U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

INGRESS: Integration of Green Renewable Energy Sources Securely with the Buildings and Electric Power

United Technologies Research Center (UTRC)

Dr. Devu Manikantan Shila

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

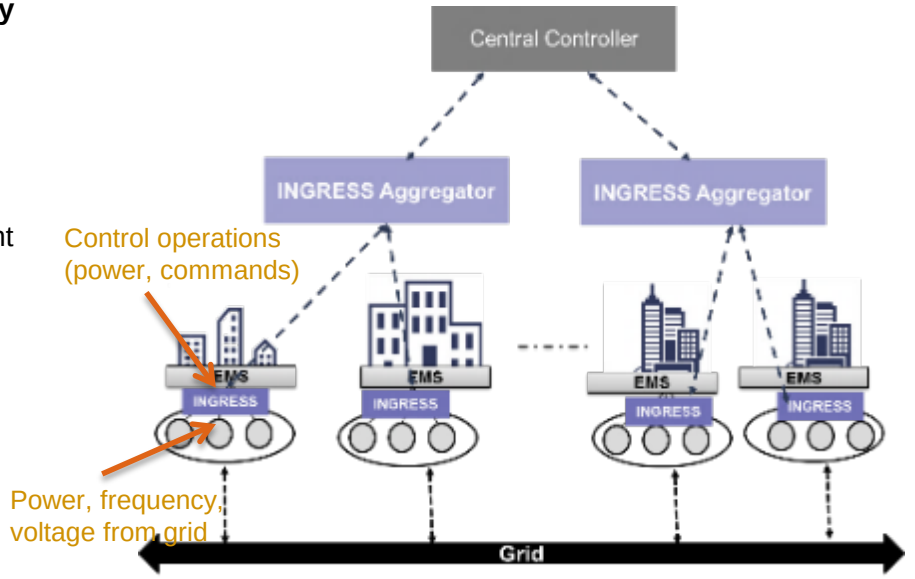
Summary: INGRESS

Objective

- **Develop a non-intrusive bump-in-the-wire (BITW) technology to:**
  - Detect synthetically valid but malicious control commands to controller (e.g., set temperatures, pressure, or change status of DERs)
  - Detect "DER under attack" using new sensor modalities
  - Achieve interoperability between DERs, building management systems and utilities
- **Demonstrate the technology in a system of system (SoS) environment**

Schedule

- **Project Timeline: Oct. 2016 – Sept. 2019**
- **Key deliverables:**
  - ✓ Report on threat and attack classification for various behind-the-meter energy systems (Dec. 16);
  - ✓ Report on implementation for model-based-validation subsystem (Sept. 18);
  - ✓ Report on sensor instrumentation and integration, architecture and design of anomaly detection subsystem (Jun. 18);
  - ✓ Developer and User Guide for INGRESS implementation (Mar. 19);
  - ✓ Phase I Final Report on Research and Development (Mar. 19)
  - Phase II Final Report on Demonstration (Sept. 19)



Total Value of Award:	**$ 3,521,324**
Funds Expended to Date:	**70% (Phase 1)**
Performer:	**UTRC**
Partners:	**PNNL, UIUC**

INGRESS will provide **an inline advanced attack detection and resiliency-enabling cybersecurity platform for behind-the-meter DERs** that automatically detects malicious control commands and prevents problematic DER operations in real-time.

Advancing the State of the Art (SOA)

State-of-the-Art:

- Network connected distributed generation, automated controls and flexible loads (Distributed Energy Resources) **create new pathways for attacks**
- Lack of control, visibility into the operation at the edge and insufficient security makes adversaries life easier
- Connection with the grid can be exploited to cause grid instabilities and potentially blackouts
- Several attacks already demonstrated on smart edge systems (e.g., Smart meter energy theft attacks, HVAC on-off attack with the potential to disrupt grid operations etc)
- Lack of advanced and sophisticated cyber security techniques to detect sophisticated and highly targeted attacks

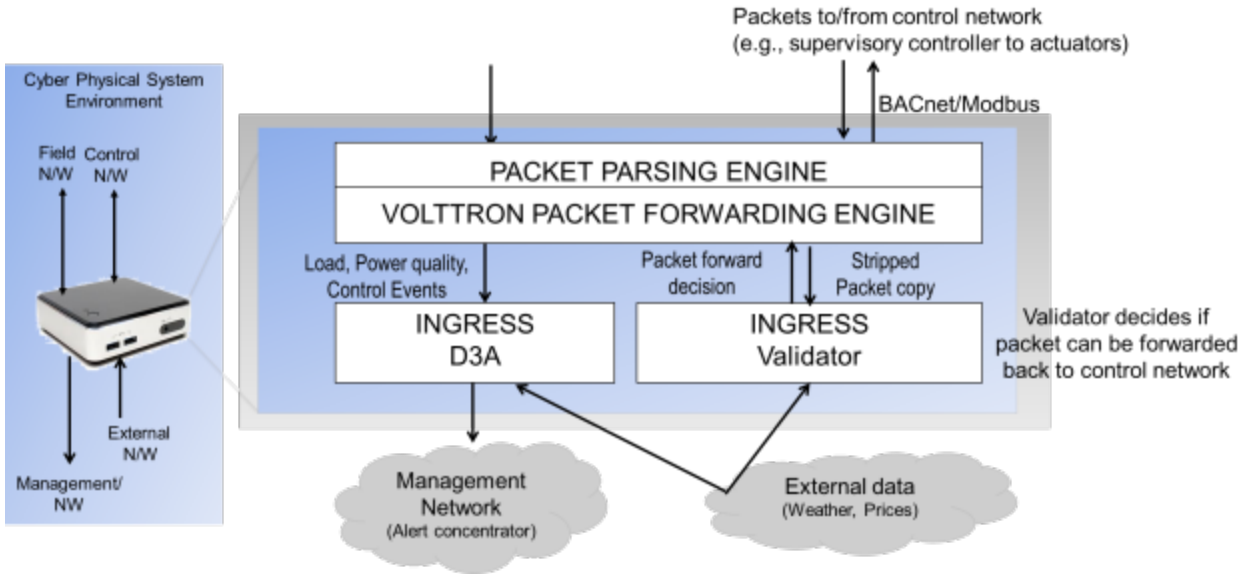
Gaps in existing solutions

- Encryption is not a panacea – especially difficulties in upgrading legacy systems
- Lack of efforts to validate **malicious but synthetically valid** control commands to edge systems
- Lack of solutions to detect and react to cyber/physical attacks on the edge devices
  - e.g., Stuxnet attack compromising the controllers
- Lack of interoperability with existing systems (how to communicate the detection events appropriately to 3rd party modules)

- Focus: **large scale coordinated attacks**, where adversary control a major segment of DER network/loads

Advancing the State of the Art (SOA)

The heart of INGRESS lies on the development of conceptual models of the controlled grid-edge devices in an automated and non-intrusive manner by harnessing machine learning and other dynamic adaptive techniques on the newly derived data streams (power quality sensors, control system operations)



Features

- An advanced attack detection and resiliency-enabling cybersecurity platform for behind-the-meter DERs
- Secure and interoperable communication with management systems and other INGRESS units
- Technology applicable to securing commercial buildings, residential units, plug-in electric vehicles, and smart inverters for solar integration.

Benefits

- Bump in the wire, transparently augments security into non-secure legacy and emerging systems
- Advanced cyber and physical attack detection and resiliency capability
- Interfacing with VOLTRON enables interoperability with a variety of different vendor network, hardware and software

Challenges to Success

Challenge 1 : Developing attack scenarios and deriving data set for model development

- Leveraged prior red teaming experiences, NESCOR electric sector failure scenarios
- Dataset generation using simulation models (GridLAB-D, MATLAB) and realistic data from (solar farm dataset from BNL, UTRC buildings test bed with EV)

Challenge 2 : Continuous use and update of models in noisy and adversarial environments

- Transfer learning
- Incremental learning

Challenge 3 : Performing technology validation involving actual physical devices connected to the HIL platform and utility partnership

- UTRC test bed, comprising of ~40,000 sq.ft buildings, office and lab, and EV network
- Phase II will connect to UIUC EV network and software based grid models
- Utility partner not yet identified and suggestions are welcomed

Challenge 4 : Determine the right set of DERs to develop models that can be applied to a broader group with minimal modifications

- Solar (NSERC and simulation), EV, and Buildings (office and lab)

Progress to Date

Major Accomplishments

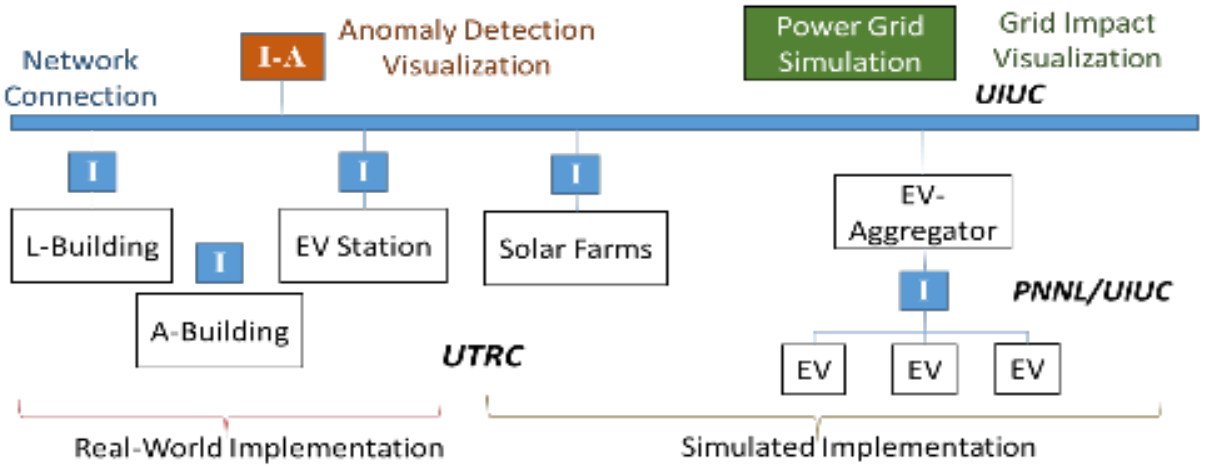
- Published results in leading conferences and journal (6 papers related to solar, buildings and EV)
- IP on “Systems and methods to detect anomalous building devices in building ", Patent no. 102153US01, 2018, filed on August 2018 by UTC CCS
- Demonstrated technology to DoD (NSA), ALC WebCTRL, NORESCO
- Outreach via invited talks (e.g., Kavli symposium by NYC, NREL, NSA)
- Developed packet validator, command validator and anomaly detector models for various classes of devices, using real/simulated data from sensors and CS
- INGRESS final system modules (PNNL packet validator, UIUC command validator and UTRC anomaly detector and visualization platform) are integrated with the sensors and deployed on UTRC campus
  - Real time communication of scores between INGRESS components and displayed using INGRESS visualization platform
  - Multiple validation using real time attacks on CS
  - Optimized software architecture for reduced communication and computation latency

Collaboration/Technology Transfer

- Most of the research results are published as journal or conference papers for knowledge transfer to the academia and the general public
- The targeted end user for the technology are the Asset Owner of the DERs, Vendor of DER or DER control system and possibly utilities
- Plans to gain industry acceptance
  - The INGRESS platform is tested on UTRC building automation system and will be transferred to UTC CCS (Climate Controls and Security), including Carrier and Automated Logic Control (ALC), for commercialization
    - IP filed via CCS, related to anomalous building operation detection using INGRESS
    - Team demonstrated potential of INGRESS platform to detect not only anomalous but also faulty building operations (e.g., unintentional flaw on control logic detected on Jan 2018)
  - The INGRESS platform will also be tested under different operation and attack scenarios of the Power Grid Simulation Platform to show impact on the energy sector so as to attract potential utility users
  - Open source INGRESS components via GitHub

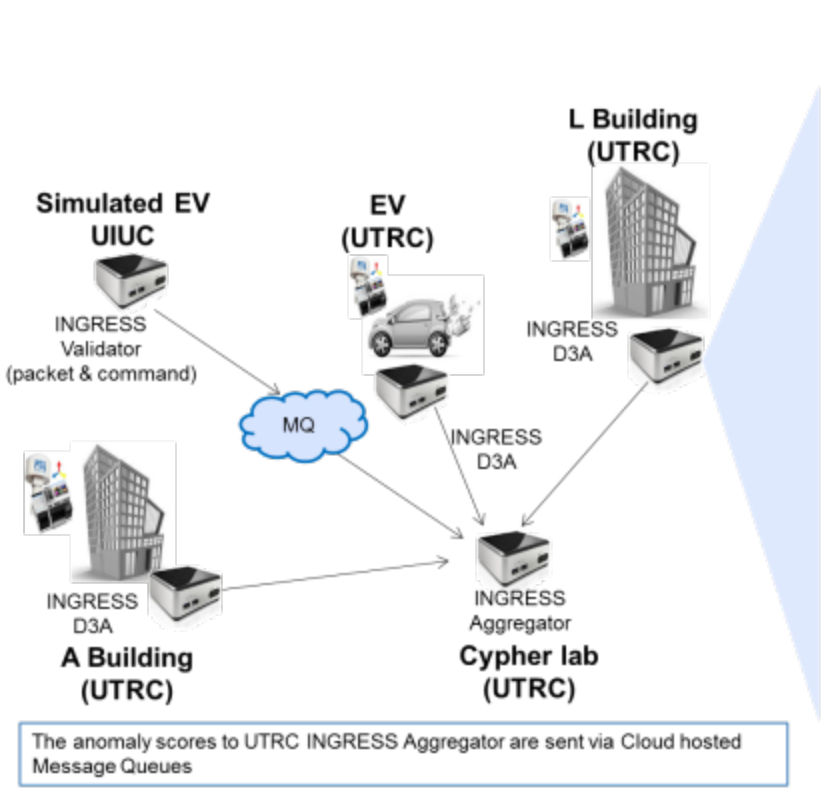
Next Steps for this Project

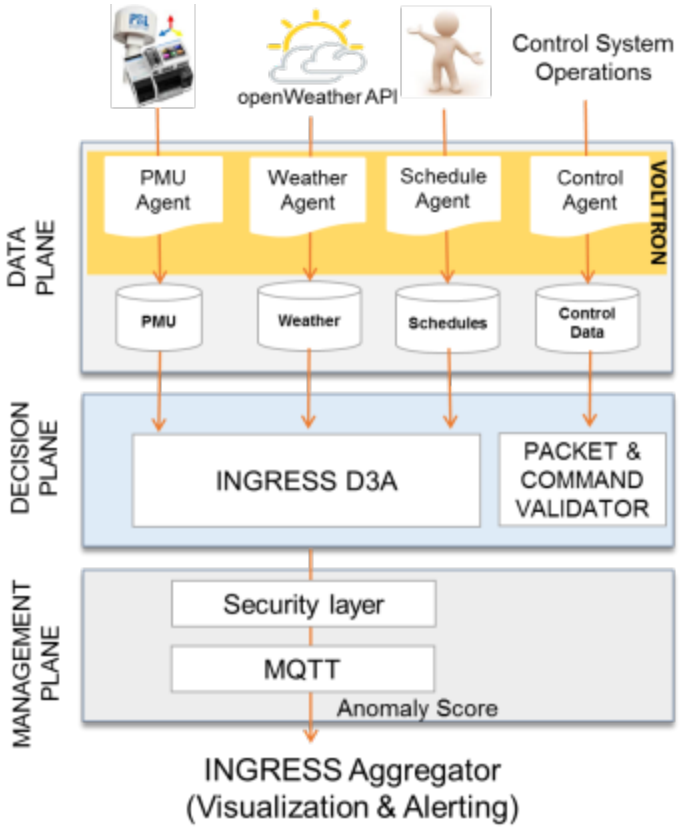
- Testing and validation of INGRESS modules, using normal and attack data
  - Metrics include false positives, missed detection, and comm./detection latency
- Integration of INGRESS and HIL components with the power grid simulation platform
- Development of attack scenarios under different operation conditions to demonstrate the attack impact and benefits of INGRESS platform
- Demonstrate the technology to DOE and potential customers (CCS, utilities)



Additional Slides

INGRESS D3A: System architecture and deployment





Additional Slides

INGRESS D3A algorithms based on PMU

μPMU Data Input

Voltage Phasors | Current Phasors | Power (Active, Reactive, Power Factor) | Frequency

Physics-based metric (DM)

- Captures transient behavior of loads
- Sampling Rate $f_s = 120\ Hz$

Correlation Matrix R
$R_{IV} = IV^*,\ R_{VV} = VV^*$ → Correlation Index $x = \left|\left|(I - uu^*)RR^*\right|\right|_F$

- (Quasi) steady-state: $x \cong 0$

Machine learning metric (ML)

- Predict next measurement using an RNN
- Trained on 2 weeks of normal data @$1Hz$
- Triggered by unpredicted events $x_t^{ML} = \left\|\hat{Y}_t - Y_t\right\|_2$
- Threshold value from distribution fitting $th = CDF_{ExponNorm}^{-1}(.99)$
- Multi-Module Detection allows different horizons and ML algorithms
- Random forest detection with customized feature extractor

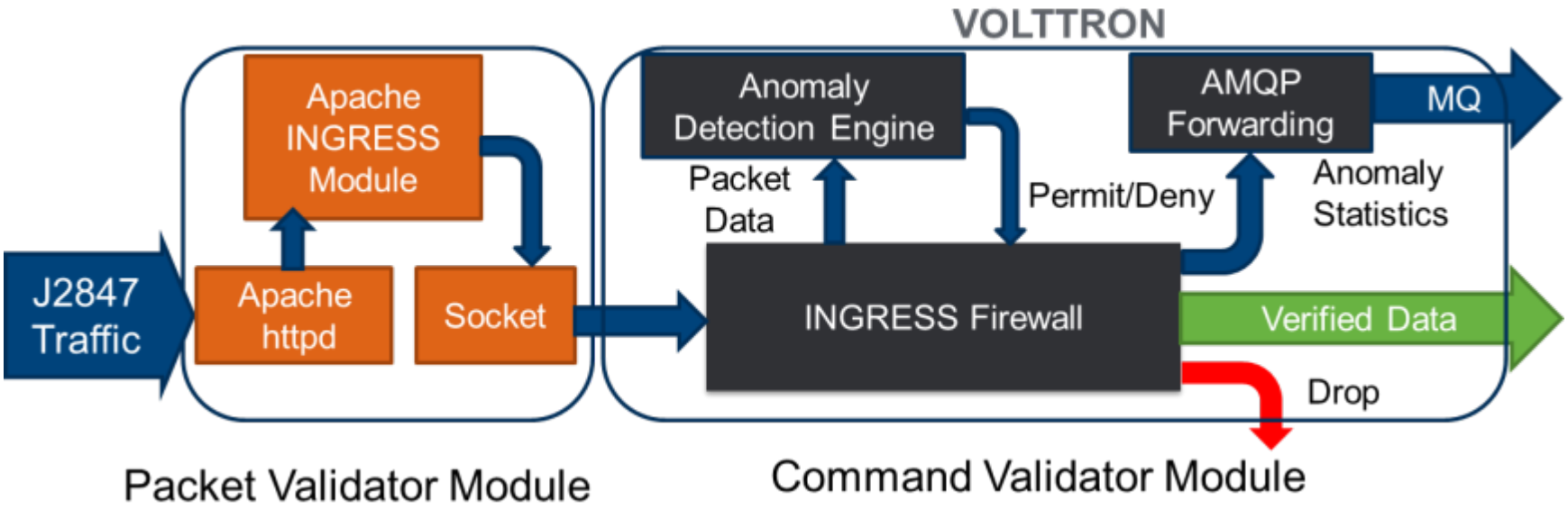
Fused score:

Additive Increase Multiplicative Decrease (AIMD) algorithm

$$z(t+1) = \begin{cases} z(t) + c & \text{if} \quad y_{DM} > T_{DM} \text{ or } y_{ML} > T_{ML} \\ \alpha z(t) & \text{else} \end{cases}$$

Additional Slides

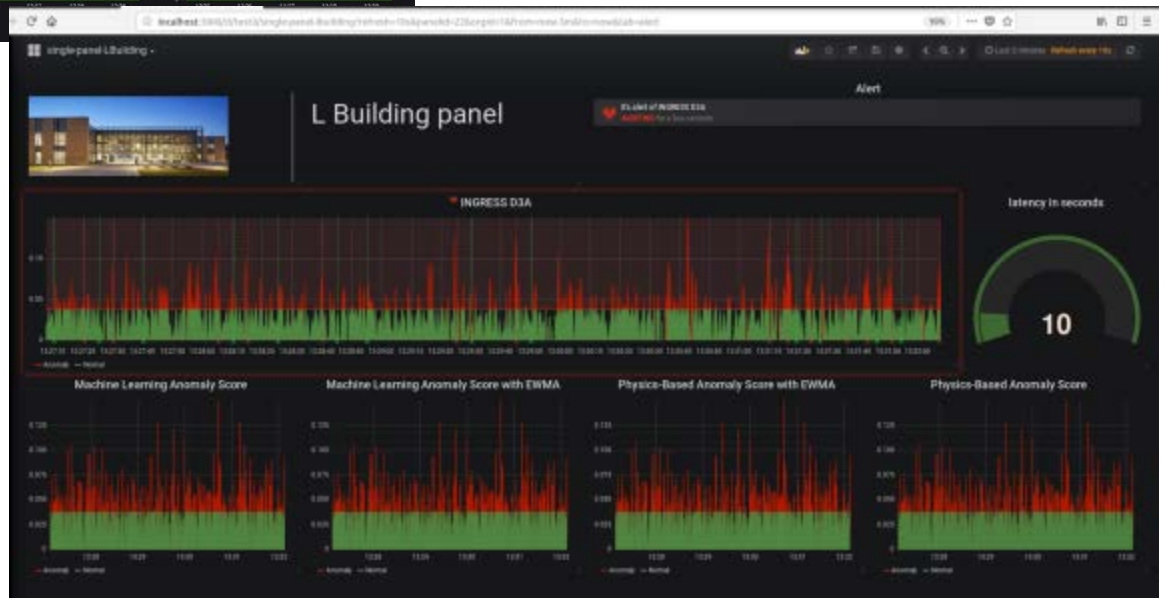
INGRESS Packet Validator and Command Validator - EV



Average packet size	Network Bandwidth	Inter-arrival time of packets	Average time taken by Anomaly Detection Engine
0.5 KB	9.6 to 56 kbps	0.07 to 0.5 s	0.0082 s

No false positives and false negatives were detected which proves the state machine is correctly implemented

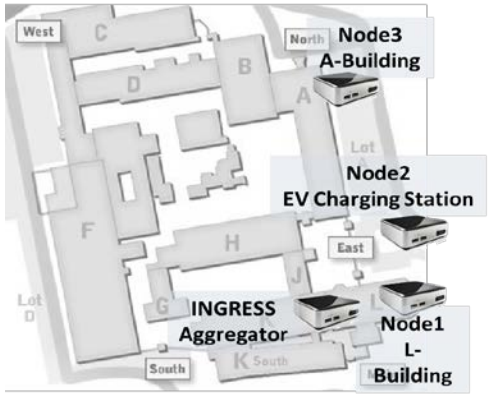
Additional Slide



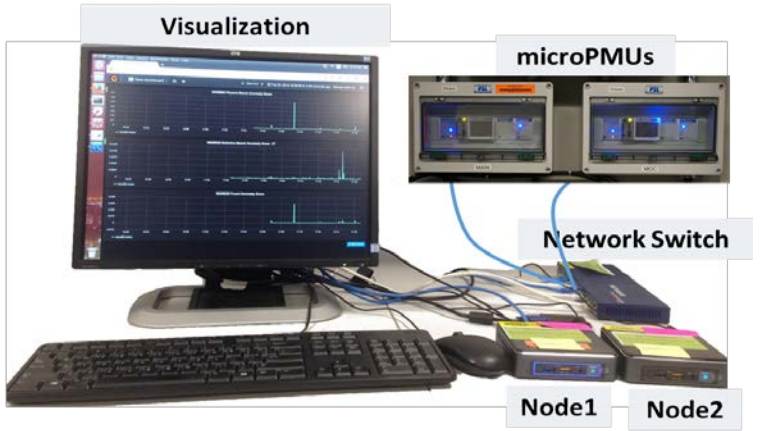
Additional Slides

INGRESS D3A – UTRC Deployment and Validation

Layout



Lab Setup

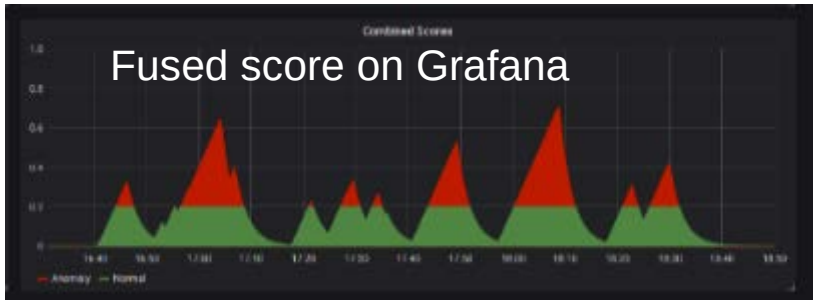


Attacks

AUTOMATEDLOGIC
United Technologies
WebCTRL

- ON/OFF Attack (3 types)
- Direct Speed Attack (3 types)
- Duck Static Pressure Attack (2 types)

Results

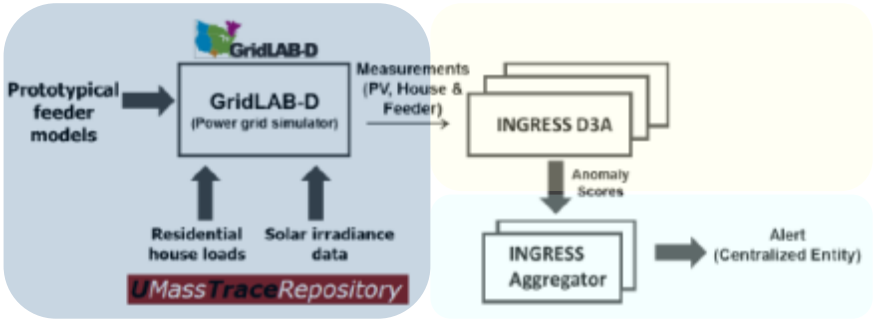


TPR 87.5%; FPR 0.5%
a time delay of 17 seconds

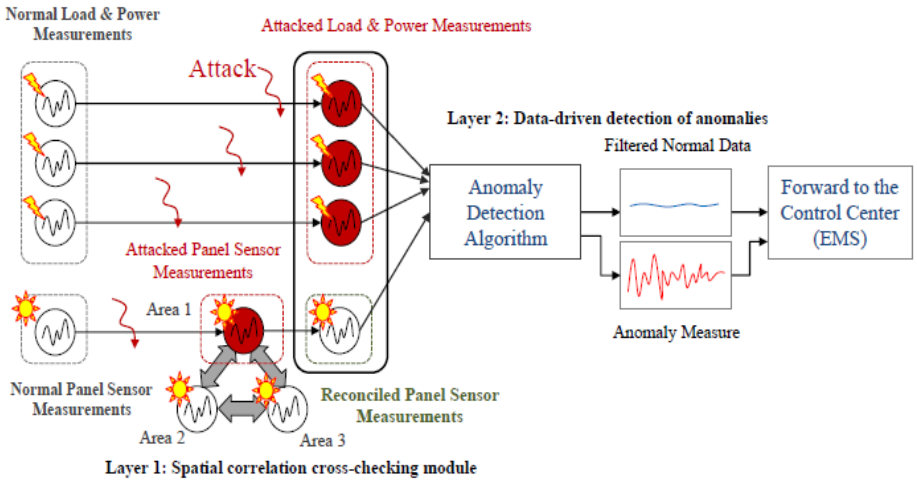
Additional Slides

INGRESS D3A for PV (residential and solar farm)

- GridLab-D based Feeder model, with 6K houses and 25% - 75% solar penetration
- Realistic home and solar datasets from UMass Trace Repository
- Four classes of attacks implemented and tested and solar features seemed to most powerful



Attack	All Combined	Disconnect	Reverse Power flow	Power Curtailment	VAR
Best Score F1	76.2%	85.5%	76.0%	70.7%	98.8%



- Real-world 3 area solar farm dataset
- 5 attacks are designed and 5 ML algorithms are tested
- Two-layer anomaly detection framework – intra and inter
- The two-layer structure is able to capture the spatial correlations in inter solar farms

Attack	Replay Attack	Correlated Attack	Random Attack	Delay Attack	Scaling Attack
Best Score F1	35.7%	23.8%	87.0%	89.5%	90.7%

Additional Slides

Thank you!

Devu M Shila, Ph.D
Associate Director, Research
United Technologies Research Center
manikad@utrc.utc.com