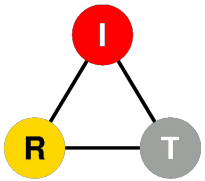
Talking After Lights Out: An Ad Hoc Network for Electric Grid Recovery

Jan Janak
with H. Retty, D. Chee, A. Baloian, H. Schulzrinne

Dept. of Computer Science
Columbia University



SmartGridComm21, Aachen, October 27, 2021

CS @CU

Talk Outline

1. Introduction
2. DARPA RADICS Program
3. Phoenix Secure Emergency Network (PhoenixSEN)
4. Experimental Evaluation
5. Summary and Q&A

Introduction

- Industrial control systems are increasingly targets of cyber attacks
  - May result in a large-scale electric power outage, a.k.a **blackout**
- Large-scale blackout recovery requires communication
  - Coordinate electricity supply and demand (SCADA or phone calls)
  - Incrementally add generating capacity and load
- U.S. grid operators often rely on ISPs for network services
  - Network connectivity difficult to guarantee during blackout

Network-based cyber attacks may actively thwart or delay power restoration

DARPA RADICS Program

"RADICS program delivers novel technologies, custom testbed, and evaluation exercises to enable utilities and first responders to quickly restore critical infrastructure amidst a cyberattack"

- 2016 - 2020
- Develop tools for:
  - cybersecurity personnel
  - grid operators and utilities
  - first responders
- Enable blackstart recovery during a cyberattack
- Without relying on external resources (including power and communication)

Field exercise at Plum Island, NY

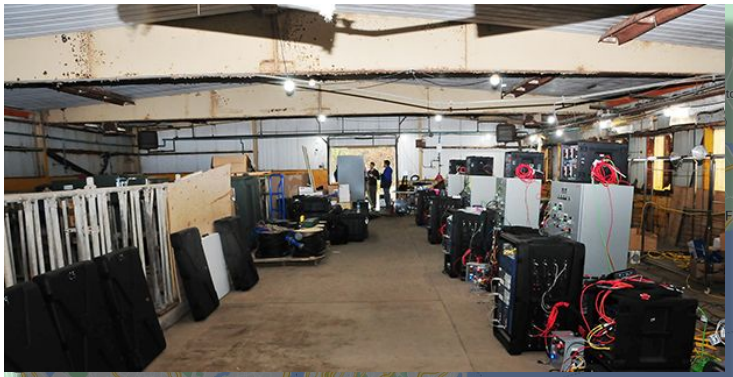
Source: https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

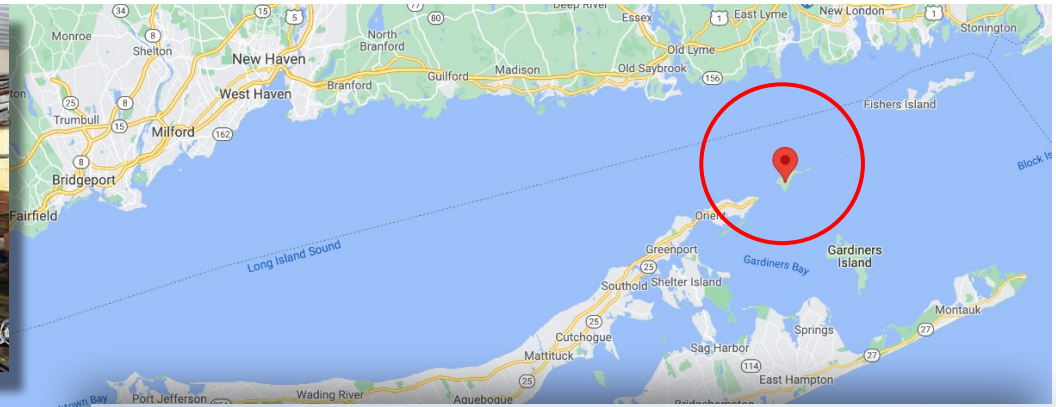
DARPA RADICS Program (continued)

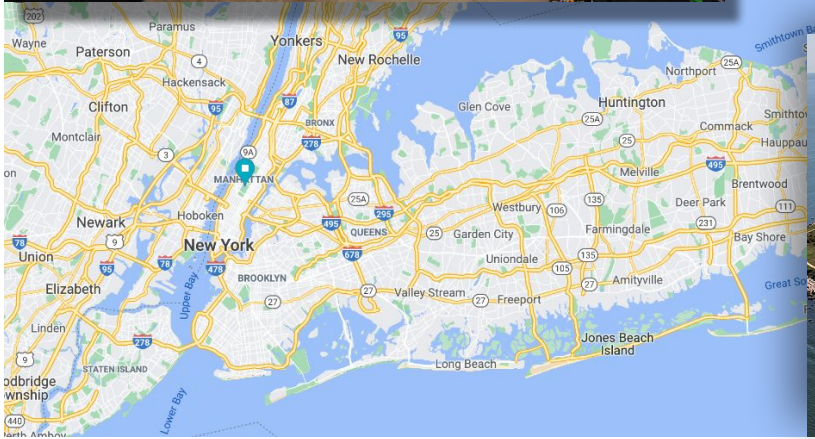
- Joint government, academia, and industry effort led by DARPA
- Custom testbed to replicate real-world conditions
  - designed around commonly deployed systems in North America
  - multi-utility grid infrastructure
  - miniaturized substations (substation-in-a-box), RTO/ISO, power lines, data networks
- Field exercises on Plum Island, NY every six month (7 in total)
  - volunteers from the energy sector recruited by the U.S. DOE
  - learn to respond to simulated attacks
- Grid restoration technology (tools for the energy sector & first responders)

Source: https://www.darpa.mil/news-events/2021-02-23

RADICS Field Exercises on Plum Island, NY

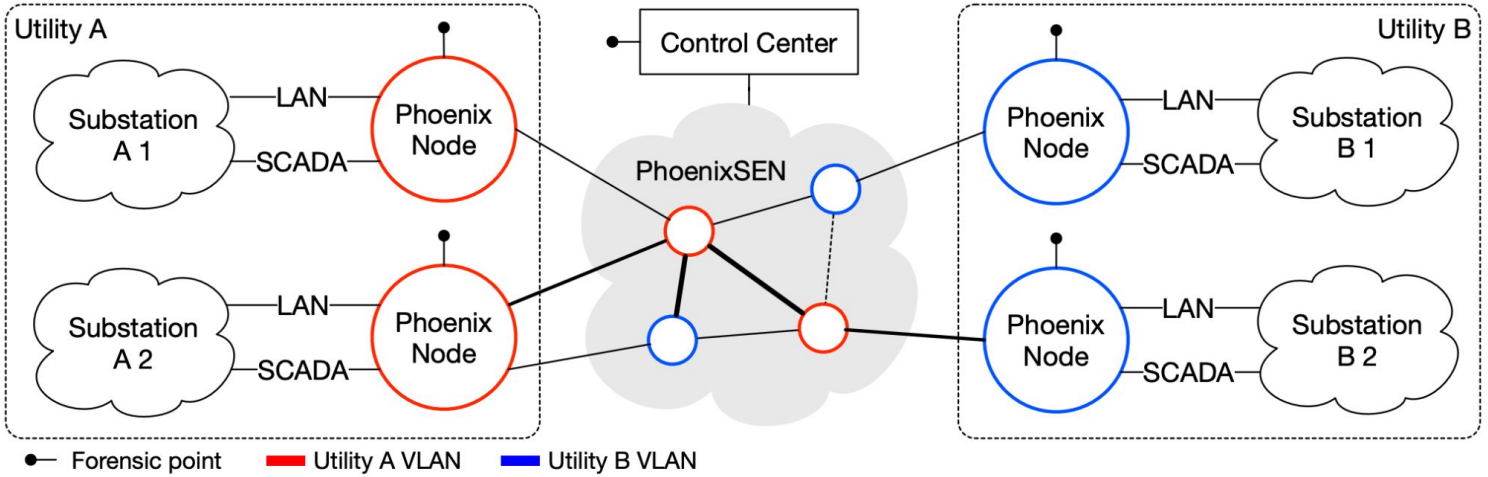






Phoenix Secure Emergency Network (PhoenixSEN)

- Uniform node architecture
- Deployable after blackout
- Built-in services for the grid
- Ad hoc backup network for blackstart
- hybrid, isolated (virtualized), self-forming
- drop-in replacement for ISP networks



PhoenixSEN Prototype

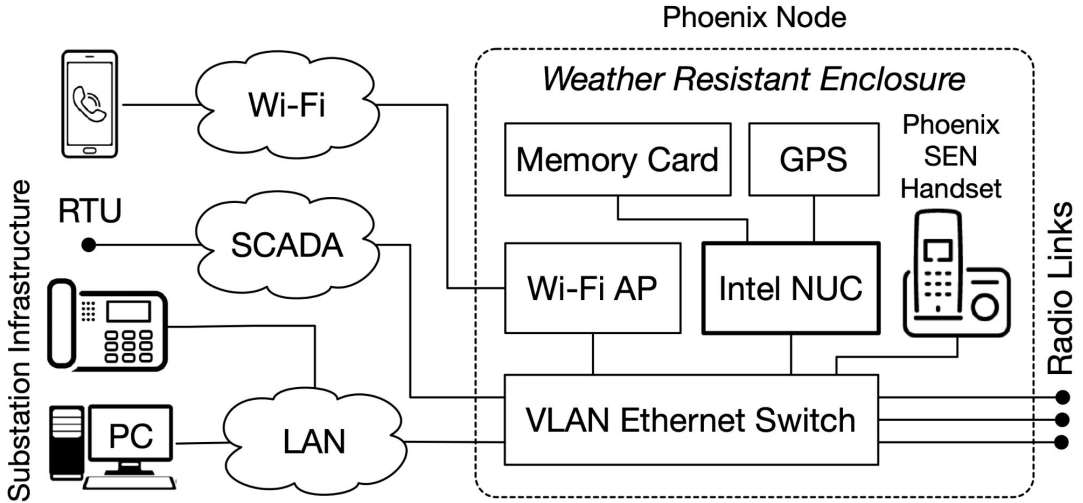
Prototype evaluated during live field exercises

PhoenixSEN node detail

Photo credit: Hema Retty (BAE Systems)

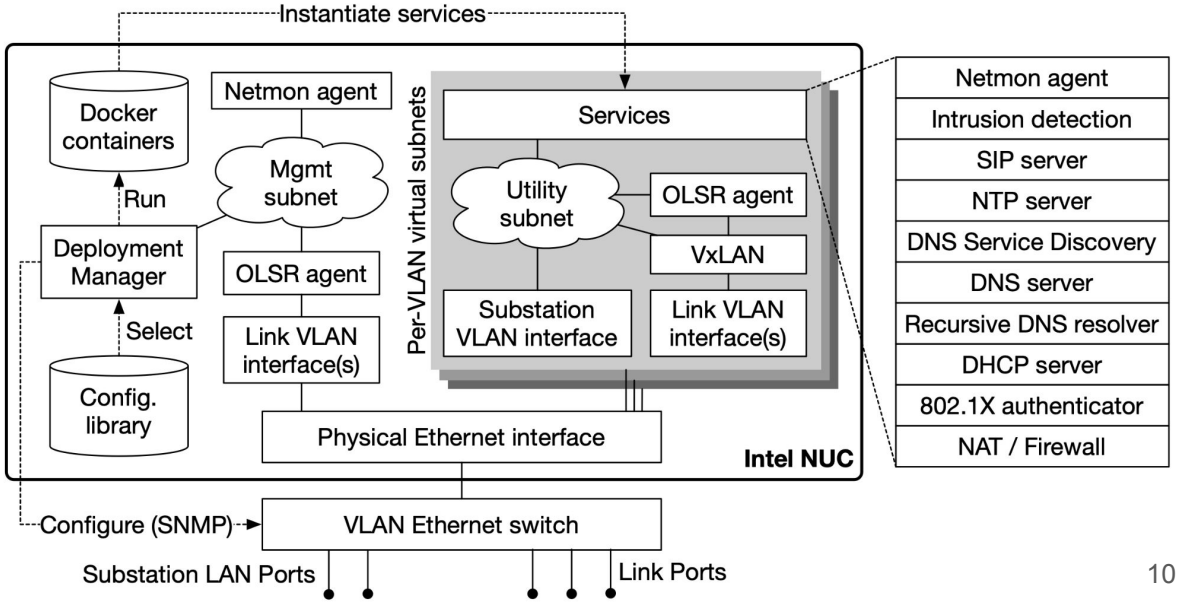
PhoenixSEN Node Hardware Architecture

- Uniform HW/SW architecture to simplify blackout field deployments
- Isolated VLANs for SCADA, backend (IT), and VoIP systems
- Pre-configured VoIP client
- 4 radio link ports
- Weather resistant box
- Integrated battery & backup



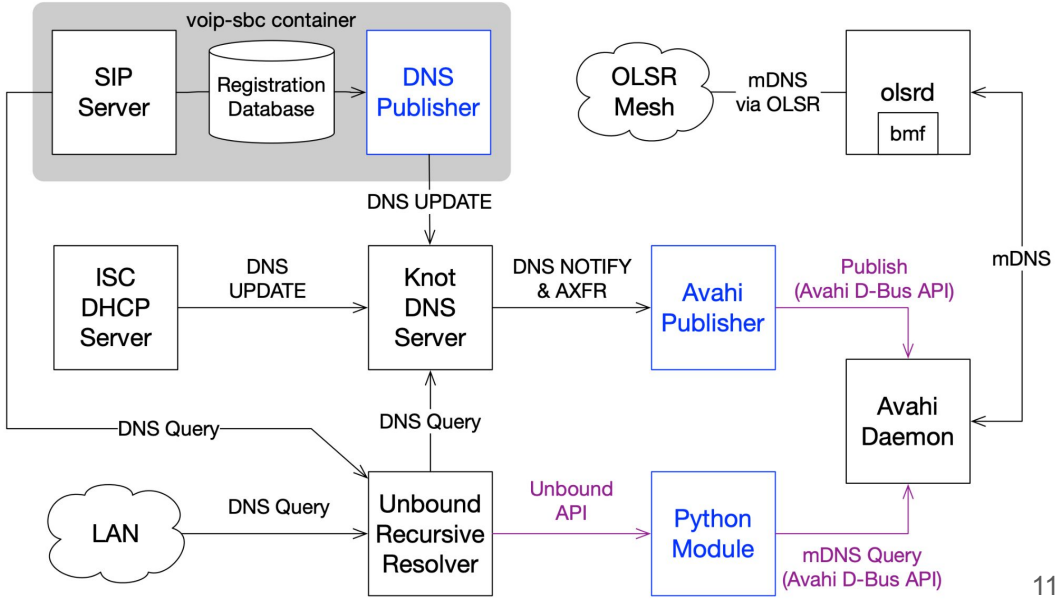
PhoenixSEN Node Software Architecture

- Virtual (per-VLAN) network services (emulate target ISP)
- Little deployment configuration, remote configuration from the CC
- Network services:
  - Decentralized VoIP
  - Intrusion detection
  - Integrated monitoring



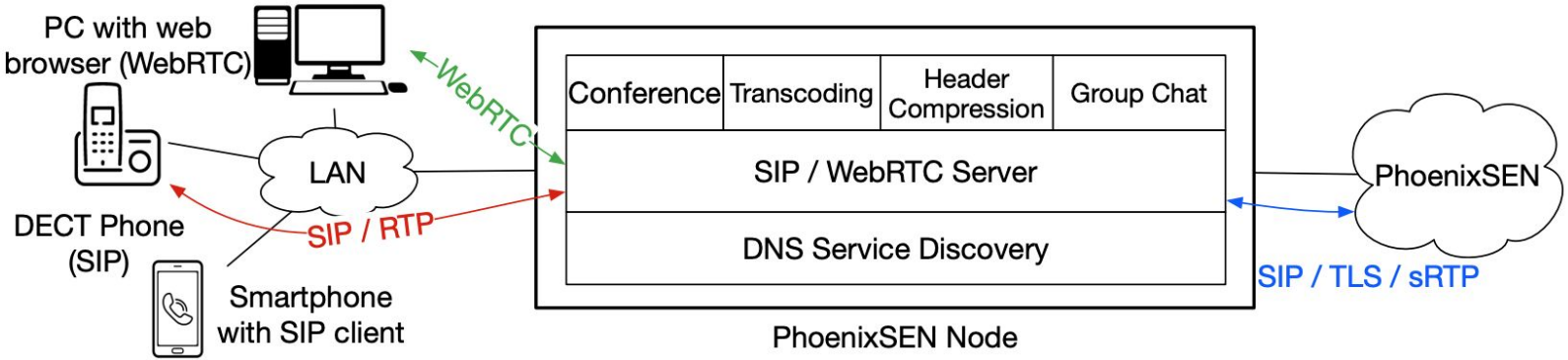
PhoenixSEN Naming and Service Discovery

- Network-wide naming and service discovery
- Multicast DNS with dissemination via OLSR spanning tree
- DNS is widely supported
- No single point of failure
- Used by other services (VoIP)



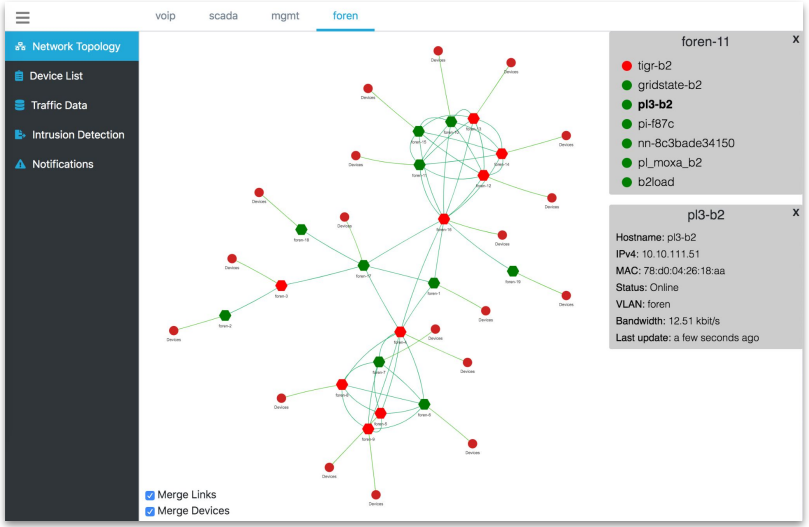
PhoenixSEN Decentralized VoIP Service

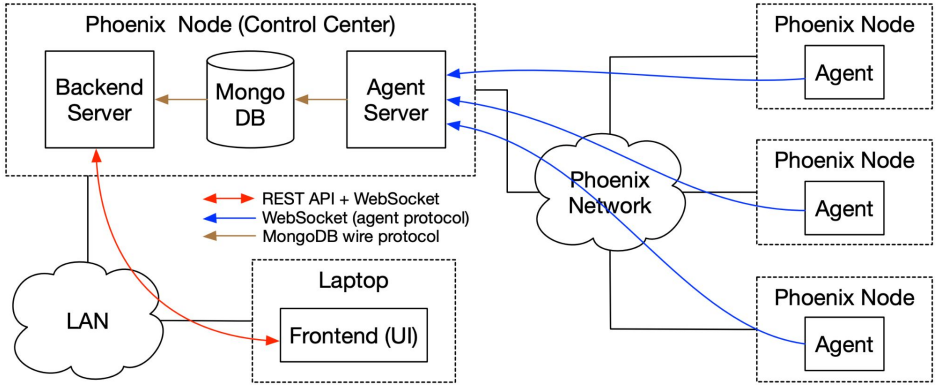
- Voice communication critical for blackstart according to NERC
- PhoenixSEN provides decentralized (p2p) VoIP service
- Compatible with substation VoIP infrastructure
- Compressed, encrypted, authenticated over untrusted links
- Dynamic conference + group chat (with tamper-resistant log)

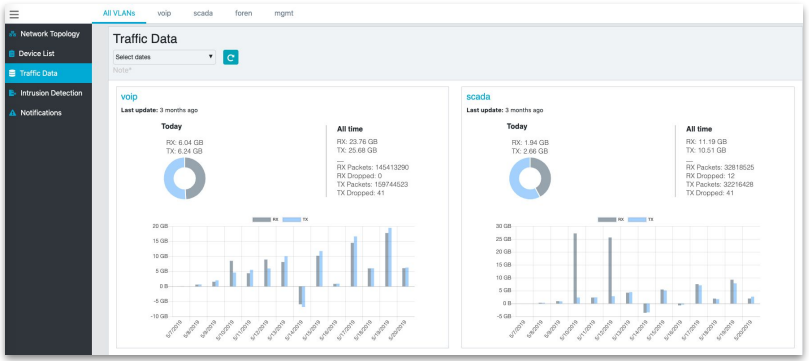


PhoenixSEN Network Monitoring

- Situation awareness via in-situ monitoring
- SCADA device discovery via active probing
- Time-traveling debugging for post-mortem analysis
- https://github.com/irtlab/netmon





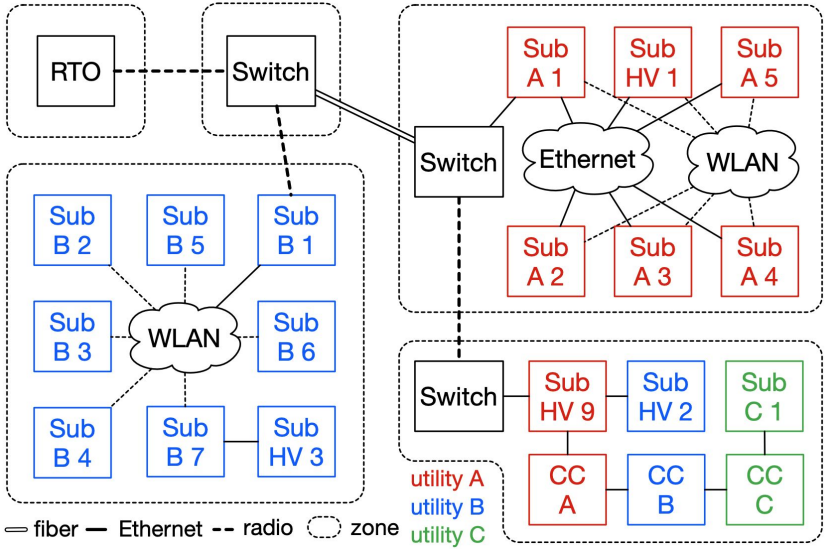


Experimental Evaluation

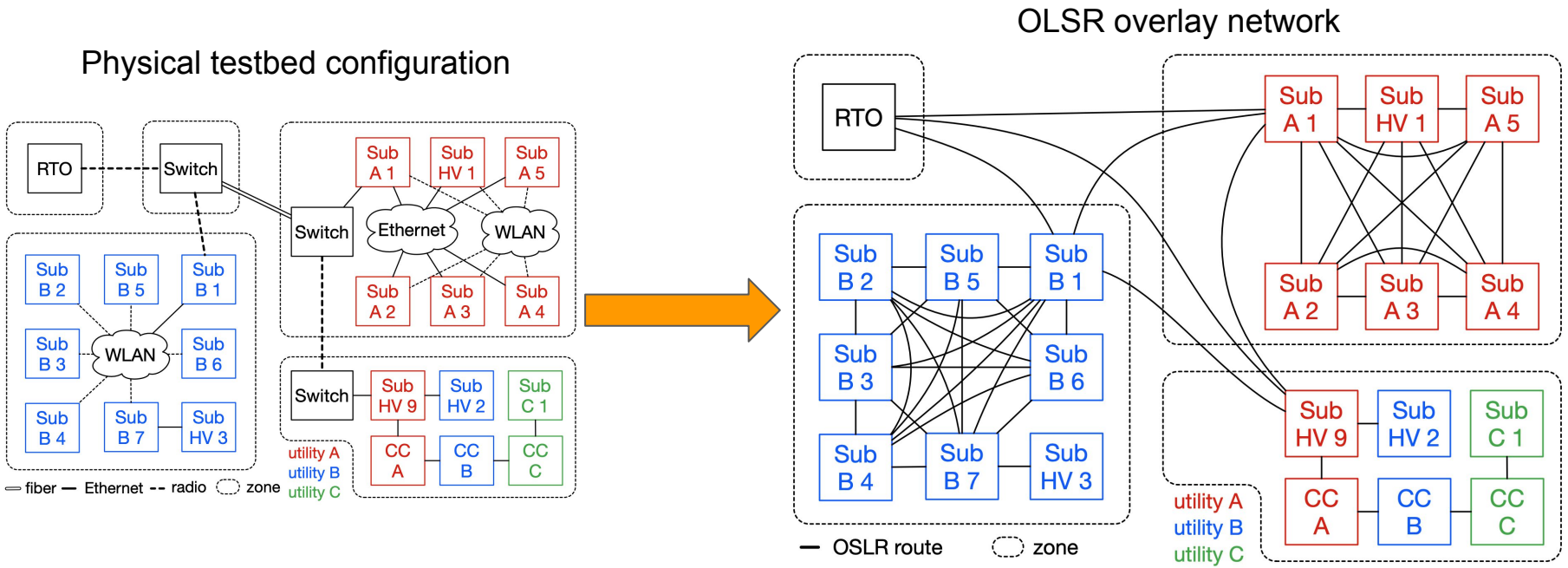
Plum Island testbed parameters and block diagram during the 6th (largest) field exercise

TABLE I
CONFIGURATION OF DARPA RADICS EXERCISE 6 NETWORK

Grid parameters	Utility A	Utility B	Utility C
Control centers (CC)	1	1	1
Substations	5	7	1
High voltage (HV) substations	2	2	0
RTOs	1 (shared across utilities)		
Maximum RTO-substation distance	5 links		
PhoenixSEN parameters	**SCADA**	**VoIP**	**Forensic**
Connected devices	33	69	265
PhoenixSEN nodes	21 (shared across VLANs)		
Physical links per node	min: 1, max: 3		
OLSR Routes per node	min: 1, average: 5, max: 9		
Inter-utility relay nodes	3 (HV 9, CC A, CC B)		
OLSR network diameter	6 (all VLANs)		

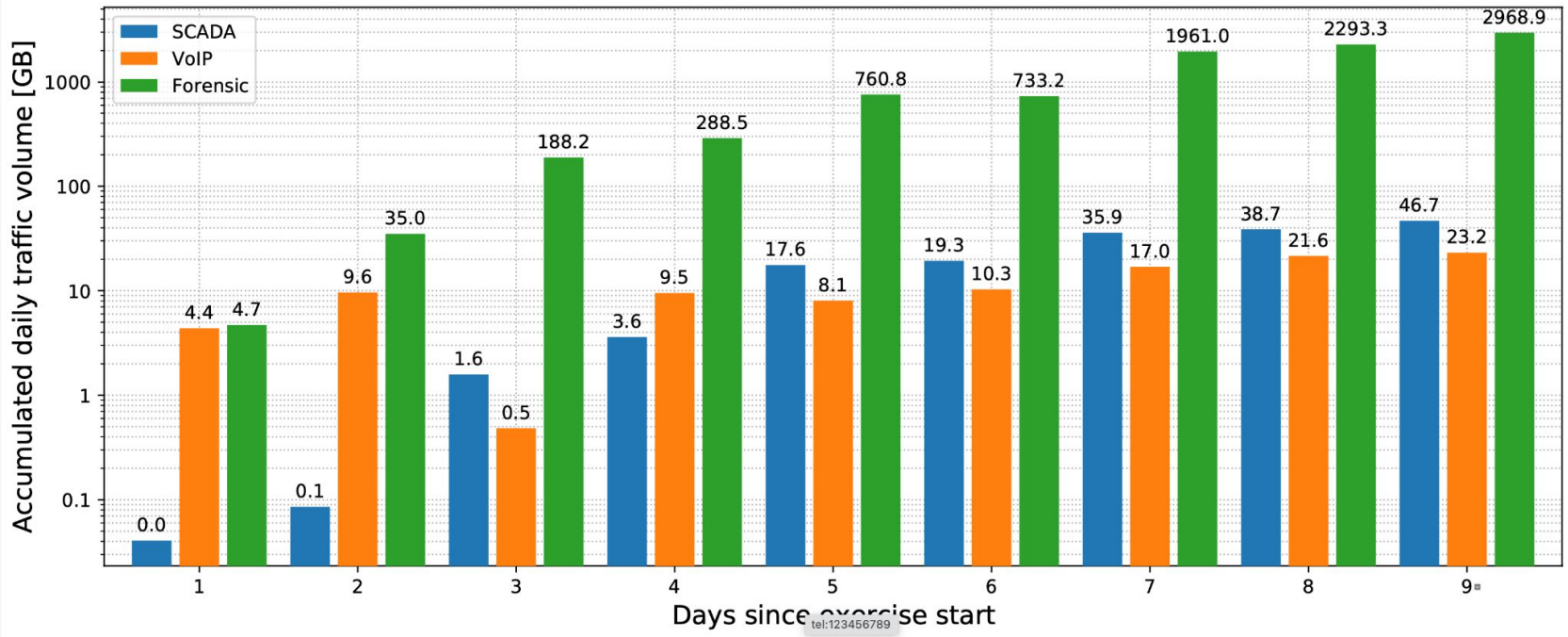


Experimental Evaluation: Overlay Architecture



Methodology: Connectivity and convergence time evaluated through artificial testbed disruptions

Experimental Evaluation: Traffic Volumes



Peak: ~250 devices transferred ~3 TB of data per day over a network of 21 PhoenixSEN nodes.
Network load during blackstart recovery was dominated by forensic/security activities.

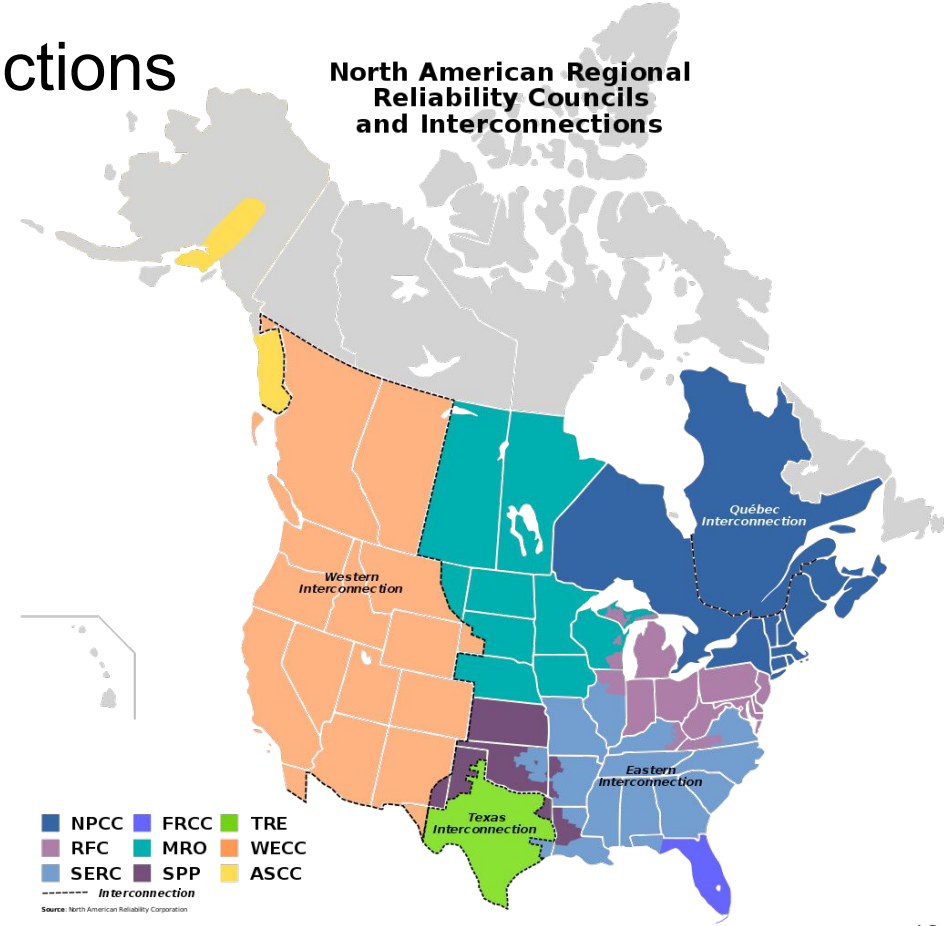
Summary

- Network-based attacks pose risk for the grid and may result in a blackout
- ISP networks are likely to be severely affected, but critical for blackstart
- DARPA RADICS: tools, testbed, and field exercises for blackstart recovery
- PhoenixSEN: Ad hoc backup network architecture for blackstart
- Experimental evaluation in field exercises on Plum Island, NY

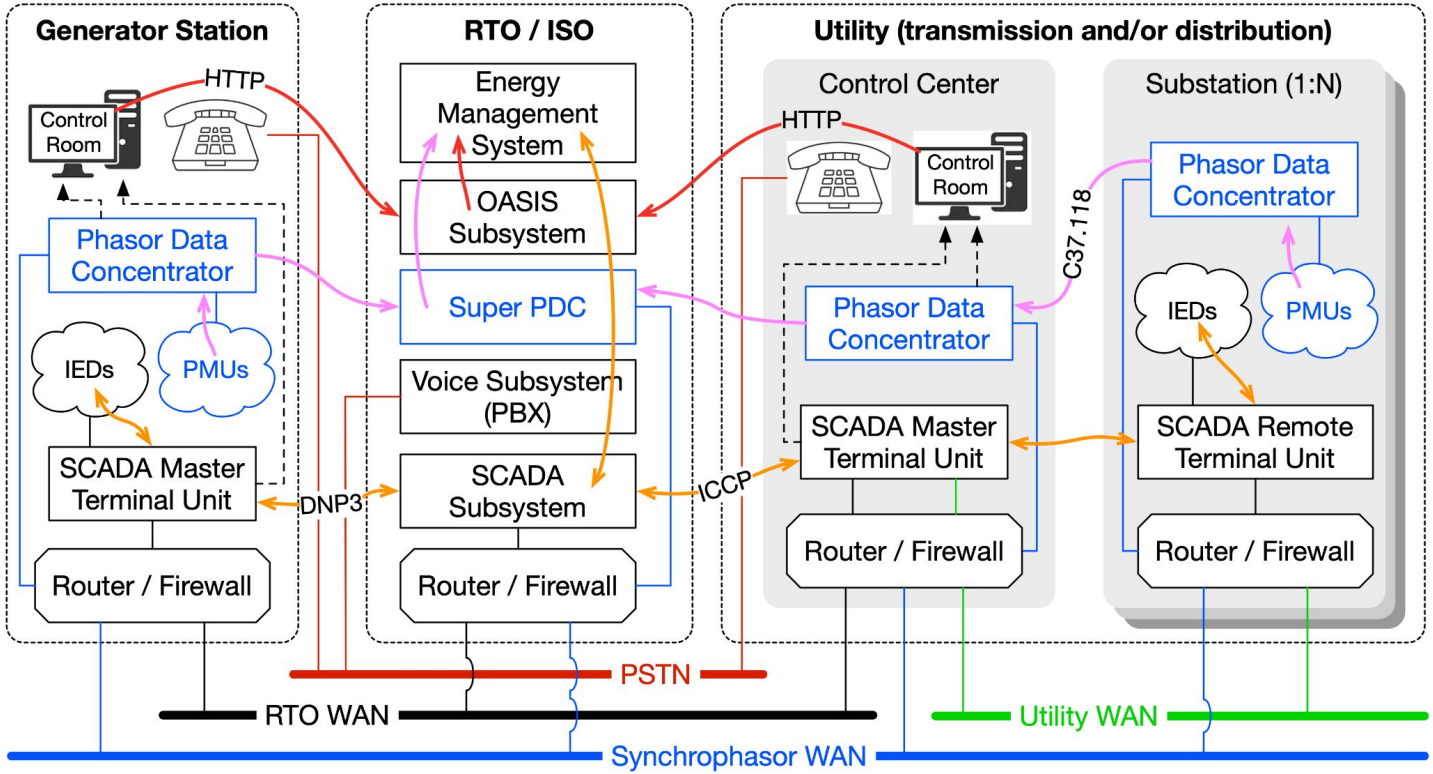
Longer arXiv paper version: https://arxiv.org/abs/2102.05870

Backup: U.S Grid Interconnections

- Western Interconnection
- Eastern Interconnection
- Texas Interconnection



Backup: U.S. Electrical Grid Networking Subsystem



Backup: Open Source PhoenixSEN Components

1. DNS-based service discovery and naming subsystem

   https://github.com/janakj/dns2avahi

2. SIP-based group chat server for DARPA RADICS exercises

   https://github.com/janakj/groupchat

3. Auto-provisioning server for SIP phones

   https://github.com/janakj/autoprov

4. Network monitoring tool for cyber-physical systems

   https://github.com/irtlab/netmon