Russell Robertson

Grid Protection Alliance

Tim Yardley

University of Illinois

ARMORE: Applied Resiliency for More Trustworthy Grid Operation

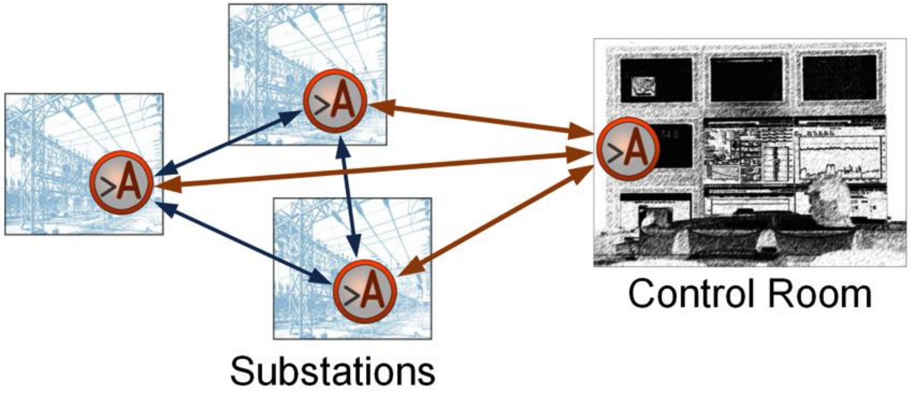
Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Summary: ARMORE

Objective

- To develop an intelligent framework that provides secure information exchange, advanced analytics, and enable actionable intelligence to increase security and resiliency of grid operation through seamless enhancement of legacy and modern protocols



Performer:	Grid Protection Alliance
Partners:	University of Illinois Pacific Northwest National Lab
Federal Cost:	$2.213 M
Cost Share:	$0.639 M
Total Value of Award:	$2.852 M
Funds Expended to Date:	83%

DE-OE-0000676

Schedule

- October 2013 – June 2017
  - Final design - 9/15/14
  - Alpha Version - 9/15/15
  - Demonstration - 1/15/17
  - Version 1.0 released - 6/15/17

Advancing the State of the Art (SOA)

State of the Art

- SCADA protocols are difficult to protect and actionable intelligence is missing
- Situational awareness is lagging
- Deployment of security technology is costly

Value Proposition

- Provides visibility and awareness at an unmatched level, enabling situational awareness
- Enables policy creation associated with semantic behavior
- Minimizes deployment costs and provides flexibility for multiple approaches
- Enhances security of legacy communications

Advancing the State of the Art (SOA)

Deployment Feasibility

- **Flexible deployment modes (passive, transparent, active)**
- **Fault tolerant middleware communications**
- **Virtualized or bare-metal**
- **No first-cost for the software**

Realizing the Value

- **Secure legacy SCADA communications without changing your configuration**
- **Get increased operational situational awareness**
- **Baseline operational systems**
  - Visualize SCADA communications
  - Classify assets
  - Create policies to feed SIEM
- **Decrease deployment costs**

Advancing the State of the Art (SOA)

Respecting Operational Requirements of EDS

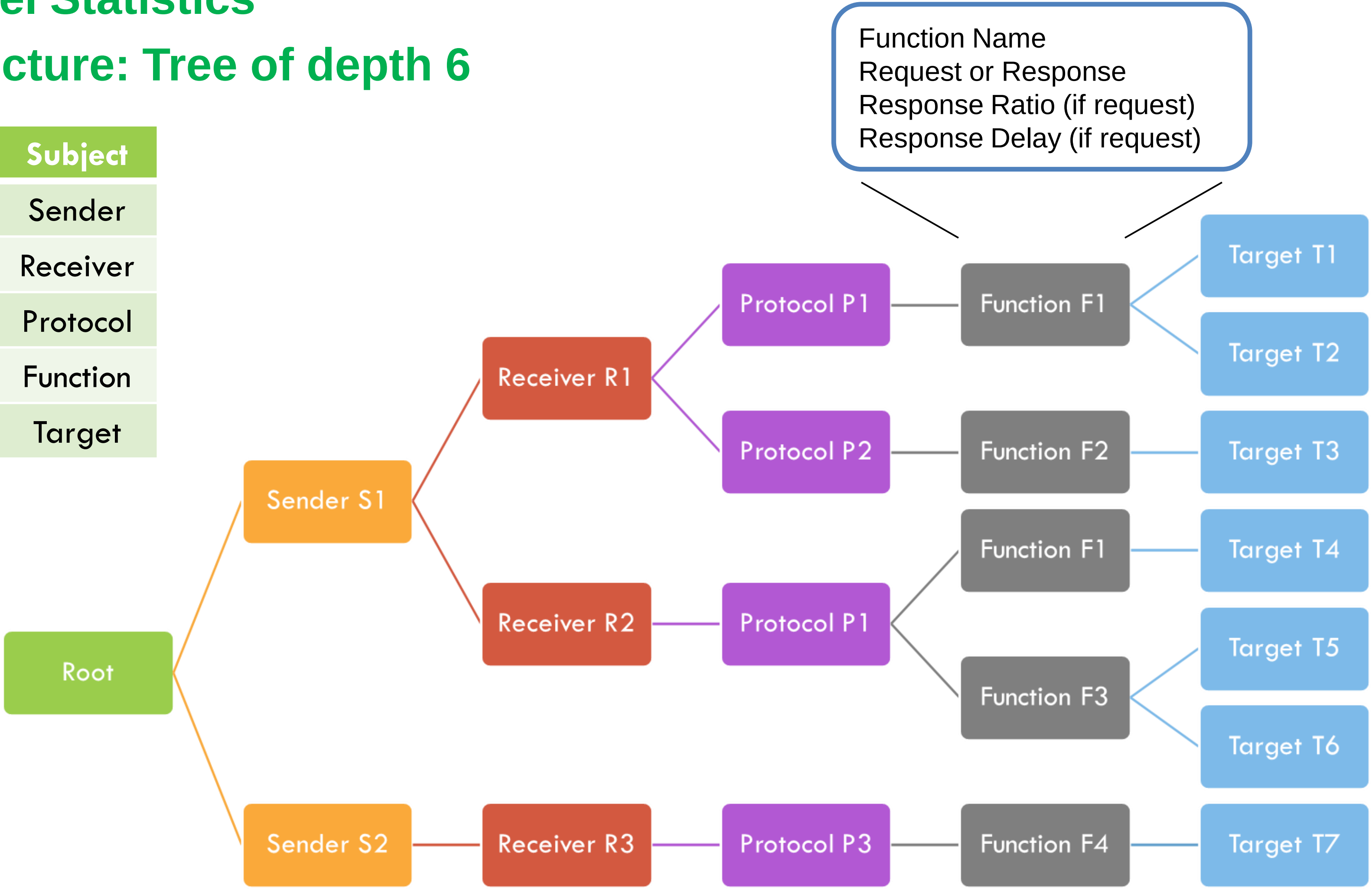
- Doesn’t require manipulating any end-device configuration
- Fails open to not affect operations, alarms by default rather than block
- Maintains timeliness constraints in active and transparent mode
- Minimizes overhead incurred for packet capture and cryptography
- Leverages fail-safe hardware to maximize system uptime
- Can operate completely passively, leaving no fingerprint on the deployed environment
- Designed with security in mind from the ground up

SOA - Analytics

Multi-Level Statistics

Data Structure: Tree of depth 6

Level	Subject
1	Sender
2	Receiver
3	Protocol
4	Function
5	Target



Function Name
Request or Response
Response Ratio (if request)
Response Delay (if request)

Advancing the State of the Art (SOA)

Advancing the Cybersecurity of Energy Delivery Systems

- **Add intelligence**
  - Passive information feed from a span port
  - Provides analytics, baselining, alarming
- **Add security**
  - Encapsulate and encrypt communications
  - Policing, alarming, and protection
- **Increased understanding**
  - Network visualization, behavior baselining
  - Historical statistics
- **Reduced deployment costs and increased resiliency**
  - Fails safe, no reconfiguration, or completely passive

Mapping to Needs

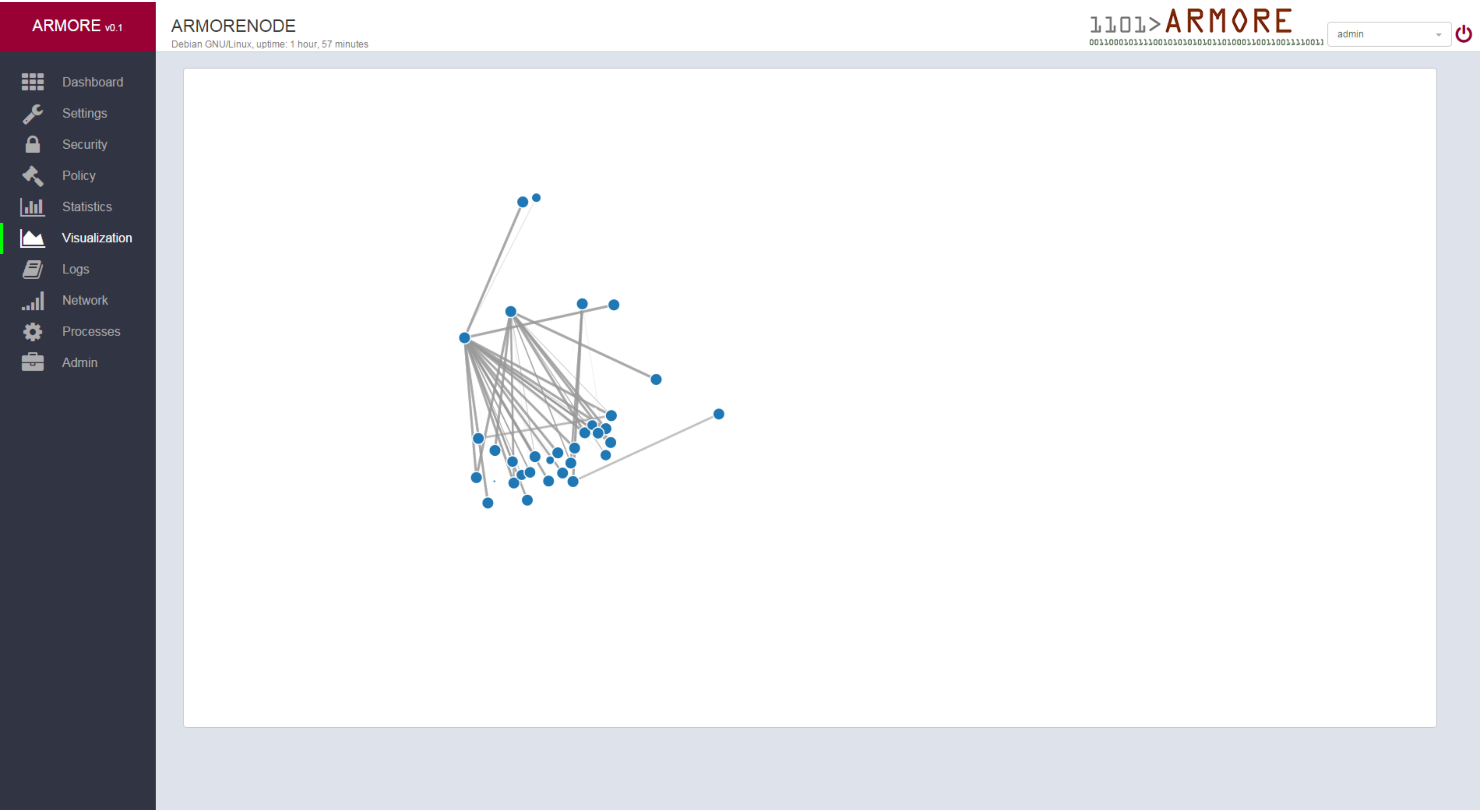
Energy Delivery Systems Environment	ARMORE Features
Ability to survive a cyber incident while sustaining critical functions	Fault tolerant communications and flexible security provisions
Contains a mixture of legacy and modern components and controls	Works with both legacy and modern devices and both known and unknown protocols in a transparent way
Resources may not have enough computing resources to support generic cyber security capabilities	Requires no additional resources on the end devices
Components are geographically dispersed	Designed to be a distributed environment from the ground up
Requires timely response to cyber security event	Allows the deployment of new access control policies amongst the nodes to respond to a change or event

Progress to Date

Major Accomplishments

- **Primary system designed and developed**
  - Base feature set complete (inspect, encapsulate, encrypt, alarm)
  - Initial analytics and administration
  - Initial baselining and detection
  - End-product approach
  - Advancing visualization
- **Future expressed interest**
  - More advanced analytics
  - Application offloading, serial communications
  - Larger library of policies and more intuitive interface
  - Ability to do continuous compliance monitoring and prevention
  - Be a source of intelligence data rather than just an end product

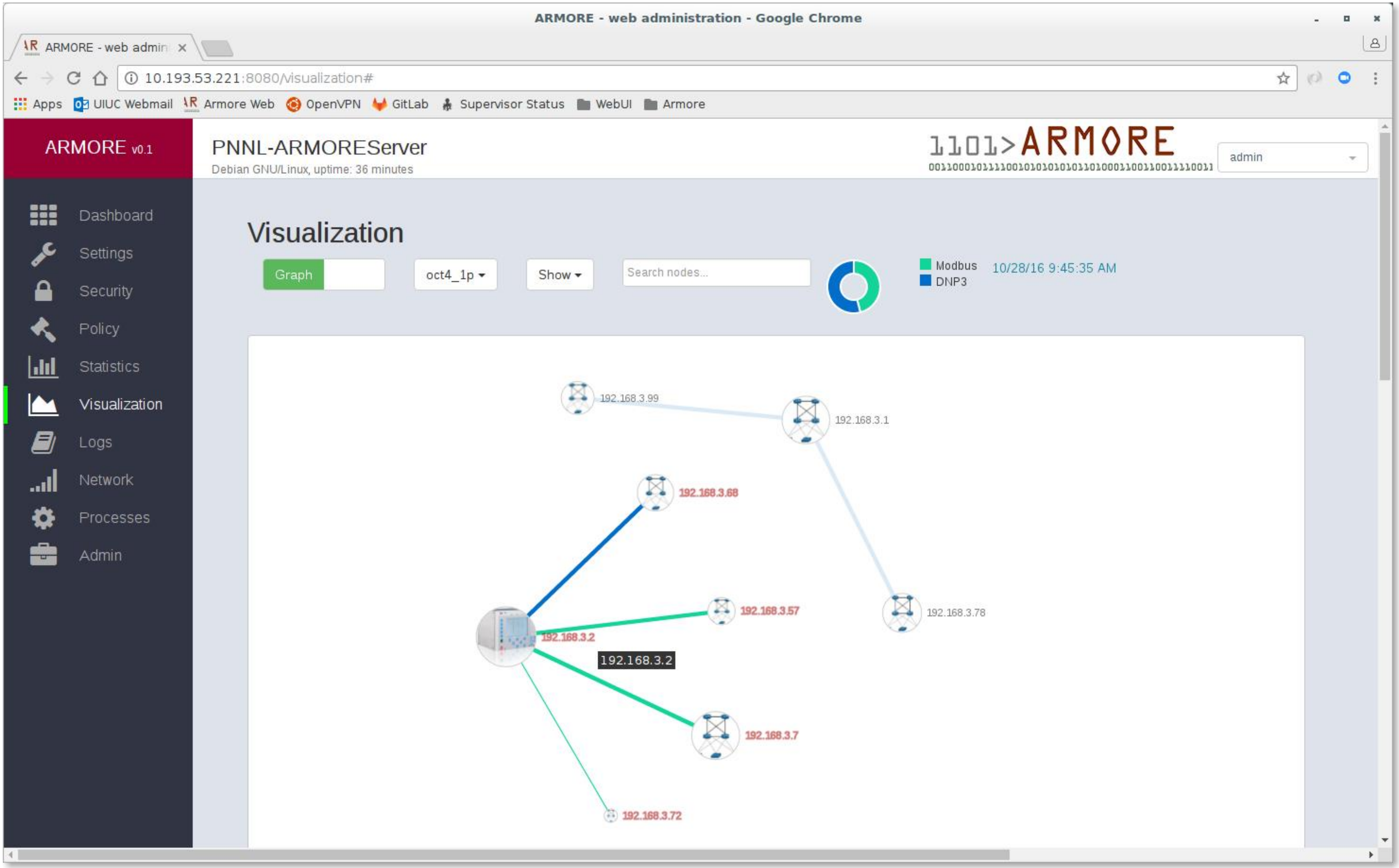
Alpha Visualization



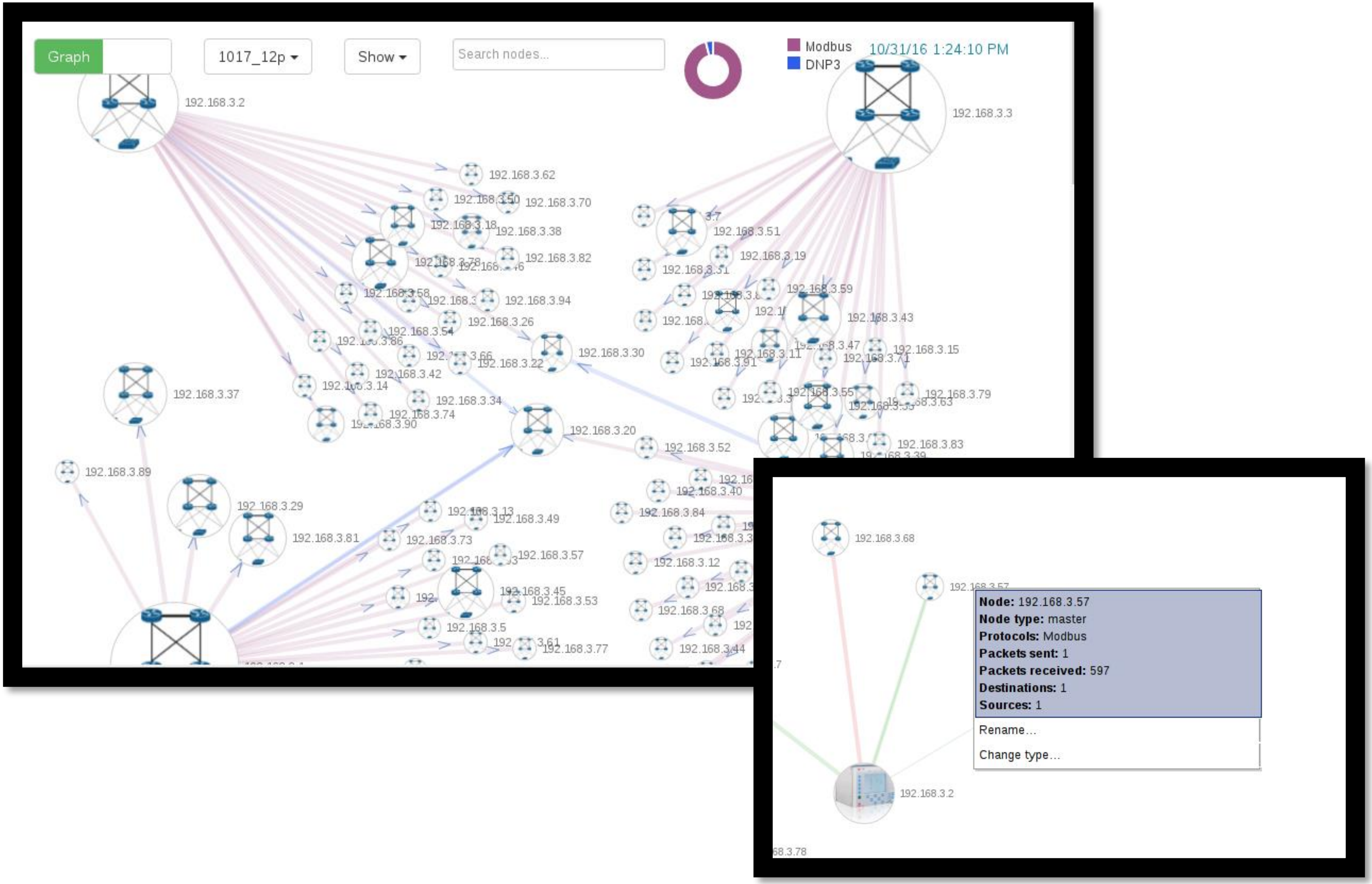
ARMORENODE

Debian GNU/Linux, uptime: 1 hour, 57 minutes

Current Visualization



Current Visualization



Node: 192.168.3.57
Node type: master
Protocols: Modbus
Packets sent: 1
Packets received: 597
Destinations: 1
Sources: 1

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- **Free, open source**
- **Transitionable interest and knowledge**
  - IDS/IPS/SIEM entities
  - NRECA Essence platform
  - DARPA RADICS program
- **Testing / Demonstration**
  - Internal Bench Test
    - Full stack – All ARMORE modes
  - Utility partners (Ameren, ComEd, TVA)
    - Demonstration Plan Complete
    - Passive (TVA in Subs) and active (Ameren at Tech App Center) deployments
  - Vendors (Various)
    - Integrations

Questions?

GRID PROTECTION ALLIANCE

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability