Spire: Intrusion-Tolerant SCADA for the Power Grid

Yair Amir, Amy Babay, Sam Beckley
Johns Hopkins University, Computer Science

John Schultz
Spread Concepts LLC

Spread Concepts

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Distributed Systems
and Networks Lab
www.dsn.jhu.edu

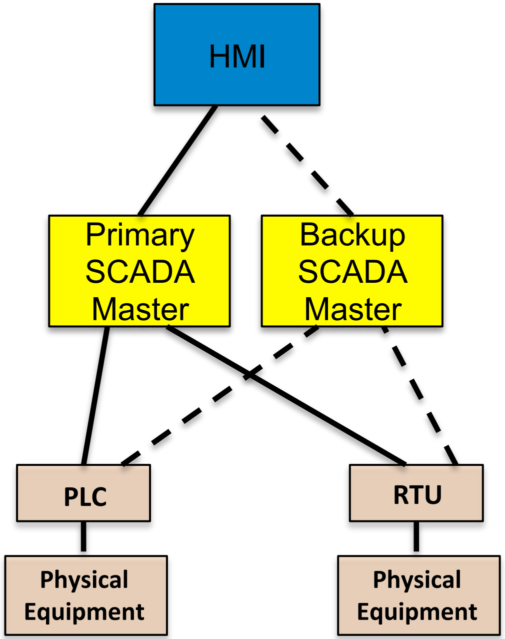
SCADA Migrating to IP Networks

- Traditional SCADA systems ran on proprietary networks
  - Created air gap from outside world and attackers
- Cost benefits and ubiquity of IP networks are driving SCADA to use IP networks
  - Exposes SCADA to hostile environments, removing the air gap
- Raises additional concerns because SCADA systems are:
  - In service for decades
  - Running legacy code with well-known exploits
  - Increasingly becoming a target for attackers
- Stuxnet (2010)
  - First sophisticated SCADA attack in the wild targeting ICS

SCADA is Vulnerable on Several Fronts

The move to IP makes SCADA vulnerable on several fronts:

- SCADA system compromises
  - SCADA Master – system-wide damage
  - RTUs, PLCs – limited local effects
  - HMIs
- Network level attacks
  - Routing attacks that disrupt or delay communication
  - Isolating critical components from the rest of the network

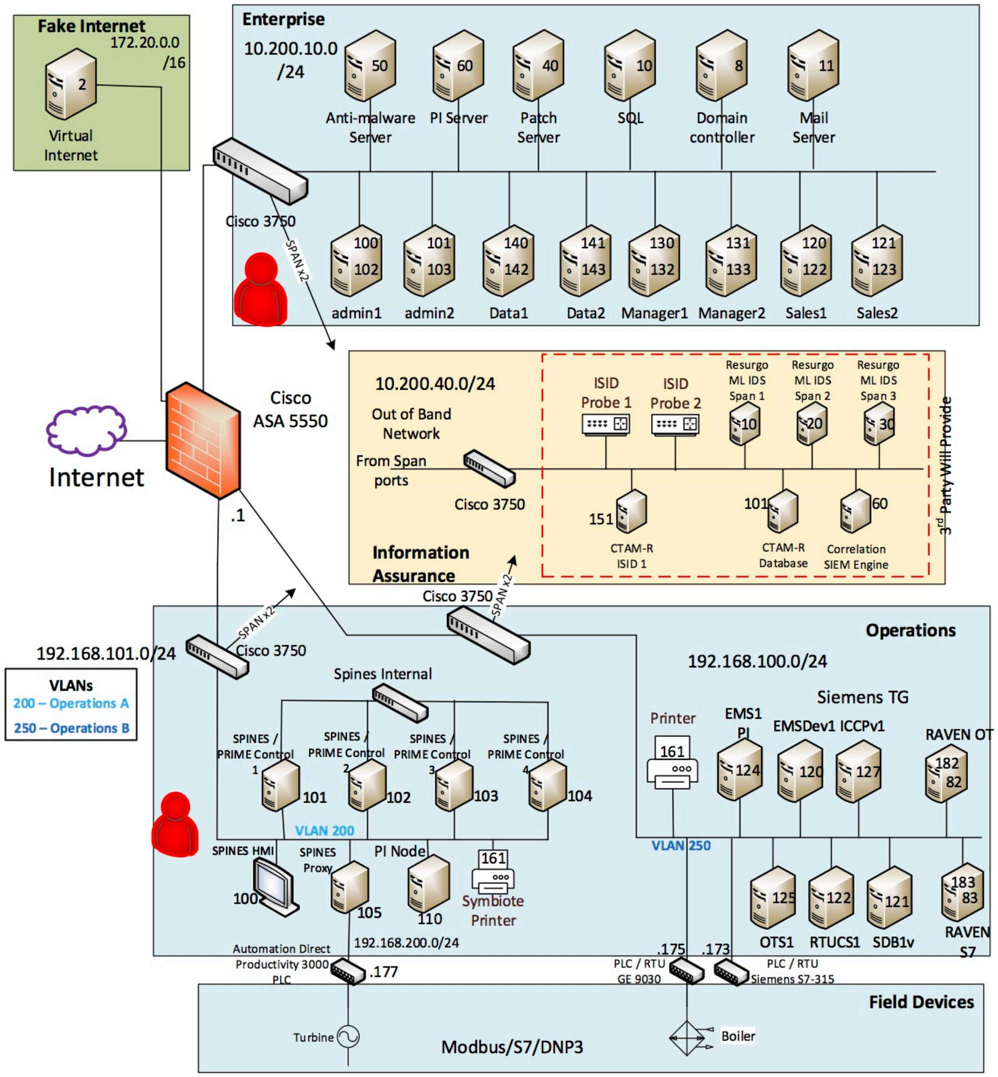


Spire

- Spire is an intrusion-tolerant SCADA system for the power grid: it continues to work even if some critical components have been compromised
- Intrusion tolerance as the core design principle:
  - Intrusion-tolerant network
  - Intrusion-tolerant consistent state
  - Intrusion-tolerant SCADA Master
- Open Source - http://dsn.jhu.edu/spire

DoD ESTCP Results

- NIST-compliant system completely taken over
  - MITM attack from corporate network
  - Direct access to PLC from operational network
- Spire completely unaffected
  - Attacks in corporate and operational network
  - Given complete access to a replica and code
  - Red team gave up after several days



Defense Across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress

Defense Across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
- What prevents an attacker from reusing the same exploit to compromise more than f replicas?

Defense Across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine

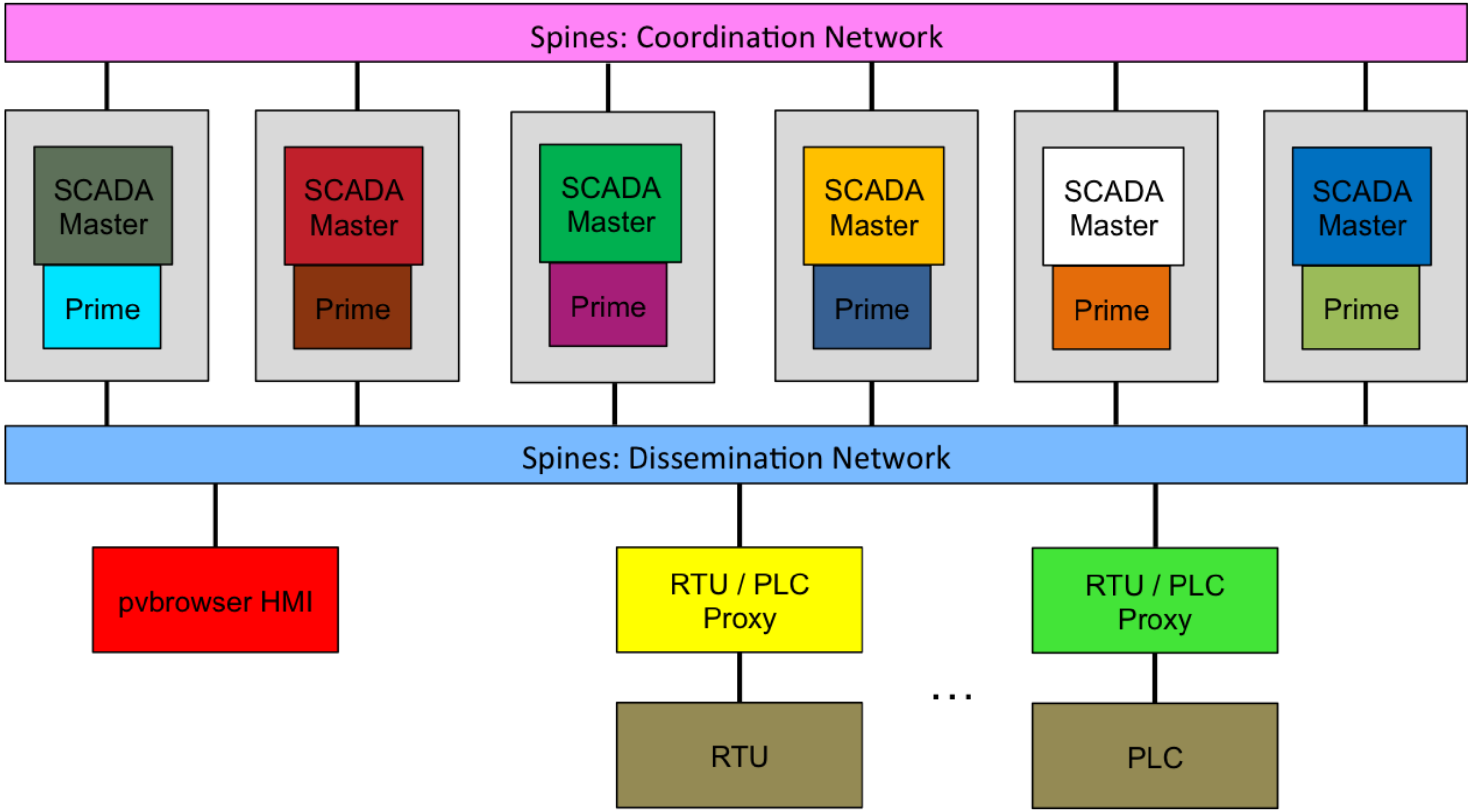
Defense Across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine
- What prevents an attacker from compromising more than f replicas over time?

Defense Across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine
- Proactive Recovery
  - Periodically rejuvenate replicas to a known good state to cleanse any potentially undetected intrusions
  - 3f+2k+1 replicas needed to simultaneously tolerate up to f intrusions and k recovering replicas
  - 2f+k+1 connected correct replicas required to make progress

Spire Architecture: Single Control Center

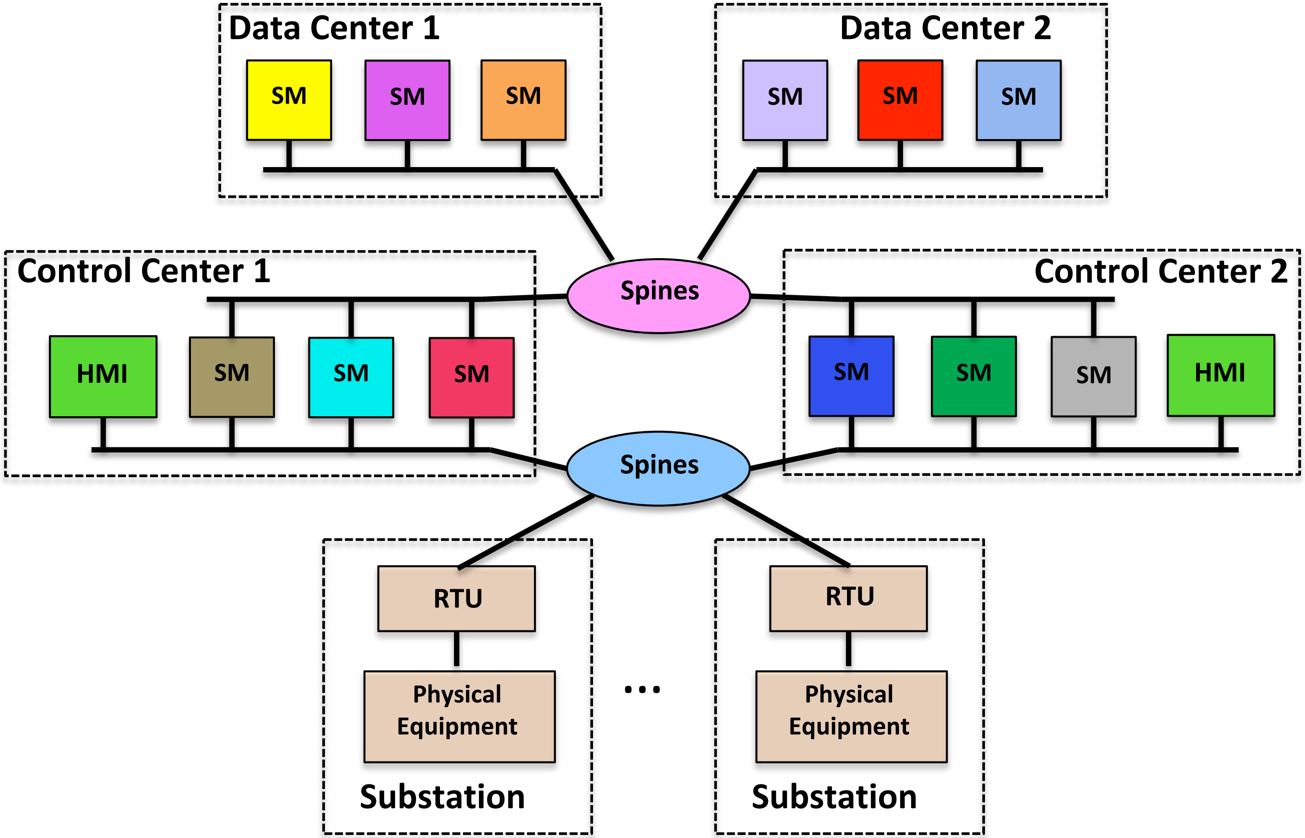


Beyond a Single Site

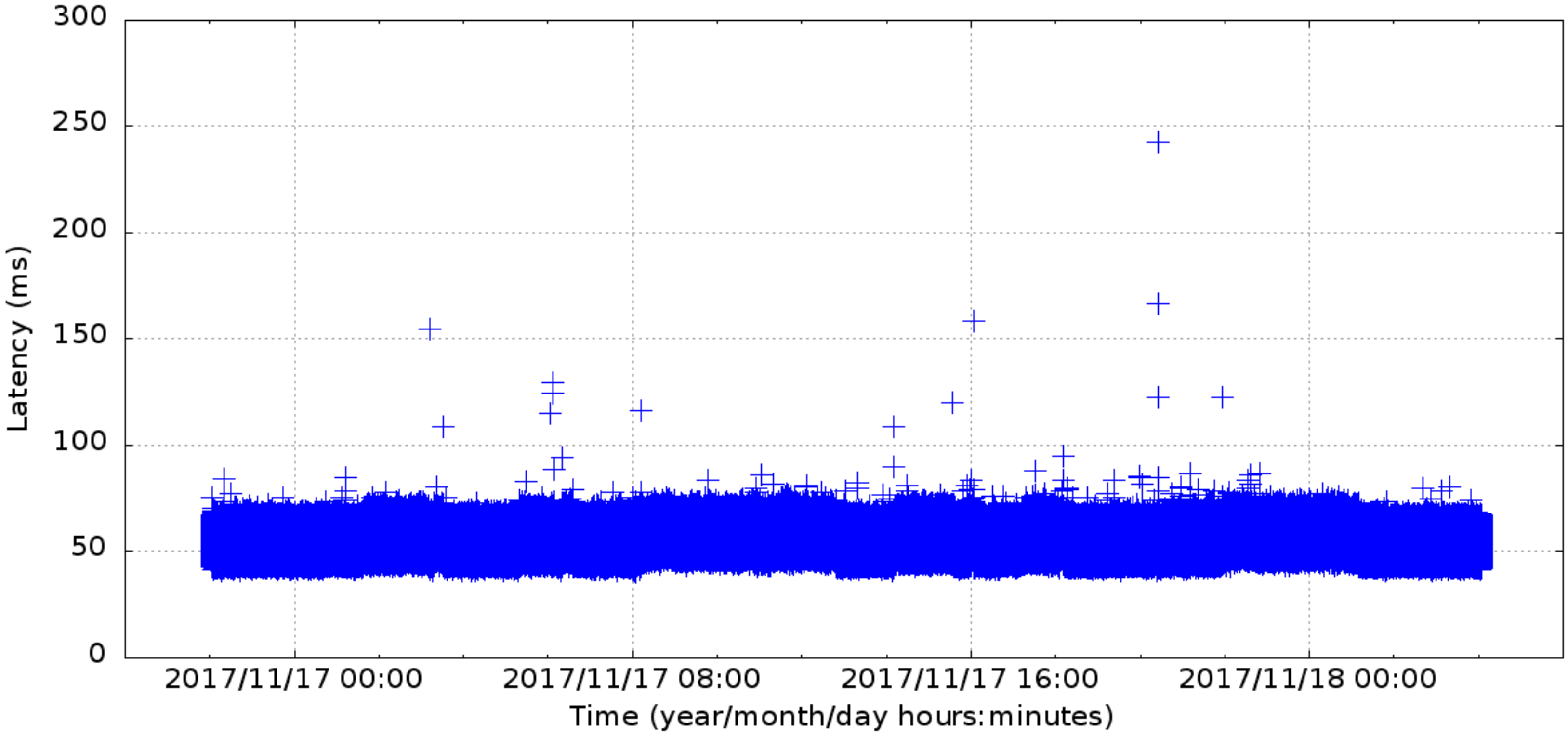
- To protect against sophisticated network attacks, Spire supports multiple control sites
- Since it is expensive to construct control sites, Spire is able to operate with two control sites plus additional sites that can be served by commodity data centers (that lack the ability to communicate with RTUs and PLCs in the field)

Novel Resilient Configuration

3+3+3+3 (progress: 7)

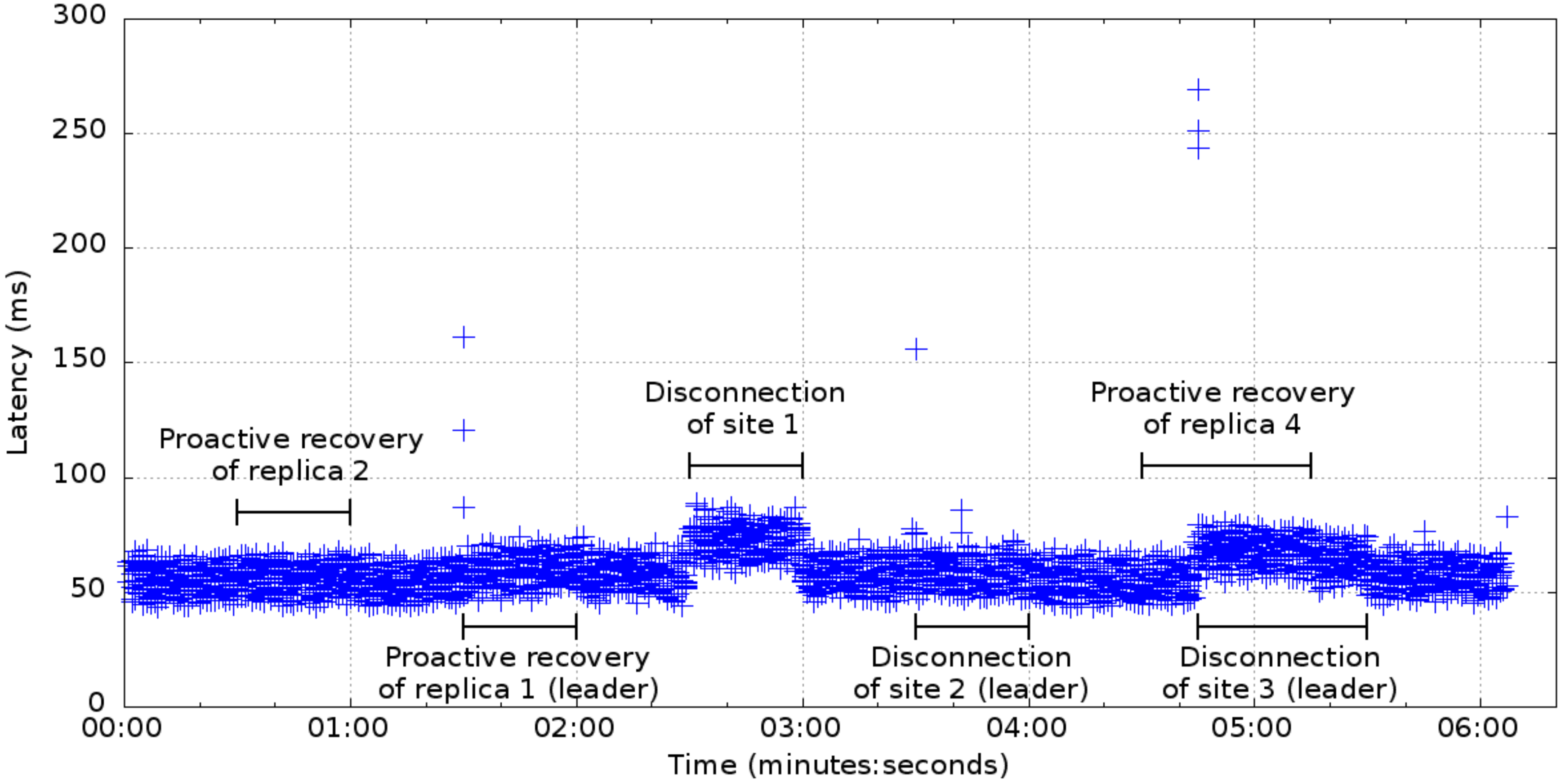


Wide Area Update Latency Plot



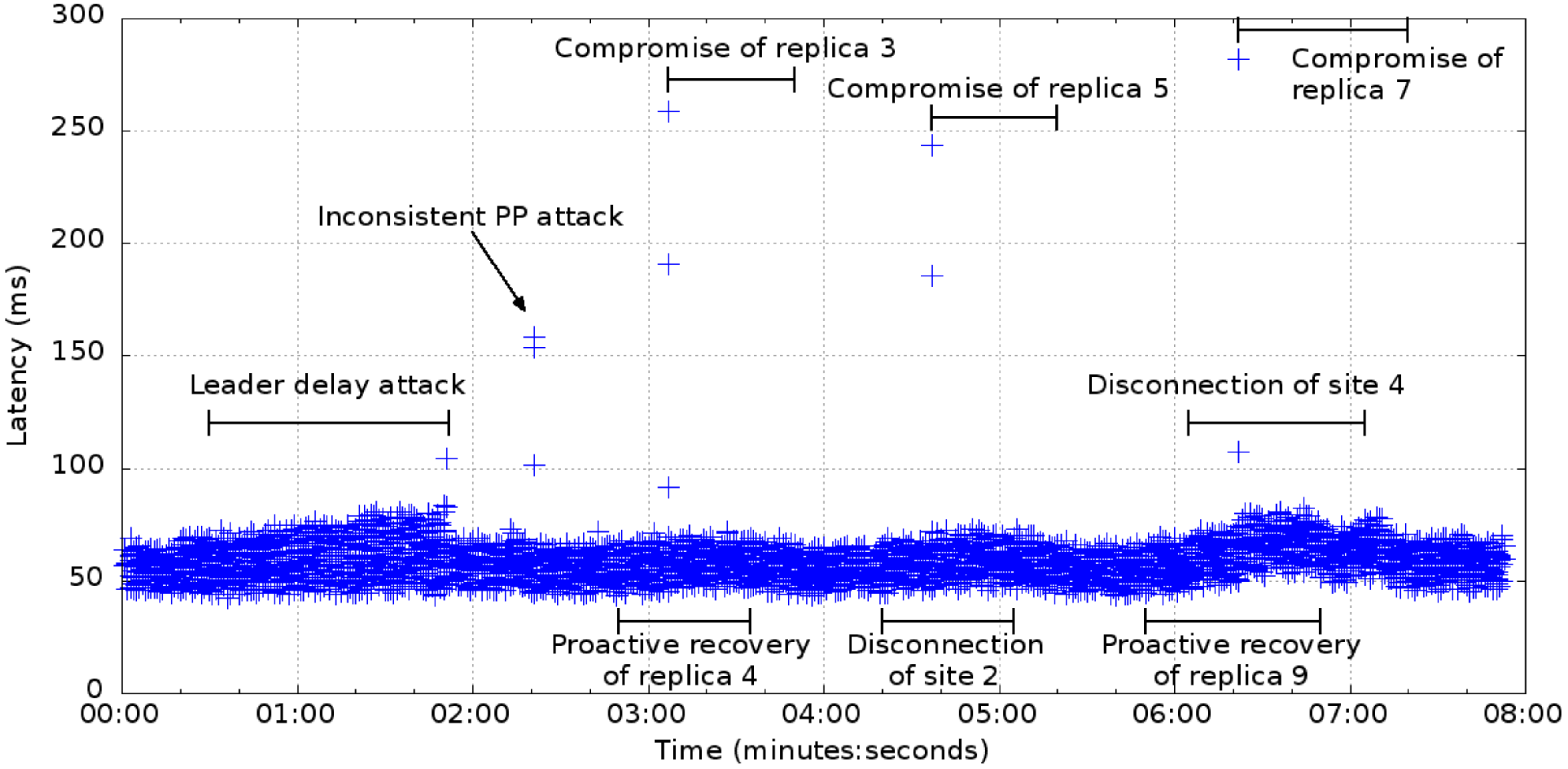
- 30-hour wide-area deployment of configuration 3+3+3+3
    - Control centers at JHU and SVG, data centers at WAS and NYC
    - 10 emulated substations sending periodic updates
    - 1.08 million updates (108K from each substation)
    - Nearly 99.999% of updates delivered within 100ms (56.5ms average)

Wide Area: Latency Under Attack



- Targeted attacks designed to disrupt the system
  - All combinations of site disconnection (due to network attack) + proactive recovery

Wide Area: Latency Under Attack



- Targeted attacks designed to disrupt the system
  - All combinations of intrusion + site disconnection (due to network attack) + proactive recovery

The Spire Forum

- Forum focused on open source intrusion-tolerant control systems for the power grid
- Please join the Spire forum if interested
- http://dsn.jhu.edu/spire

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Distributed Systems
and Networks Lab