U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Himanshu Khurana

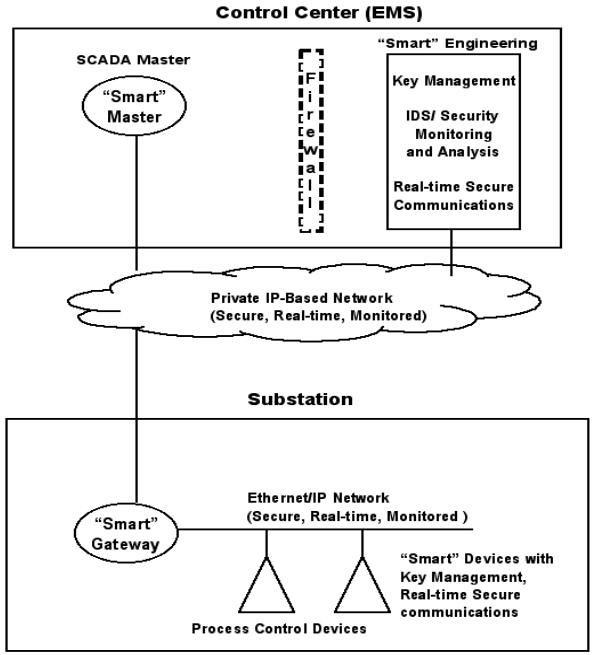
University of Illinois

TCIPG: Converged Networks for SCADA

(Joint work with Erich Heine and Tim Yardley)

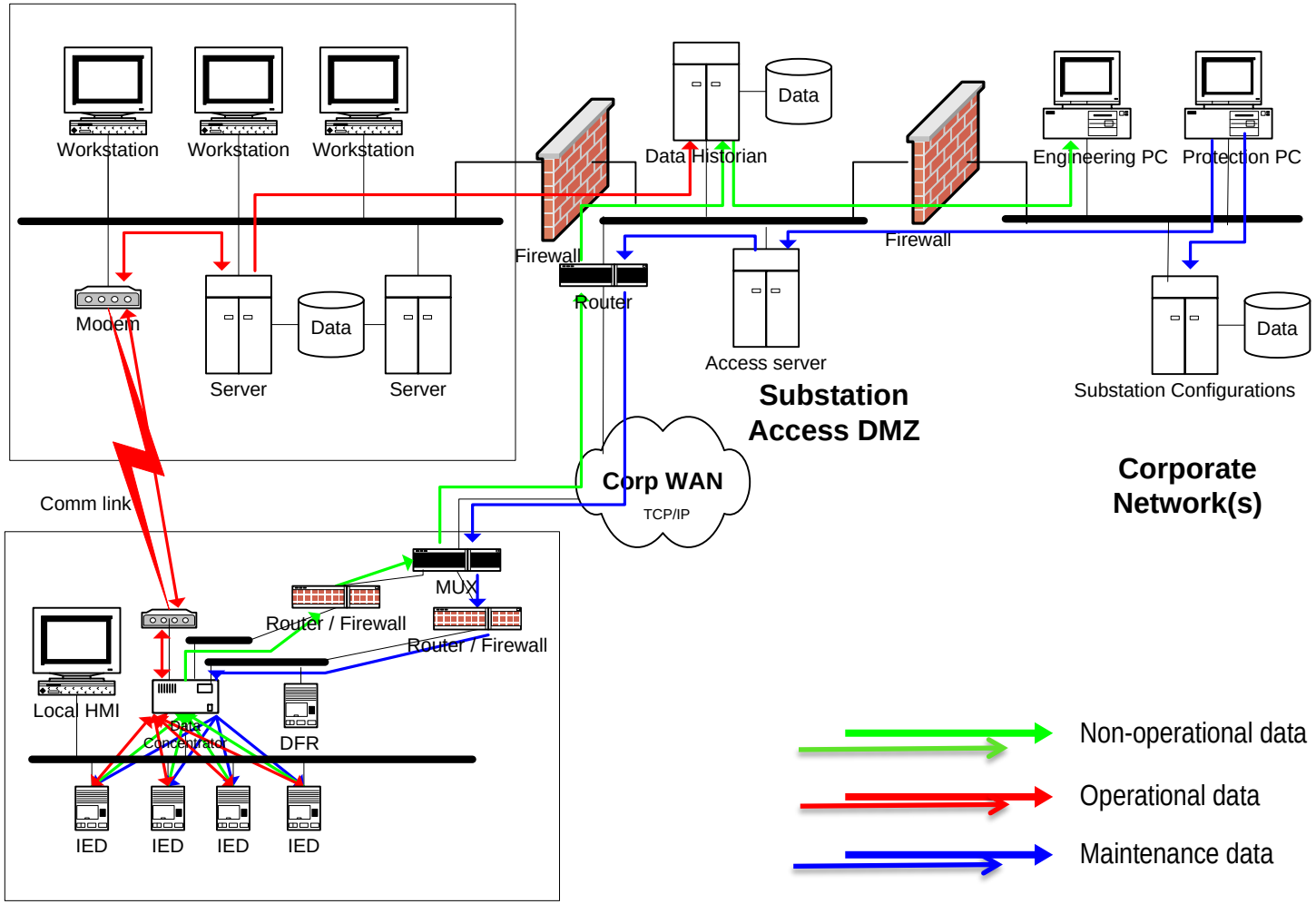
Summary Slide: CONES

- **Outcomes:** Specify and create an architecture and platform for maintaining real-time and secure communications for control in a converged network.
- **Roadmap Challenge:** Develop and Integrate Protective Measures
- **Major Successes:** CONES enhanced machines outperform non-enhanced machines in representative scenarios; major real-time constraints met.



- **Schedule:** Started 2/8, Design 8/8, Prototype 7/9, Experiments 4/10, Transitioned to TCIPG 2/10
- **Level of Effort:** $250k DOE and TCIPG Funding
- **Funds Remaining:** TCIPG Funding
- **Performers:** University of Illinois
- **Partners:** PNNL

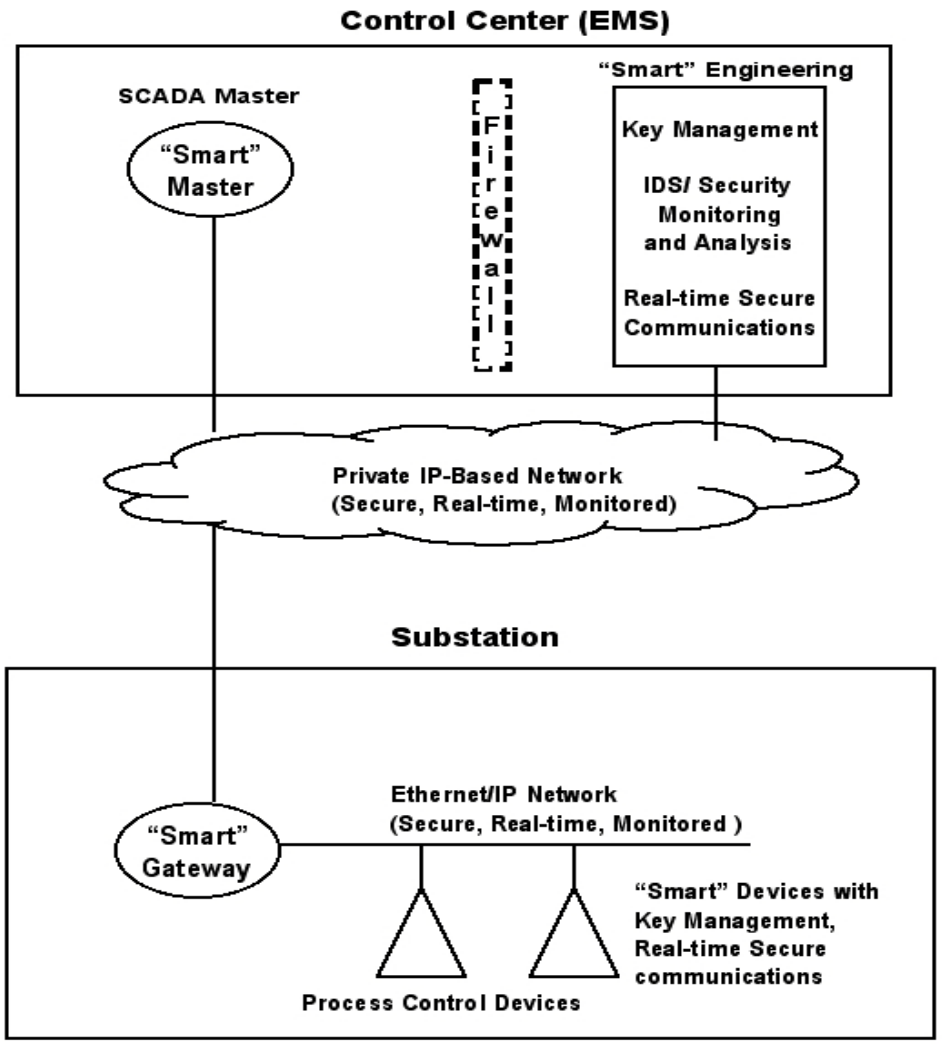
Background: Control Systems networks today



Source: Scott Mix Lecture 04/07

Research Problem

- Objective: Enable network convergence for Control system applications
  - Multiple traffic paradigms
    - SCADA and other control
    - Monitoring
    - Engineering
    - Enterprise
  - Understand and support communications requirements/properties for existing and emerging applications



Research Challenges

- Technical Challenges:
  - Resource management
    - Quality of Service, Real-time scheduling, Wide area network optimization
  - Security
    - Access control, Integrity, Availability
- Development and Integration challenges
  - Use commercial, off-the-shelf platforms and tools
  - Minimal use of custom software
  - Support legacy devices and applications
  - Support existing and emerging applications

Technical Approach and Feasibility

- **Research Approach**
  - Gather requirements with industry input
  - Establish SCADA emulation environment
  - Prototype real-time middleware to support network convergence
  - Evaluate performance in representative scenarios
- **Design and Development approach**
  - Real-time, Secure Middleware for timeliness and availability
  - Real-time: support tight timing guarantees
    - CPU scheduling, Network scheduling
  - Middleware:
    - Common API for all systems
    - Coordinate multiple resource management component
    - Dynamic re-prioritization of QoS policies
  - Secure: Access Control, Integrity (Future work)

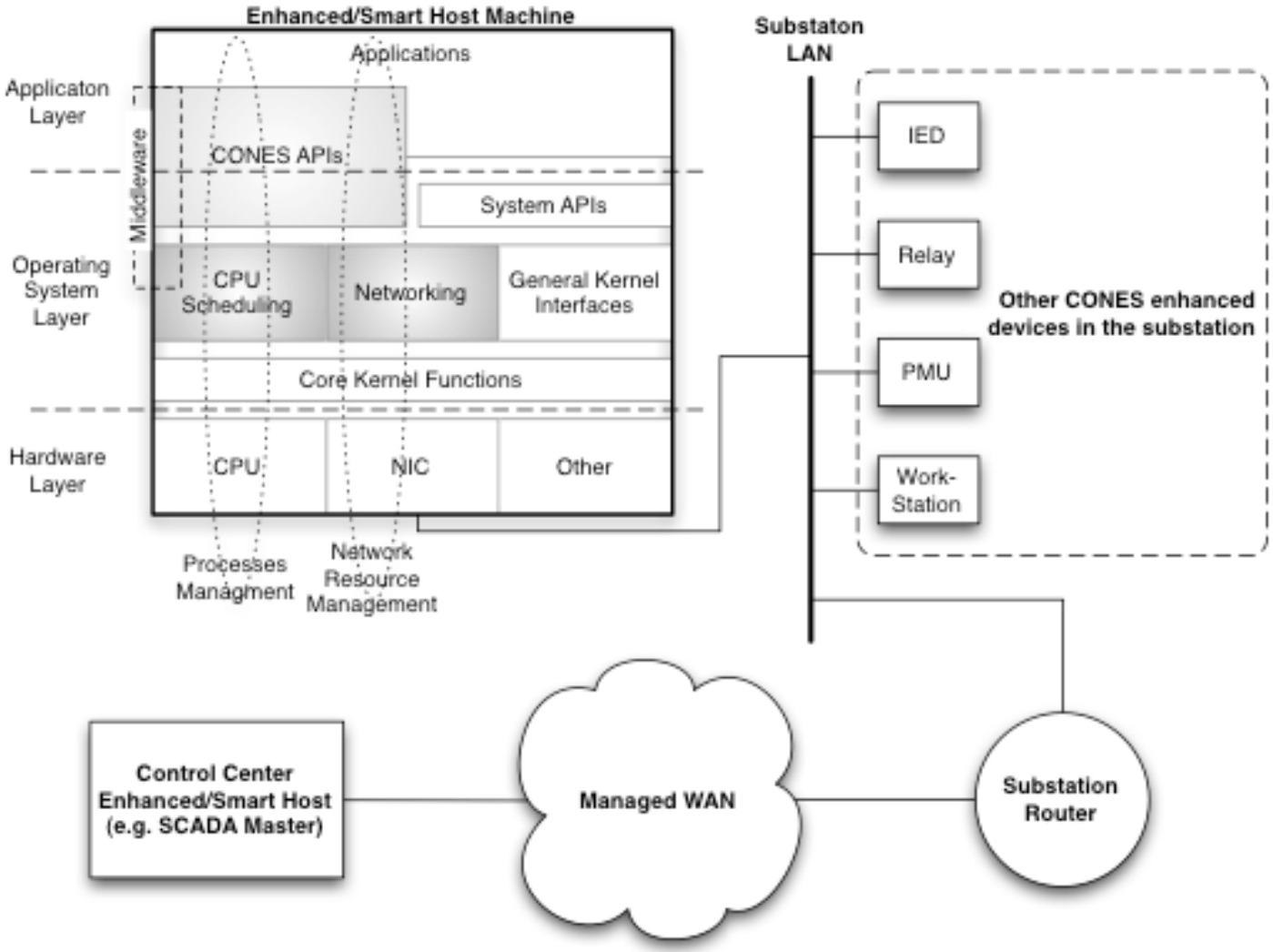
Development: Requirements

Power Systems Application	Traffic Type	Traffic Path	Qualitative Quality of Service (QoS) Parameters	Packet Characteristics (size, timing) per device	Scalability considerations	Stream Bandwidth Characteristics (per device, total)
Protection/ Control	SCADA	IED(substation) -> Control Center	Low latency, high priority, no loss	Size: 256B – 1KB Frequency: 1 packet every 2-4s	~5 devices per bus	.5KB/s per device 2.5-5KB/s per bus
	SMV/ GOOSE	IED -> IED	High speed/low latency, high priority.	Size: typically less than 1 Ethernet frame Frequency:	1 event per second per bus	1-15KB per protection event
Monitoring	PMU	IED/PMU -> Phasor Data Concentrator (Control Center)	Low latency, medium priority.	Size: 128 Bytes Frequency: 30 – 120 samples/sec	2 PMUs per bus	30Kbps per device, 60Kbps per bus
	Other Monitoring Data	IED/master -> Control Center	Low latency, medium priority.	Size: 32-64 Bytes Frequency: 1 sample/sec	20-25 Devices/substation	256-512Kbps per device 1-5 Mbps per substation (not all data leaves the substation)
Engineering	Interactive	Control Center <-> Substation	Medium latency, medium priority	N/A (these are not critical timings and can vary greatly)		1M per occasional request
	Data Transfer	Control Center <-> Substation	Low priority	N/A (Big packets, but not a standard size)	A flow 1-2 times per day	1-5M per occasional request
Surveillance	Video	Substation -> Control Center	Medium – High latency, medium priority.	Varied video frame sizes and rates	2-10 cameras per substation.	100 Kb/s -1Mb/s per camera ~5Mbps per substation

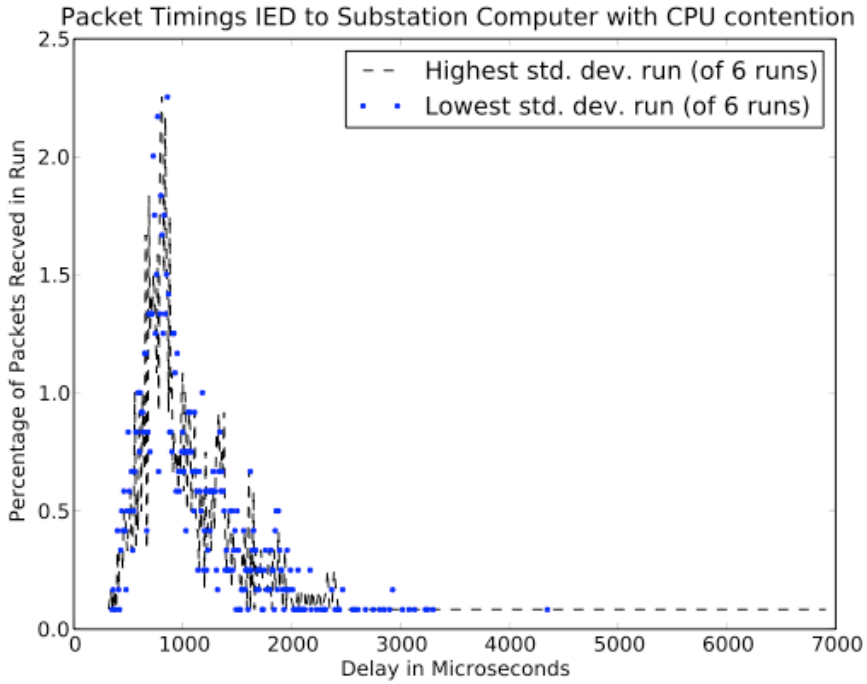
Tool selection and development

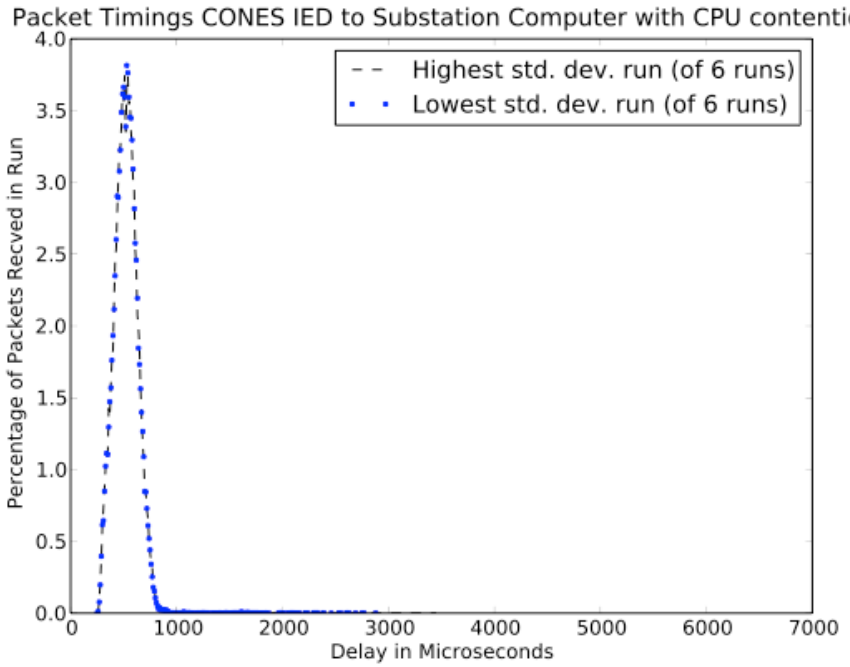
- **Linux Operating System**
  - Easily available
  - Open source, therefore extremely flexible
  - Good networking support
  - iDSRT: soft real-time kernel with network stack scheduling (previous UIUC tool)
    - Enhanced with socket options and more extensive process support
    - Guarantees of timeliness to network interface card level
    - Uses Earliest Deadline First scheduling
  - *Results of study applicable to other platforms*
- **Control Network Emulation**
  - Custom tools emulate networking conditions described above
  - Allows fine grained testing
- **Wide area networking**
  - Use of common technologies, such as DiffServ and MPLS
  - Chose Juniper routers for minimal added latency

Results: Architecture



Results: Performance



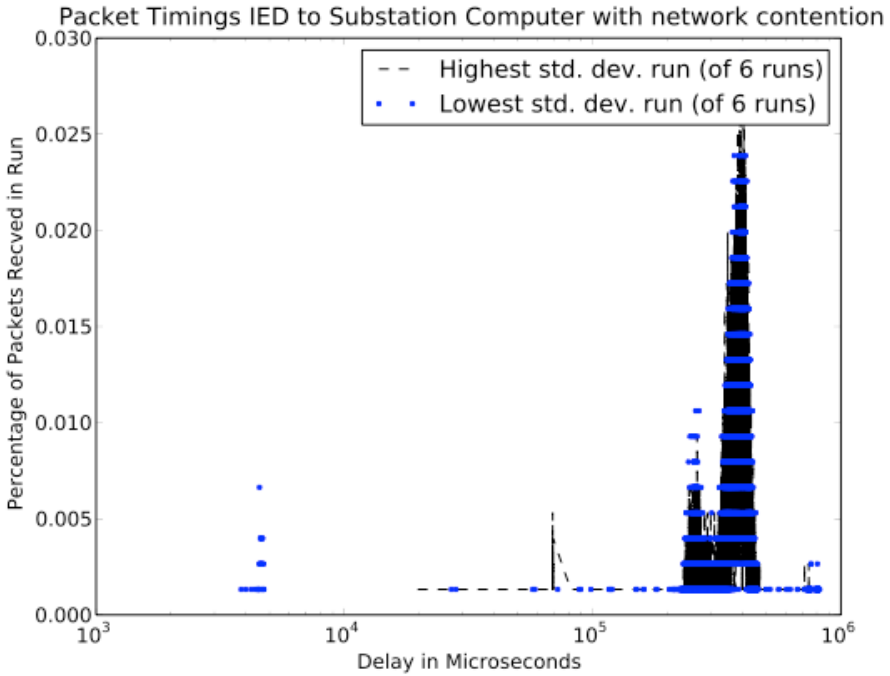


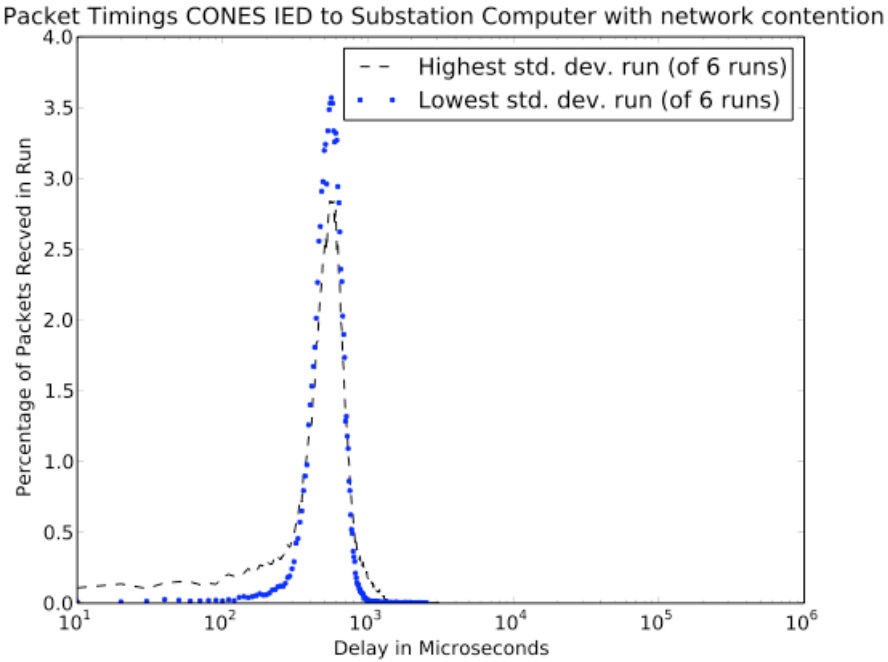
Packet latency timings with CPU contention

Left: unenhanced host

Right: CONES enhanced host

Results: Performance





Network latency timings with network interface contention.

Left: unenhanced host

Right: CONES enhanced host

Collaboration/Technology Transfer

- **Plans to gather further industry input**
  - Work closely with industry partners such as Entergy, TVA, PJM and others to understand limitations, requirements and concerns about communications, particularly for control.
  - Approach TCIPG partners for access to network traces and data to gather more accurate information for testing and development
  - Alternative approach: industry standard set of reference data

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - CONES provides a good base for new devices and networks
    - Part of a full solution for new build-outs and complete overhauls
    - Integrates nicely with modern networking equipment
  - Plan to use CONES and it's technological lessons in future prototypes and products for new networks such as NASPInet
  - Release CONES open source
  - Since CONES is built on commonly available and widely used technologies, it provides easy integration with modern communications networks, providing a simple transition path
  - Interact with TCIPG vendor partners to discuss technology transfer opportunities

Next Steps

- **Approach For the Next Year**
  - Improve timing measurements
  - Implement security layers
  - Release software under open source licensing
  - Develop sample QoS policy specifications
- **Follow-on work**
  - Spinoff project: Tools development
    - Attempt to create a standard set of tools and techniques to aid research on power system networks