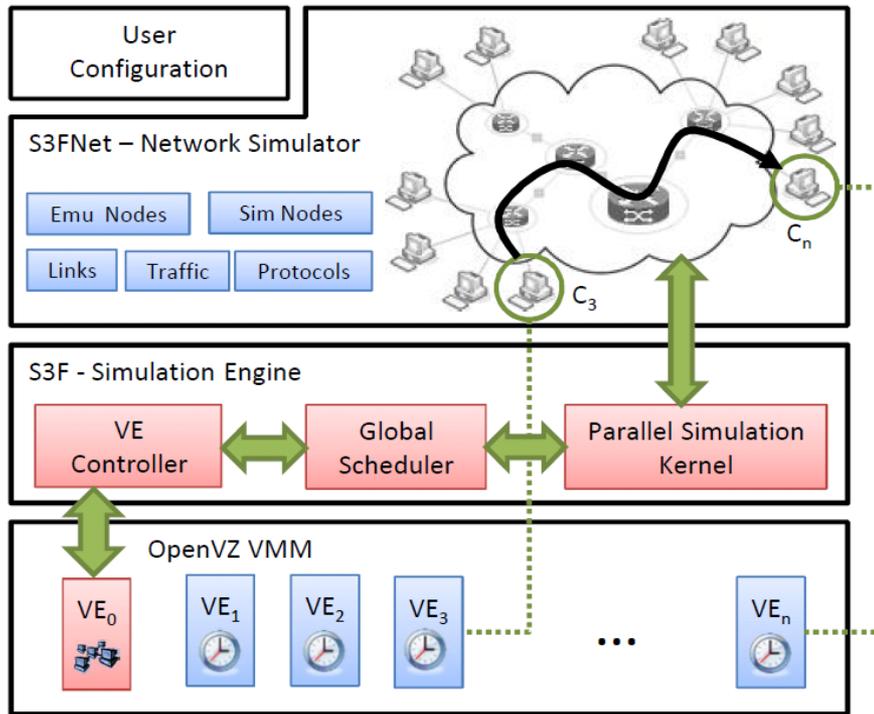
- a DDoS attack using C12.22 trace service in AMI network



A Parallel Network Simulation/Emulation Testbed

- Emulation provides fidelity
 - live experiments, real devices
- Simulation provides scalability and flexibility
- Our network testbed
 - OpenVZ: a light-weighted virtual machine based emulation
 - S3F/S3FNet: a parallel network simulator
- Features
 - Functional and Temporal fidelity
 - Scalability
 - Sophisticated networking environment
 - background traffic
 - wireless/wired-line medium
 - Zigbee models

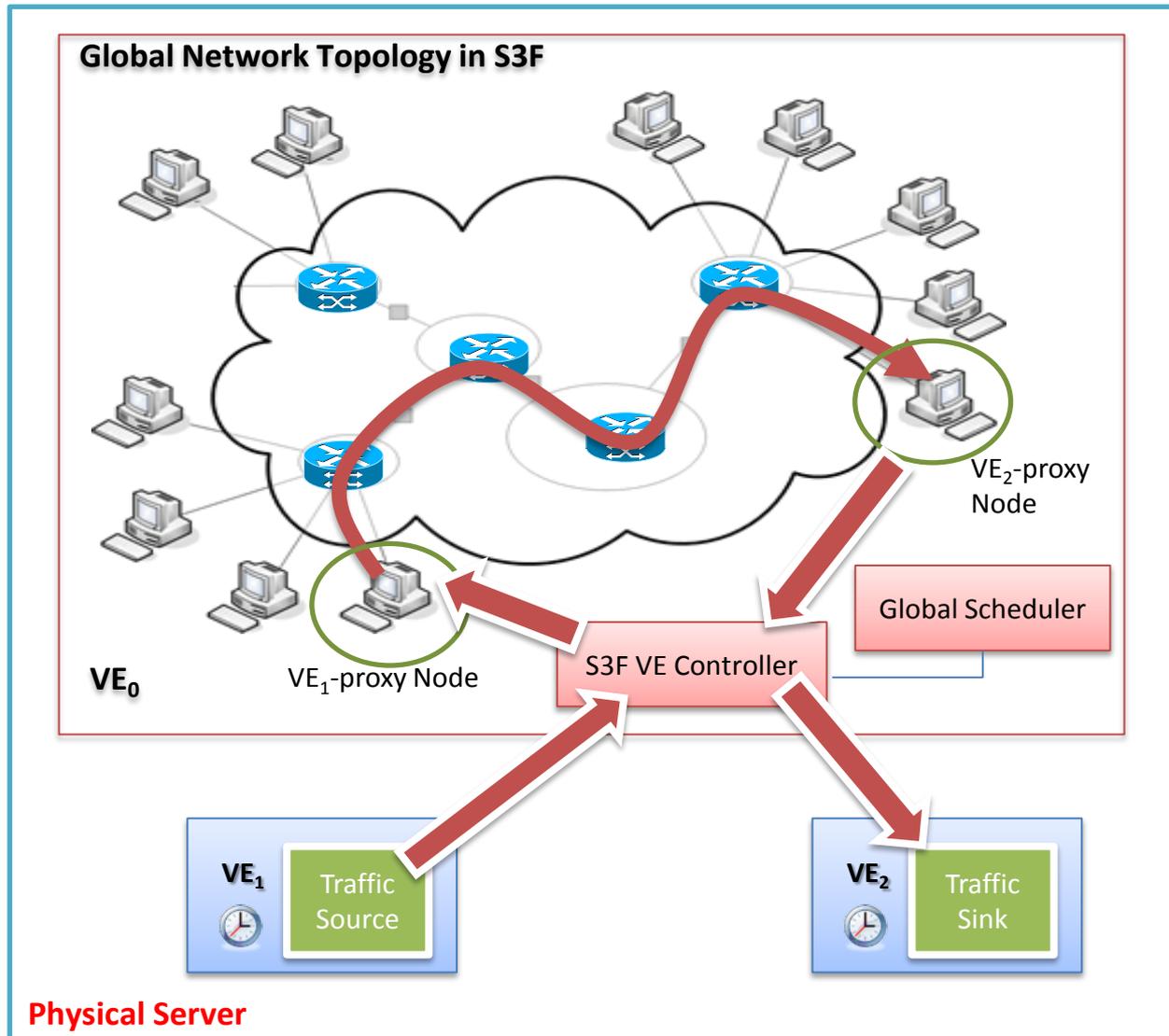
A Parallel Network Simulation/Emulation Testbed



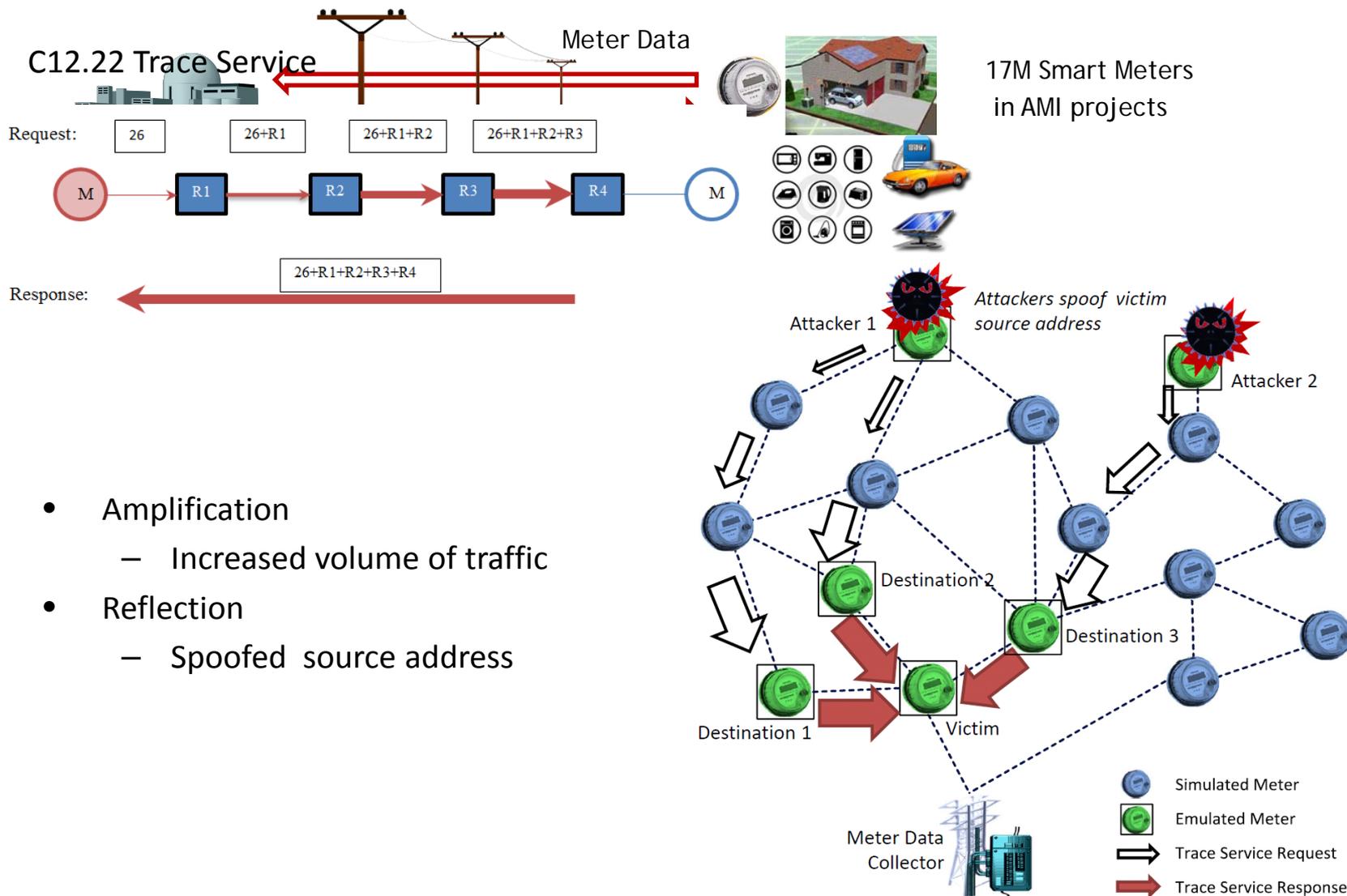
System Architecture

- OpenVZ Emulation
 - virtual time system
 - 300 + virtual machines (VE)
 - Real app, real OS
- S3F Simulation Engine
 - parallel simulation kernel
 - synchronization and message-passing between emulation and simulation systems
 - 10,000+ simulated nodes
- S3FNet Network Simulator
 - background traffic
 - wired-line, wireless medium model
 - switches, routers, virtual hosts
 - protocols

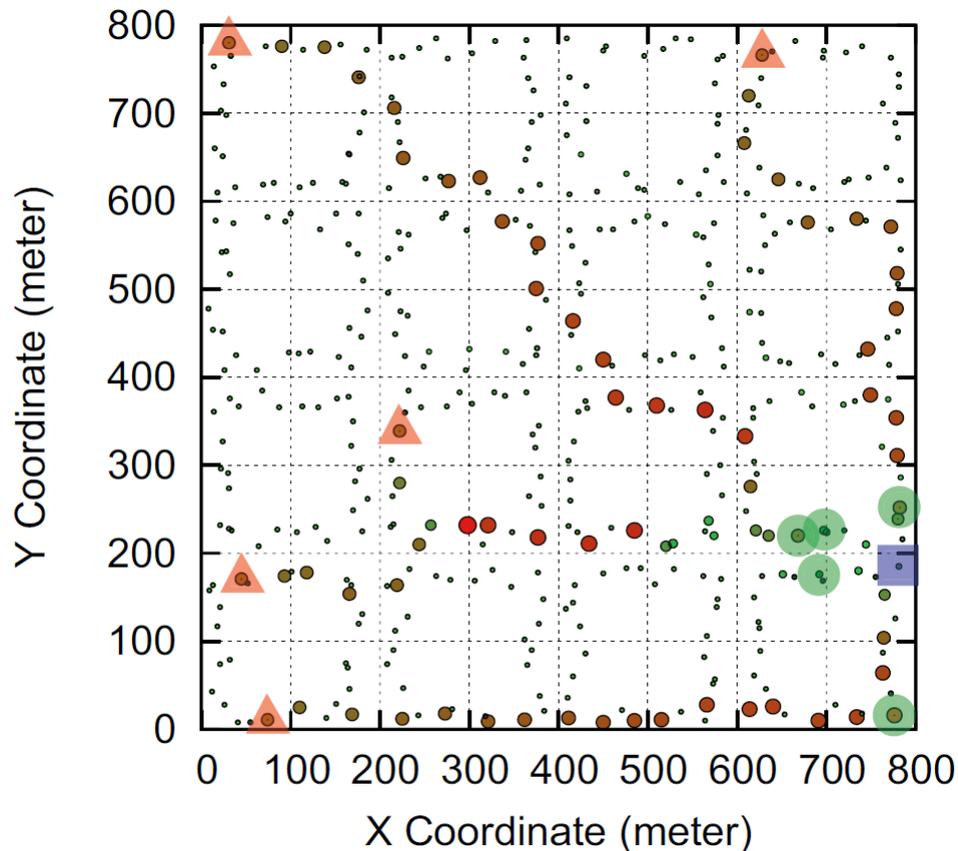
Journey of a packet in the system



DDoS Attack Using C12.22 Trace Service in AMI



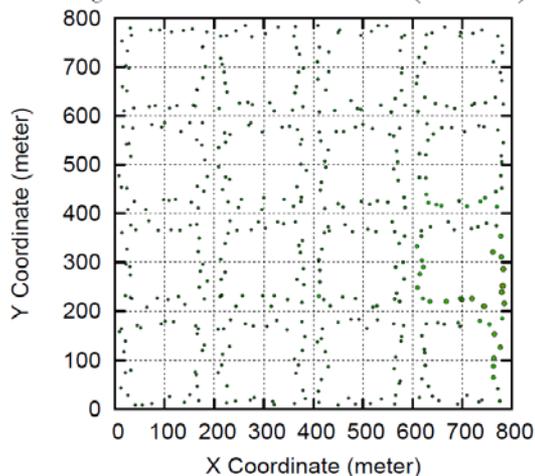
Attacking Experiment



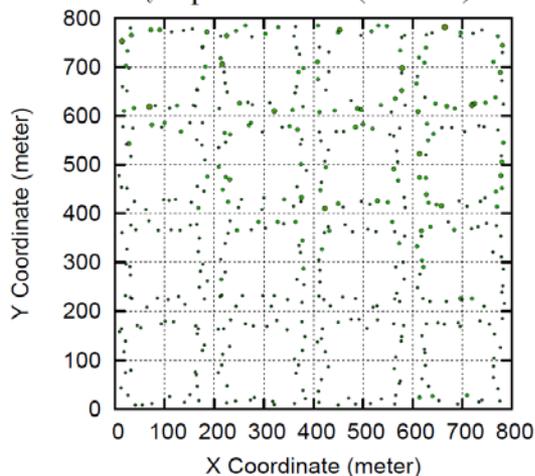
- 4x4 blocks, 448 meters
- 5 attackers
- Victim: the single egress point (meter gateway)
- ZigBee wireless network, 1 Mb/s bandwidth
- Normal traffic: 100-byte packet per 10 second
- Attacking traffic: 200 times faster, 15-30 hops

Experimental Results

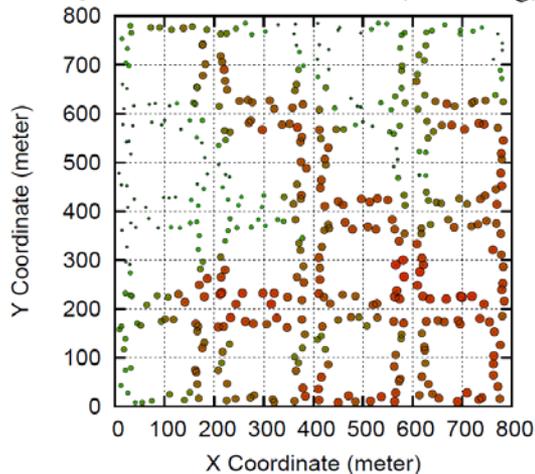
B1. r_c - channel contention (normal)



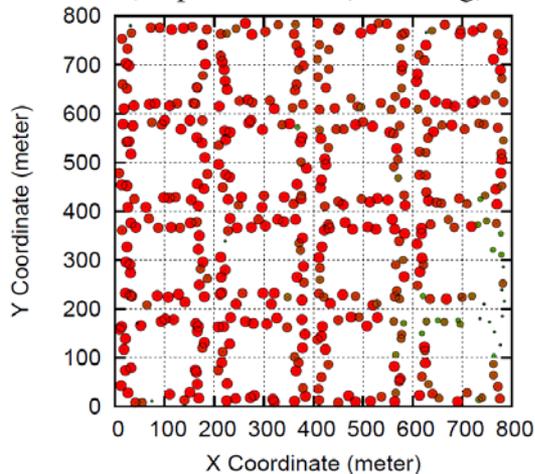
C1. r_l - packet loss (normal)



B2. r_c - channel contention (attacking)



C2. r_l - packet loss (attacking)



Summary

Security evaluation of AMI is importance, has challenges

Tools help! We're developing some

Next up:

- What to test
- How to test
- Experimental design