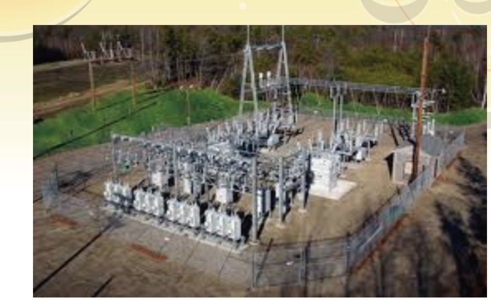
CyberSAVe – Situational Awareness Visualization for Cyber Security of Smart Grid Systems

William J Matuszak, Lisa Dipippo and Yan Lindsay Sun

Research Overview

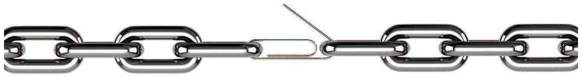
- Problem:
  - Lack of visualization techniques for Cyber Trust



- Application:
  - Power Grid SCADA system
- Solution:
  - Mathematical model for Cyber Trust
  - Geo-Spatial Visualization of trust for each power plant and sub-station
  - Calculation / Visualization of Trust Metrics (Time history, Histogram)
  - Visualization of data aggregations (Geographic & bar graphs)
- Results
  - Identification of small-scale Hactivist attack (Power source e.g. Nuclear, company)
  - Identification of mid-scale Geographic attack
  - Identification of large-scale Nation State Attack (“Stuxnet” like)

Cyber Trust Theory

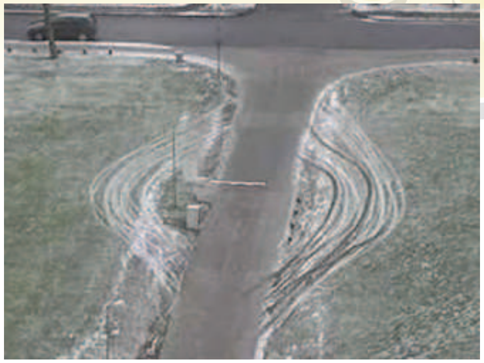
- Trust
  - A well studied concept in sociology and psychology.
  - known as the driving force for collaboration in social communities.
- Developed Mathematical Foundation for Visualization
  - Based on observed behaviors.
  - Good behaviors reinforce trust.
  - Bad behaviors reduce trust.
  - Unpredictable behavior also reduces trust.



Inherent trust in sensors is a weak link in SCADA Cyber Security

Multi-Dimensional Trust

- Different behaviors lead to different types of trust
- Power grid cyber attacks
  - False alarm ➔ False alarm trust
  - Missed detection ➔ Detection trust
  - Damaged/affected sensor ➔ Availability trust
- Overall trust
  - Computed from all three types of trust
  - Weighted average, minimum, predictability



Trust knowledge is essential: Hackers will find a way in to systems

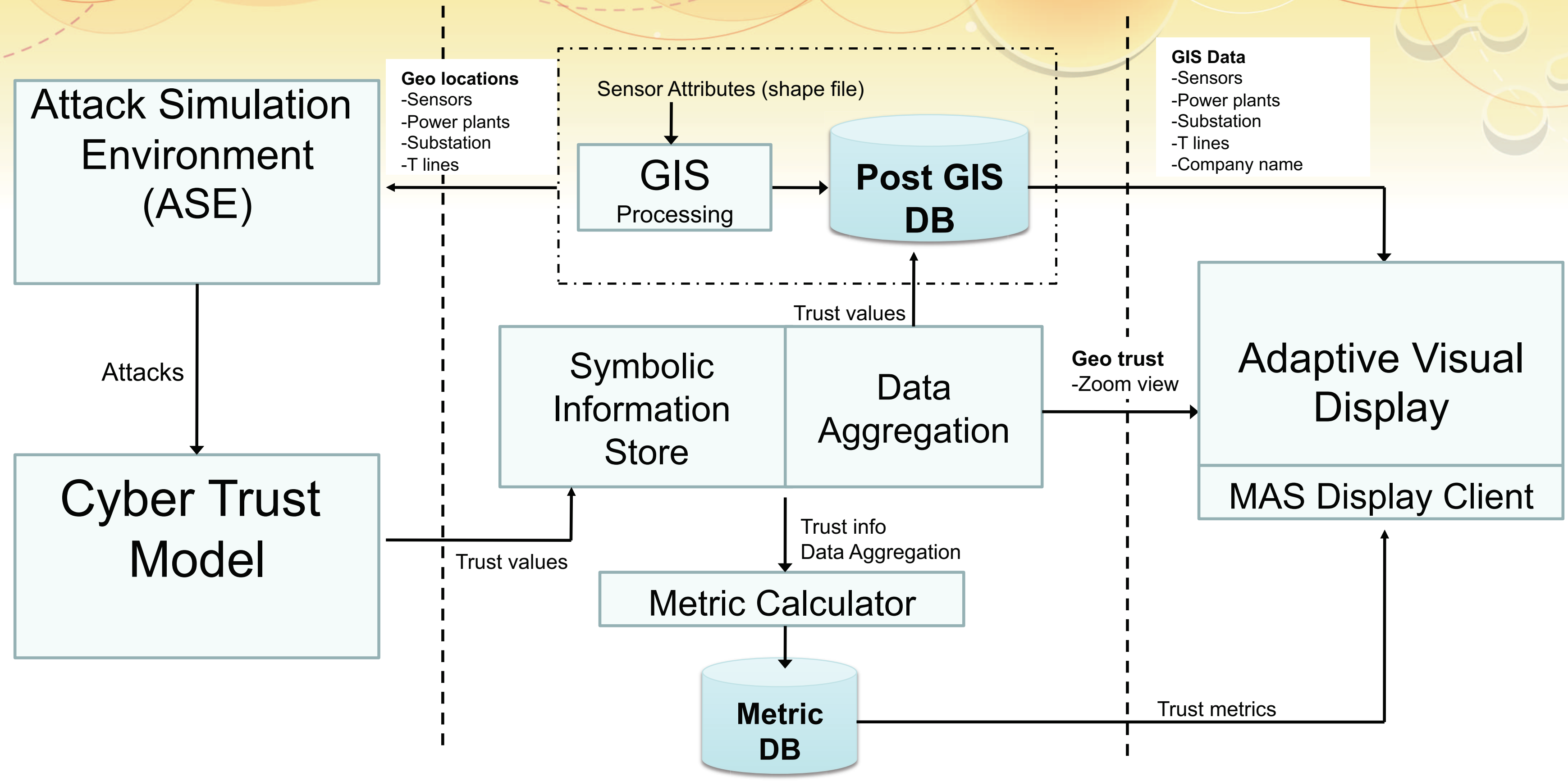
VIS 2013 VAST • INFOVIS • SCIVIS BIOVIS • LDAV

Predictability Trust

- On/Off Attack
  - Attacker knows how trust is computed
  - Mostly good behaviors – occasional bad behavior
  - Basic trust computation will not reflect the pattern
- Predictability trust
  - If behavior “disappoints” – reduce predictability trust
  - Predictability trust used to compute overall trust
  - On/off attack can be detected after a few bad behaviors
  - Ratio of on/off attack detected is parameterized by bad behavior window size

Cyber Trust Visualization

CyberSAVe Overview



Attack Simulation Environment (ASE)

Geo locations
-Sensors
-Power plants
-Substation
-T lines

Sensor Attributes (shape file)

GIS Processing

Post GIS DB

GIS Data
-Sensors
-Power plants
-Substation
-T lines
-Company name

Attacks

Trust values

Symbolic Information Store

Data Aggregation

Geo trust
-Zoom view

Adaptive Visual Display

MAS Display Client

Cyber Trust Model

Trust values

Trust info
Data Aggregation

Metric Calculator

Metric DB

Trust metrics

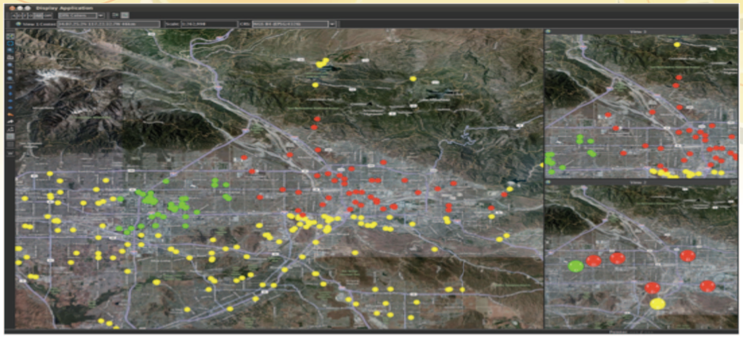
Visualization Framework

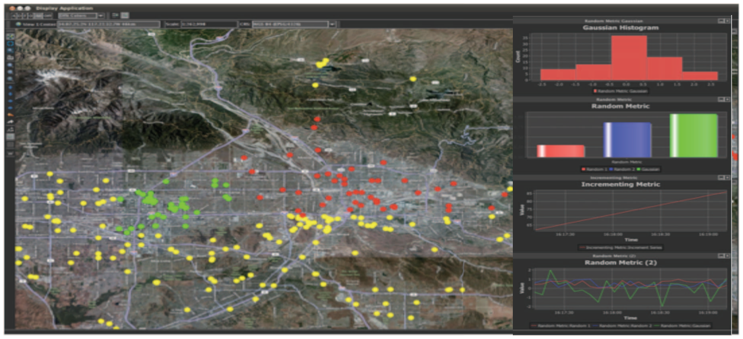
- Framework for building highly modular Java-based visualization applications
- Provides common look-and-feel, application programming interfaces, foundational services (UI management, service registration/discovery, application events and persistence)
- Uses the standard OSGi services platform to provide module loading, version management and sandboxing
- Supports mix-and-match assembly of separately developed functional modules
- Service-oriented layered architecture
  - Core framework
  - (Optional) GIS framework (geographic map, overlays, tools, API)
  - Separation of interface (API specification) and implementation
- Reduces application development time by providing almost-complete application requiring only domain-specific module development
- Supports a high degree of re-usability of modules

Adaptive Visual Display

Adaptive Visual Display

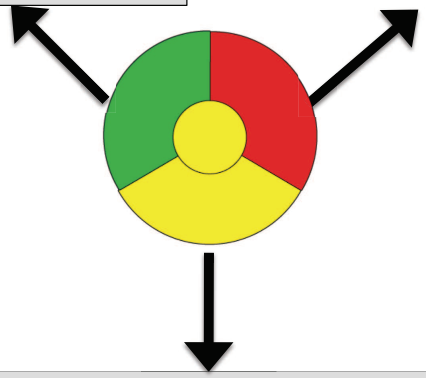
- Multiple Geo displays at independent zoom levels
- Collapsible to single Geo
- Aggregation with zoom
- Metrics plotted real time in context with Geo
- Built on Visualization Framework





Configurable at Run Time to Meet Operational Requirements

Operational Trust Indicator (OTI)



Indicator of False Alarm Trust

Indicator of Availability Trust

Indicator of Overall Trust

Center Circle

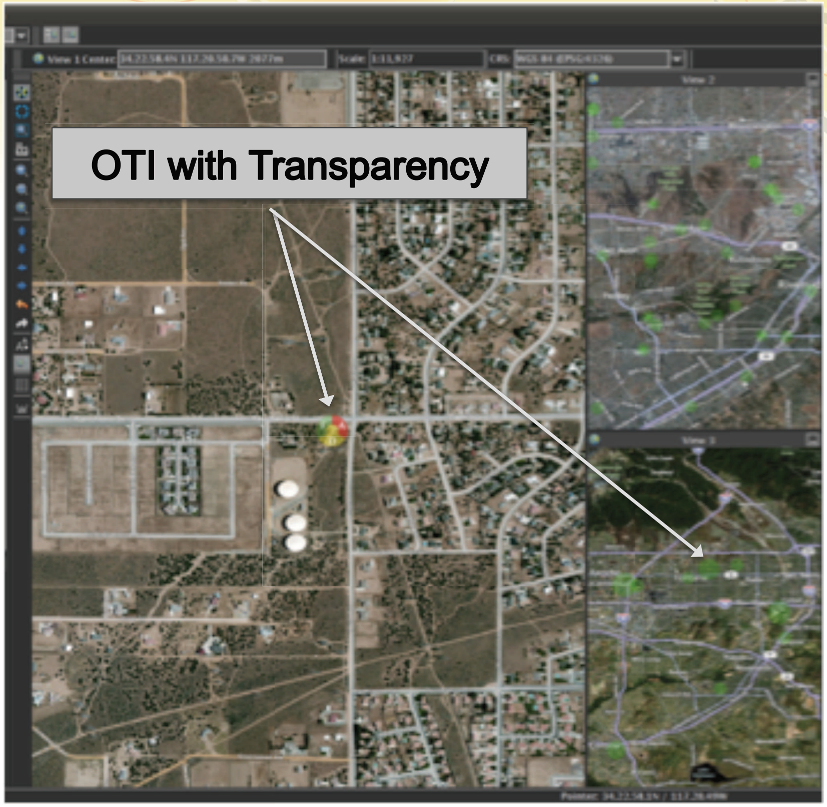
Indicator of Detection Trust

🟥	Trust < 0.3333
🟨	0.333 < Trust < 0.6666
🟩	Trust > 0.6666

Note: Color configurable to color palette

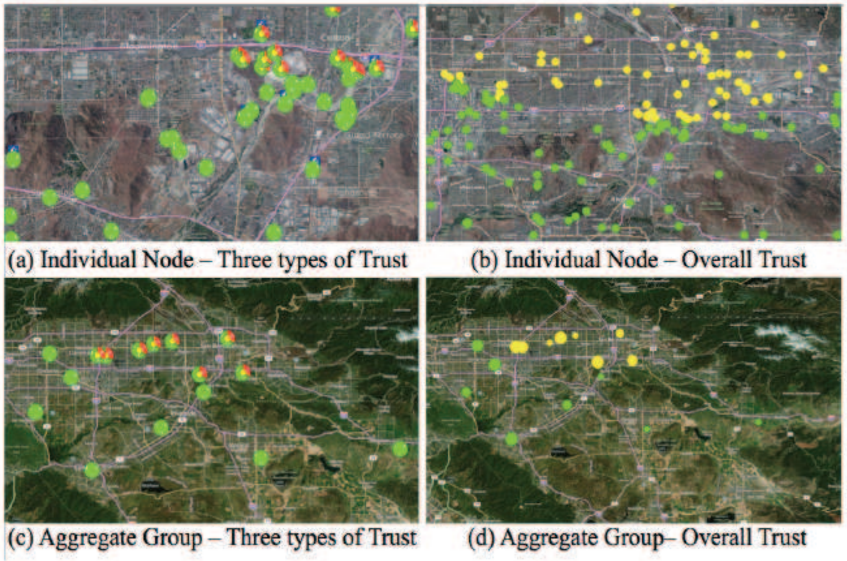
Flexible / Configurable Design

- Opacity / Transparency
  - Operator control
- OTI Size
  - Slider Control
- Color Alert levels
  - Demo 3 Quantized levels
  - Adaptable to entire color palette
- Types of Trust
  - Demo = 3 trust types
  - Configurable based on application
- Display Layers
  - Toggle data on/off



Aggregation Levels

- Configurable Aggregation
  - Currently set-up is 4 levels of automatic aggregation with zoom
    - Individual substation with all three trust types plus overall
    - Individual substation as dots for overall trust only
    - Aggregated group (e.g. City) with all three trust types plus overall
    - Aggregated group (e.g. City) as dots colored for overall trust
      - Size of dots proportional to number of substations in the aggregation
      - Aggregate dots located at the mean location

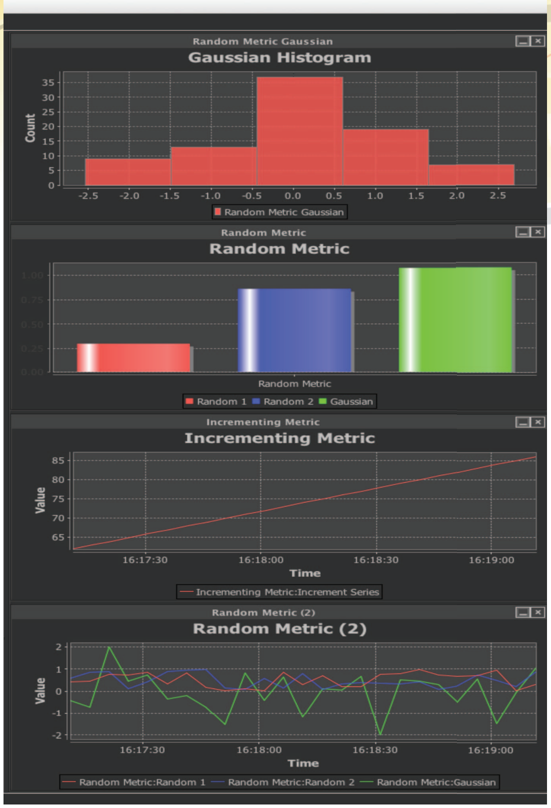


(a) Individual Node – Three types of Trust (b) Individual Node – Overall Trust

(c) Aggregate Group – Three types of Trust (d) Aggregate Group– Overall Trust

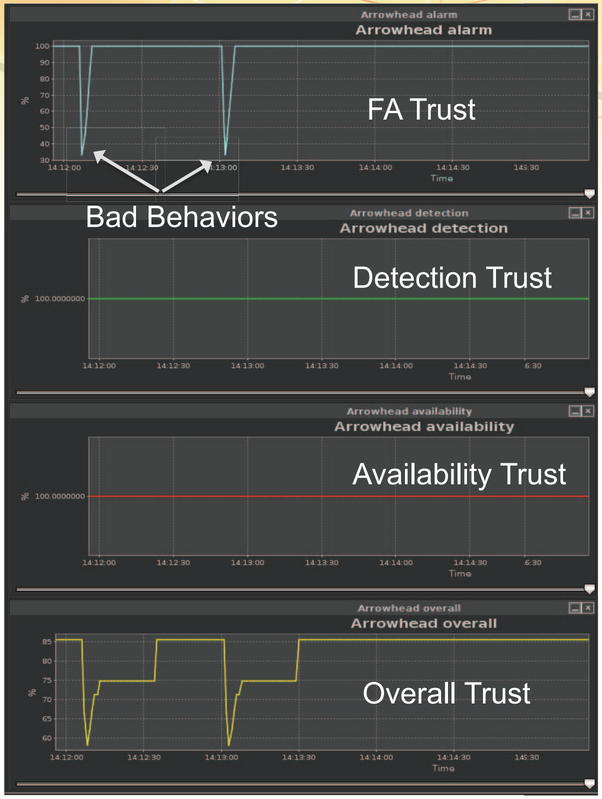
Metric Assessment System (MAS)

- MAS Allows for real time assessment of data
  - Support plotting of data in various formats and axis in context with geographic visualization
    - Single node Historical trust of time
    - Multi-node historical trust
    - % of nodes at low trust / high trust
  - Bar graph by aggregated value
    - Plant owner
    - Fuel type (nuclear, solar, gas)
    - City (zip code)
    - Equipment (sensor type, generators, controllers)
  - Histogram of all sensor nodes



Trust Over Time

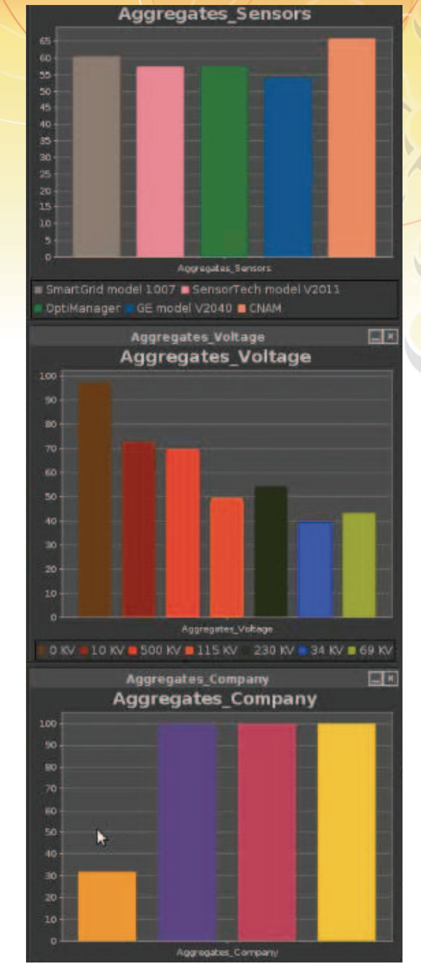
- “Drill-down” from Geographic display detailed trust evaluation
- Time History plot for each type of trust and overall trust
  - False Alarm
  - Detection
  - Availability
  - Overall
    - Overall trust calculated with ***Predictability Trust***



On – Off attack False Alarms

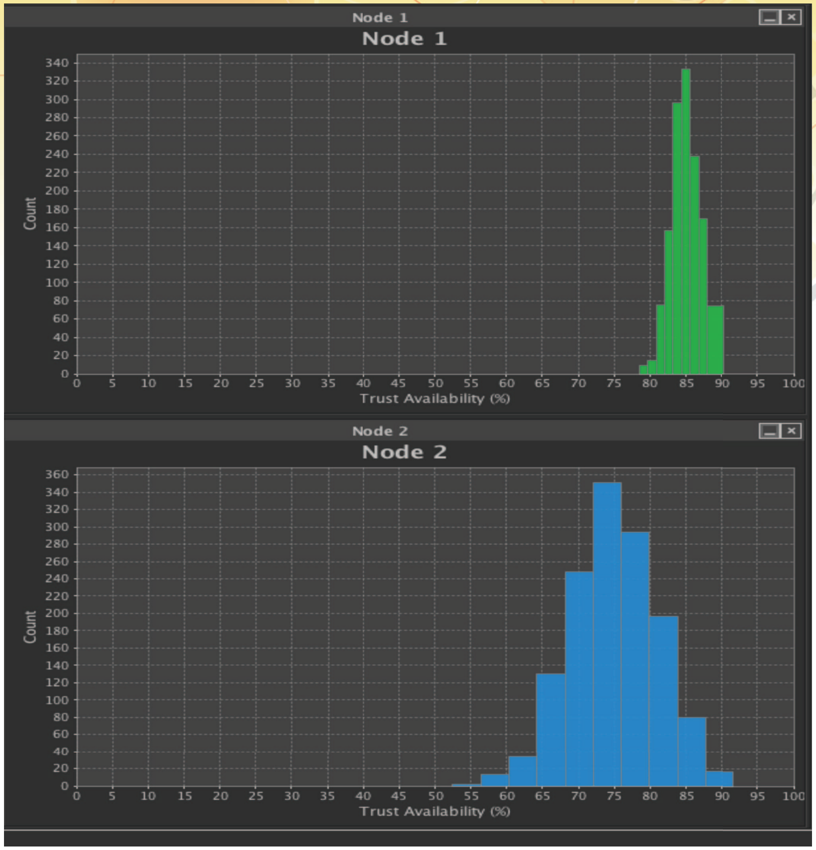
Metric Assessment System (MAS)

- Visualization of trust based on aggregated parameters
  - Provides insight into type attack and goals attacker
    - Visualization of correlations of “bad behaviors”
      - Sensors -> Worm aimed at specific equipment
      - Voltage –> Terrorist looking to inflict most damage
      - Company -> Disgruntled employee attacking their employer
      - Power source -> Hactivist attacking a specific originating fuel source



MAS Histogram Example

- Comparison of histogram from different areas can help operator understand environmental conditions and / or Threat posture
  - Node 1 (top) is an example of a histogram of trust for benign environment
    - Mean availability trust value high
    - Variance small
  - Node 2 (bottom) is an example of a histogram of trust for a poor environment
    - Mean availability trust lower
    - Variance larger

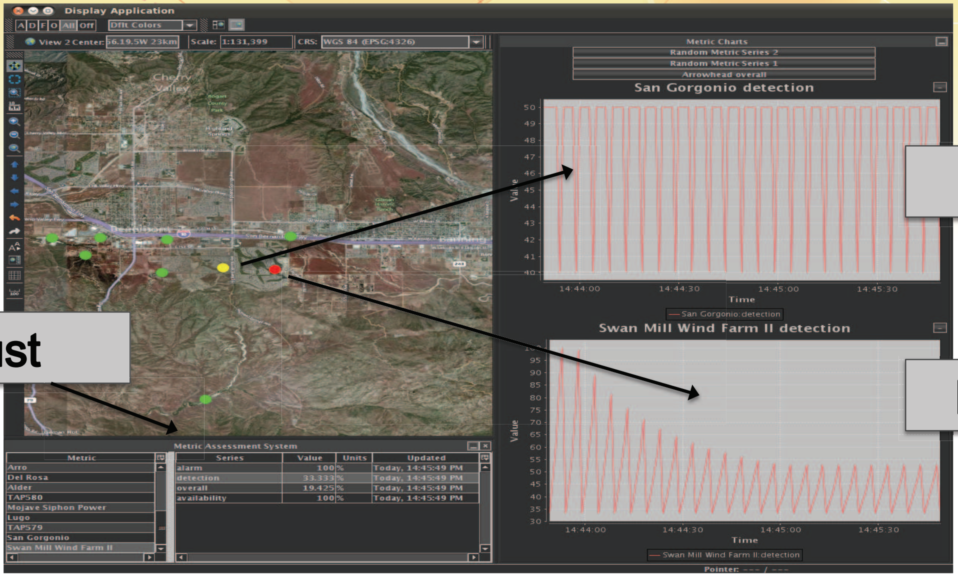


Results

Results

Protection vs. Attack	**Sensor**	**Firewall+**	**Cyber Trust+**	**Predictability+**	**Visualization+**
Physical Attack (PA)	✔	✔	✔	✔	✔
Known Malware Attack		✔	✔	✔	✔
Simple Cyber Attack			✔	✔	✔
Advanced Cyber Attack				✔	✔
Advanced Attack Hactivist					✔
Advanced Attack Geographic					✔
Advanced Attack Nation State					✔

Complex “on / off” Attack



Metric Assessment System

Metric
Arro
Del Rosa
Alder
TAP580
Mojave Siphon Power
Lugo
TAP579
San Gorgonio
Swan Mill Wind Farm II

Series	Value	Units	Updated
alarm	100	%	Today, 14:45:49 PM
detection	33.333	%	Today, 14:45:49 PM
overall	19.425	%	Today, 14:45:49 PM
availability	100	%	Today, 14:45:49 PM

Simple Trust

Instantaneous Trust

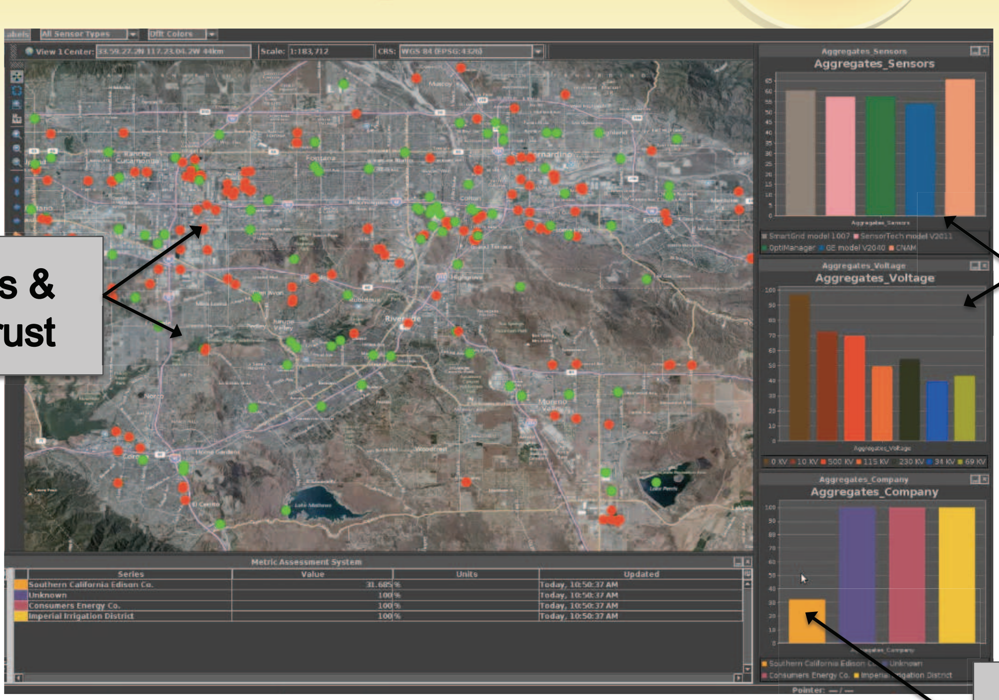
Predictability Trust

Predictability Trust

- On/Off attack (4 good behaviors, 1 bad)
  - Designed to fool trust processing
- Trust metric plot shows how trust goes down
  - Forgetting factor changes with negative behaviors

Hacktivist / Disgruntled Employee Attack

Multiple power plants & substations w low trust



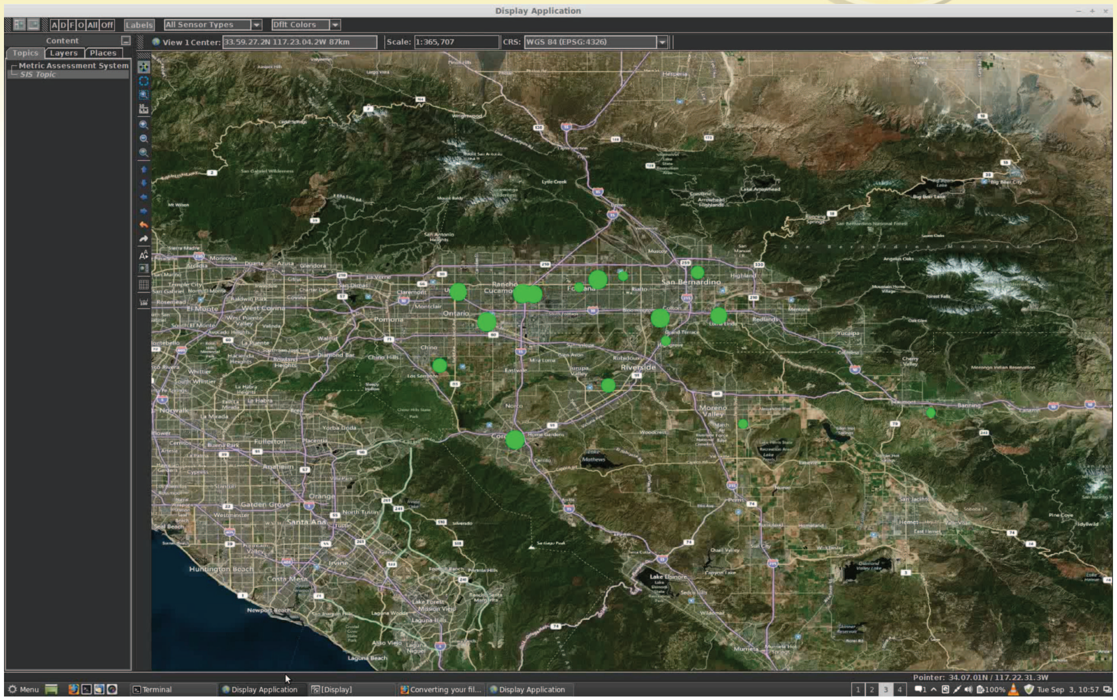
Metric Assessment System

Series	Value	Units	Updated
🟧 Southern California Edison Co.	31.685	%	Today, 10:50:37 AM
🟪 Unknown	100	%	Today, 10:50:37 AM
🟥 Consumers Energy Co.	100	%	Today, 10:50:37 AM
🟨 Imperial Irrigation District	100	%	Today, 10:50:37 AM

Trust evenly distributed among other parameters

Low Trust on Southern California Edison

Results - Geographic



All Sensor Types

Dflt Colors

Metric Assessment System
- SIS Topic

View 1 Center: 33.59.27.2N 117.23.04.2W 87km

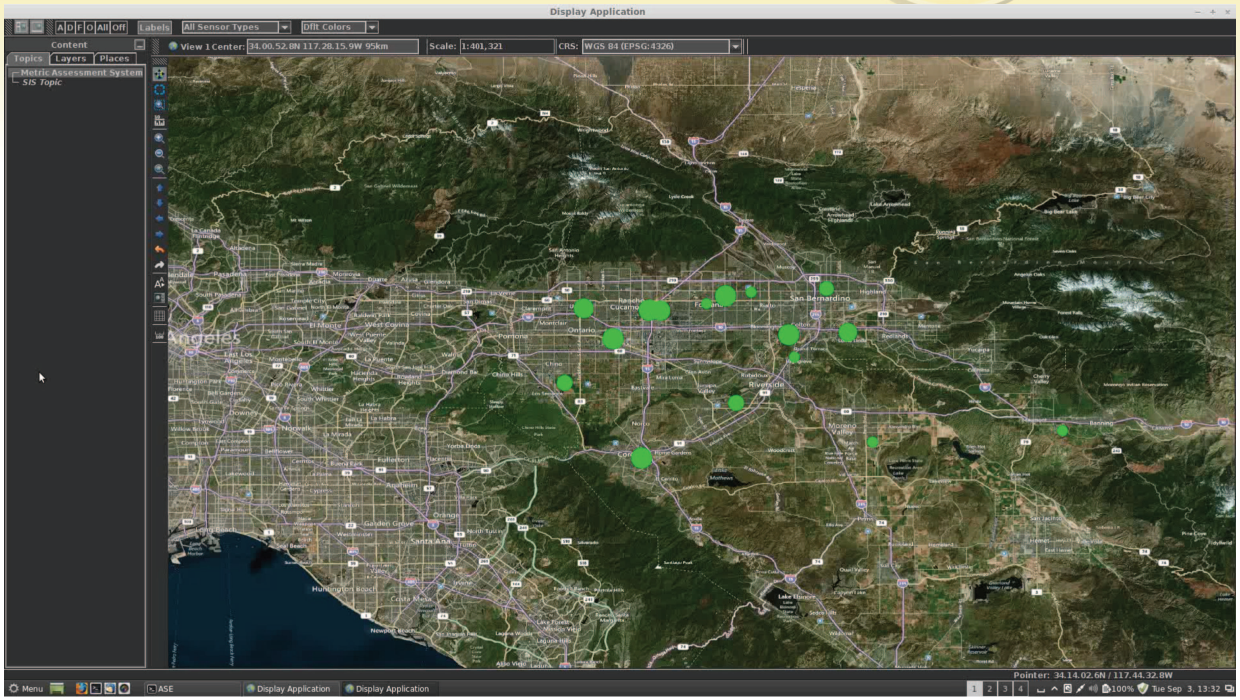
Scale: 1:365,707

CRS: WGS 84 (EPSG:4326)

Pointer: 34.07.01N / 117.22.31.3W

100% Tue Sep 3, 10:57

Results – Nation State Attack



View 1 Center: 34.00.52.8N 117.28.15.9W 95km

Scale: 1:401,321

CRS: WGS 84 (EPSG:4326)

Pointer: 34.14.02.6N / 117.44.32.8W

100% Tue Sep 3, 13:32

Summary

- We researched techniques to calculate and visualize Cyber Trust in a power grid SCADA system
- We demonstrated visualization of Cyber Trust versus various attacks
- Potential Follow-on R&D
  - Visualization of Cyber Risk
  - Behavior monitoring to determine trust values
  - Indirect vs. direct trust computation
  - Symbolic Fusion and Ontology Visualization