Secure and Resilient Cyber-physical Systems

Arupjyoti Bhuyan	An Innovative Secure & Energy Efficient Sub-Terahertz Wireless System for Sixth-generation (6G)
Jed Haile	Red Teaming Artificial Intelligence
Matthew Anderson	Secure and Resilient Machine Learning System for Detecting Fifth-generation (5G) Attacks including Zero-Day Attacks
Michael Cutshaw	Automated Malware Analysis Via Dynamic Sandboxes
Paul Talbot	Signal Decomposition for Intrusion Detection in Reliability Assessment in Cyber Resilience
Ruby Nguyen	A quantitative approach to multiple critical supply chain resilience assessment

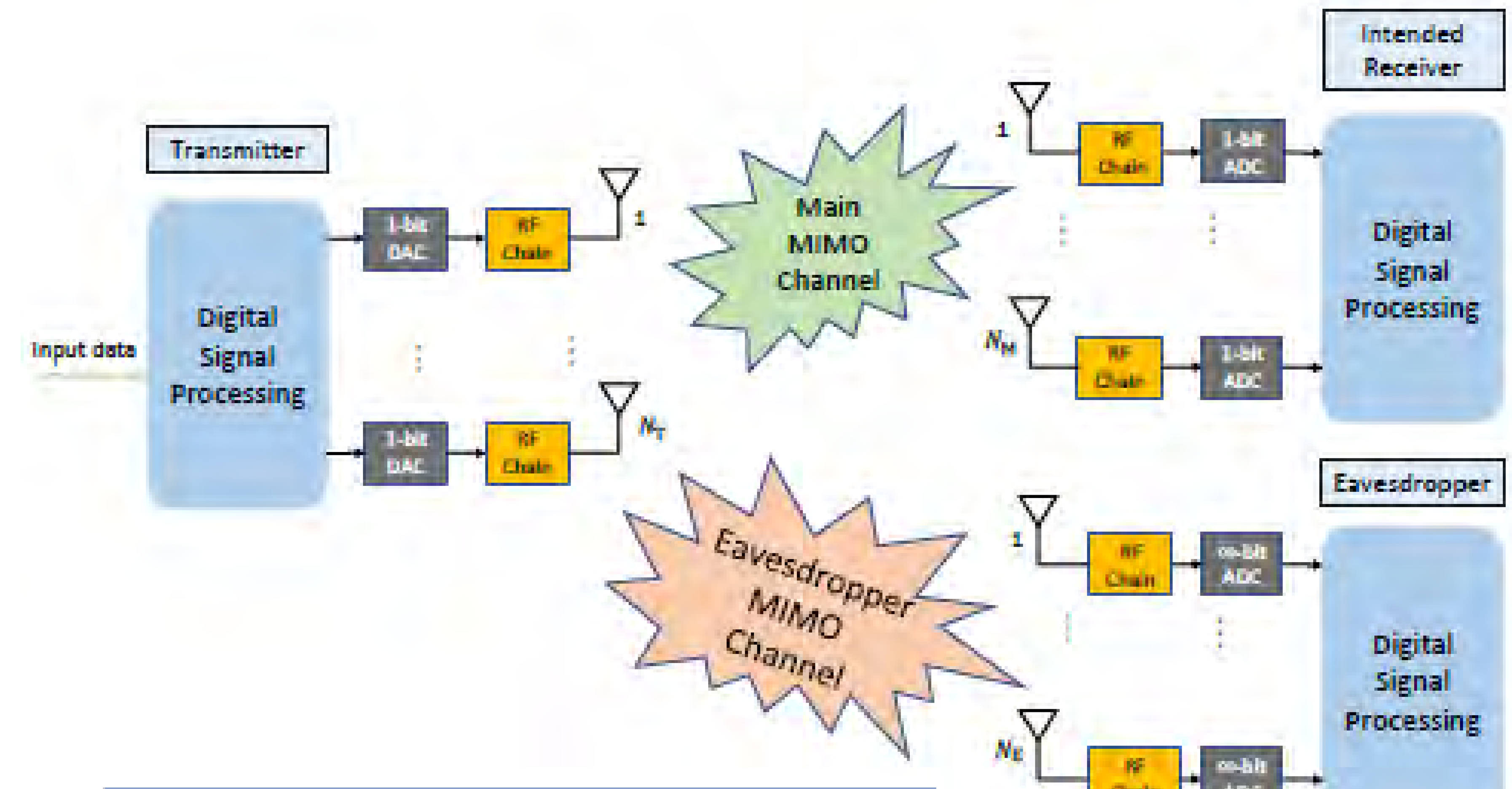
Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517."

Secure & Energy Efficient Sub-Terahertz Wireless System for 6G

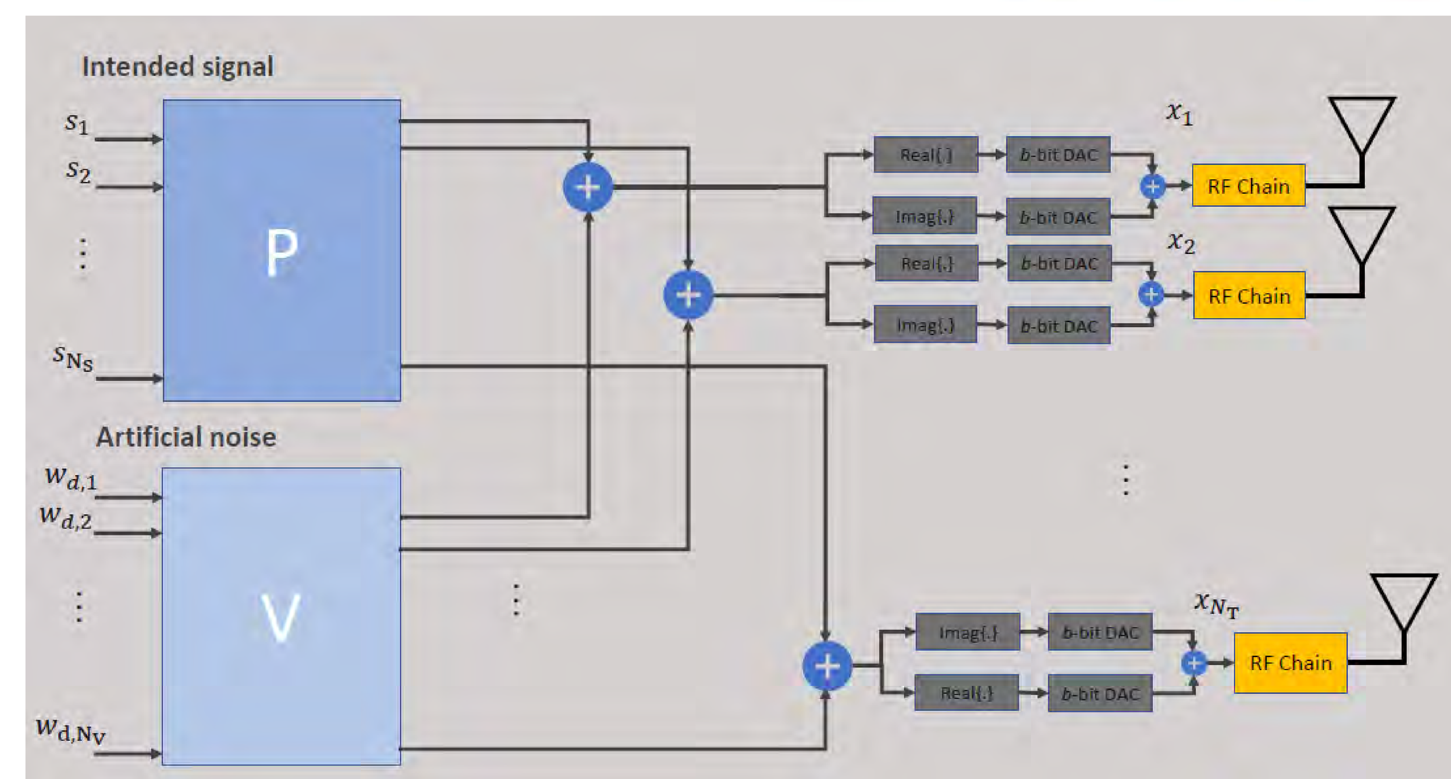
Arupjyoti (Arup) Bhuyan (INL), Robert Heath (North Carolina State University)

Need and Significance

- Required energy efficient 6G **low resolution multiple-input and multiple-output (MIMO) systems degrades security.**
- This research proposes to prove the principle that **security can be designed into low resolution 6G MIMO system** that operates in the sub-Terahertz (100-300 GHz) bands.
- Successful conclusion will **lead to secure next generation cellular systems worldwide.**



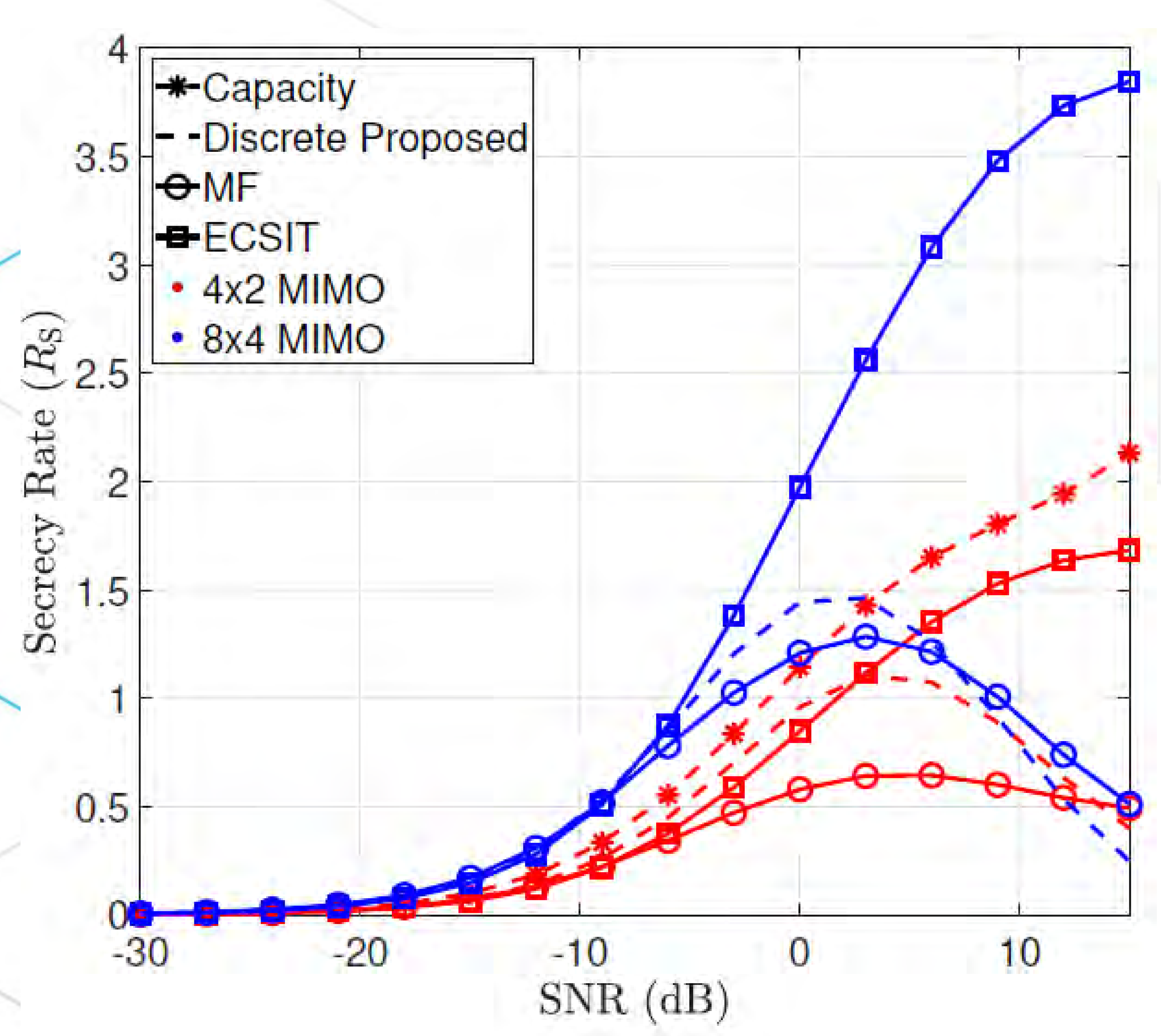
$$\mathbf{x} = \mathcal{Q}(\mathbf{z}) = \mathcal{Q}(\phi \mathbf{P}\mathbf{s} + (1-\phi)\mathbf{V}\mathbf{w}_{\mathrm{D}})$$



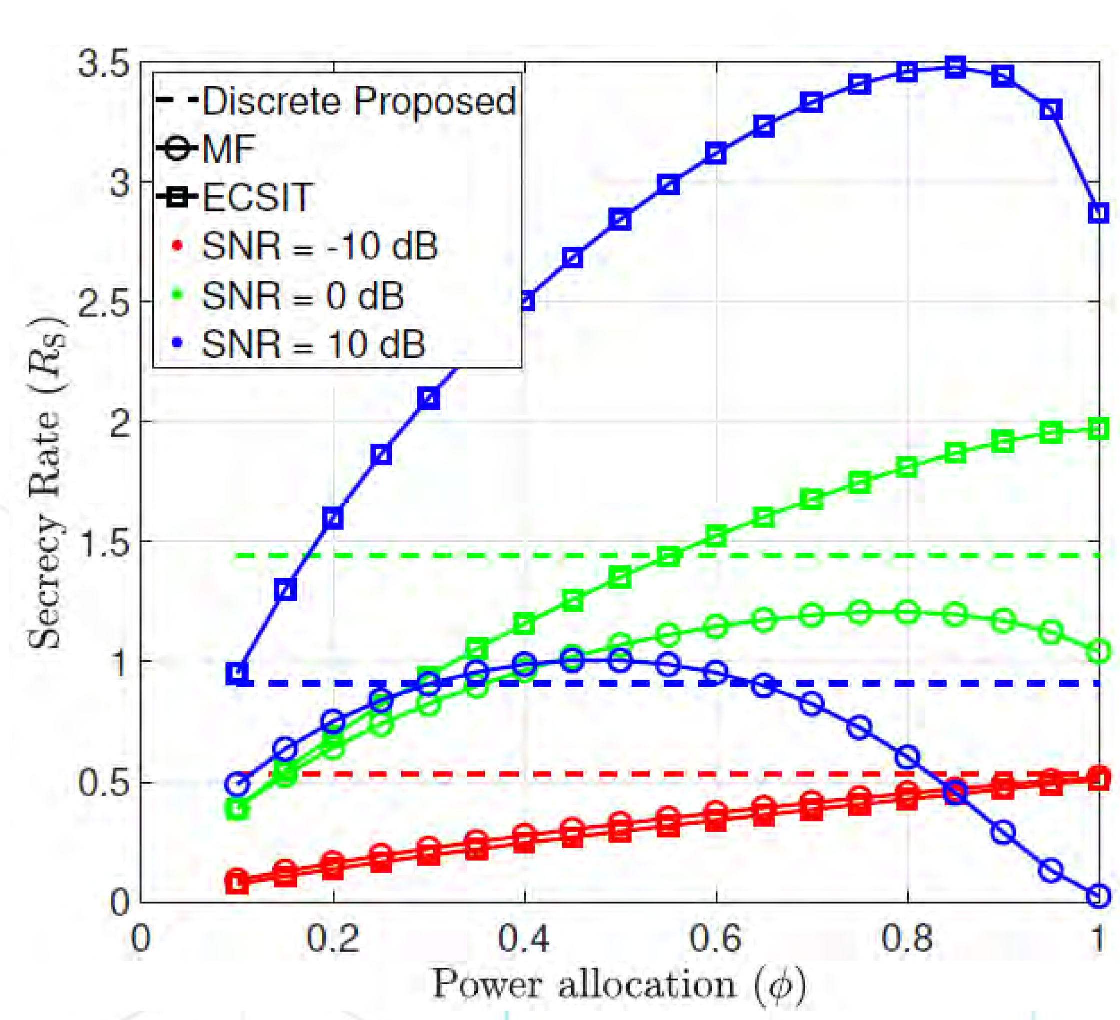
Approach and Innovative Aspects

- Use directional modulation (DM) in low resolution systems
- Transmit artificial noise and symbols to increase secrecy rate/capacity

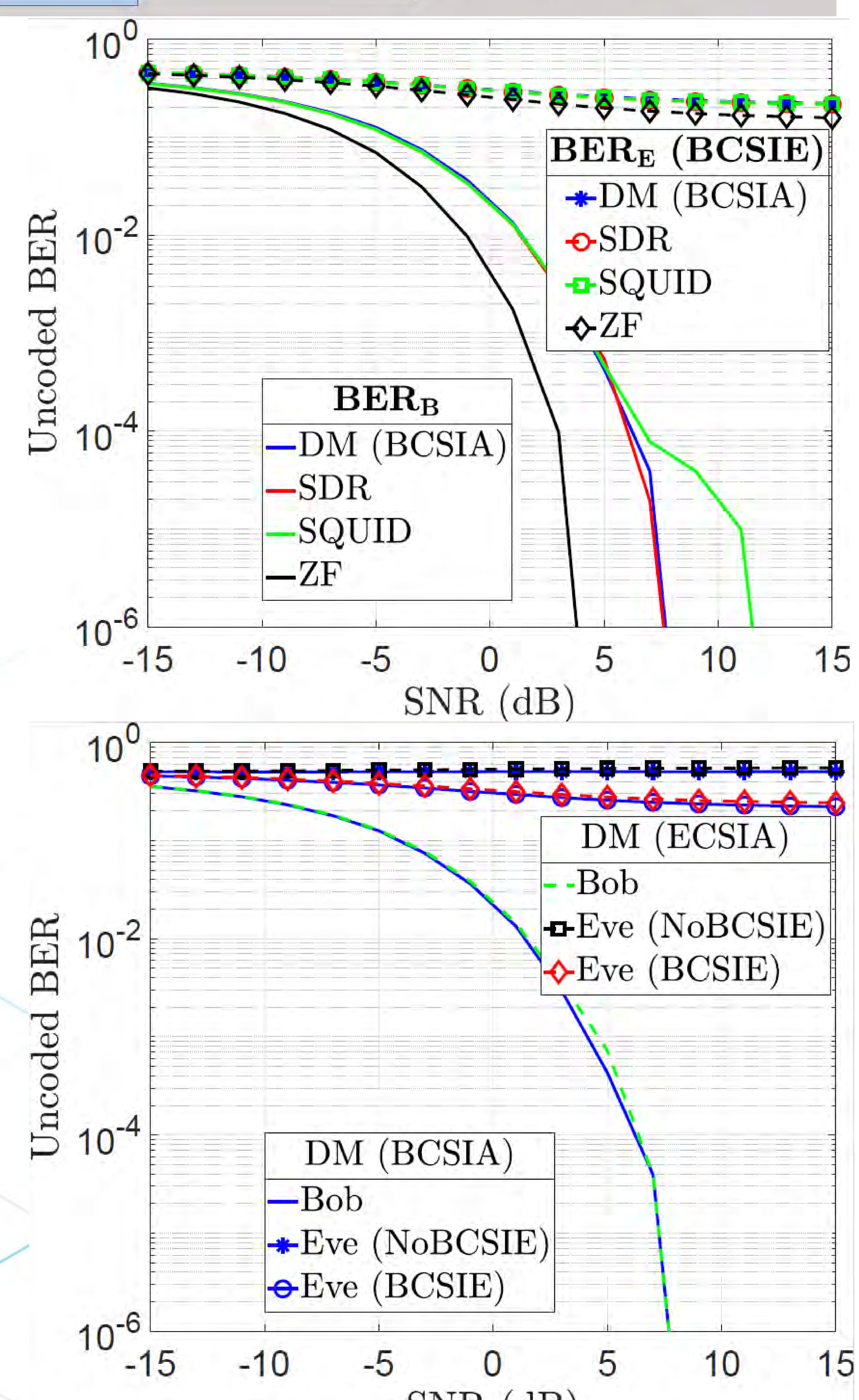
Summary of Results



Secrecy rate for low resolution MIMO



Secrecy rate as function of Signal vs. Artificial Noise power allocation



Performance of Direction Modulation in Low Resolution MIMO

Publications

- “Physical Layer Security at a Point-to-Point MIMO System With 1-Bit DACs and ADCs”, IEEE Wireless Communications Letters, May 2023.
- “Directional Modulation-Aided Secure MIMO Communication Using 1-Bit Converters”, submitted to IEEE Transactions on Vehicular Technology, Feb 2023.
- “An Innovative Secure & Energy Efficient Sub-Terahertz Wireless System for 6G”, INL Invention Disclosure Record (IDR) BA-1289.

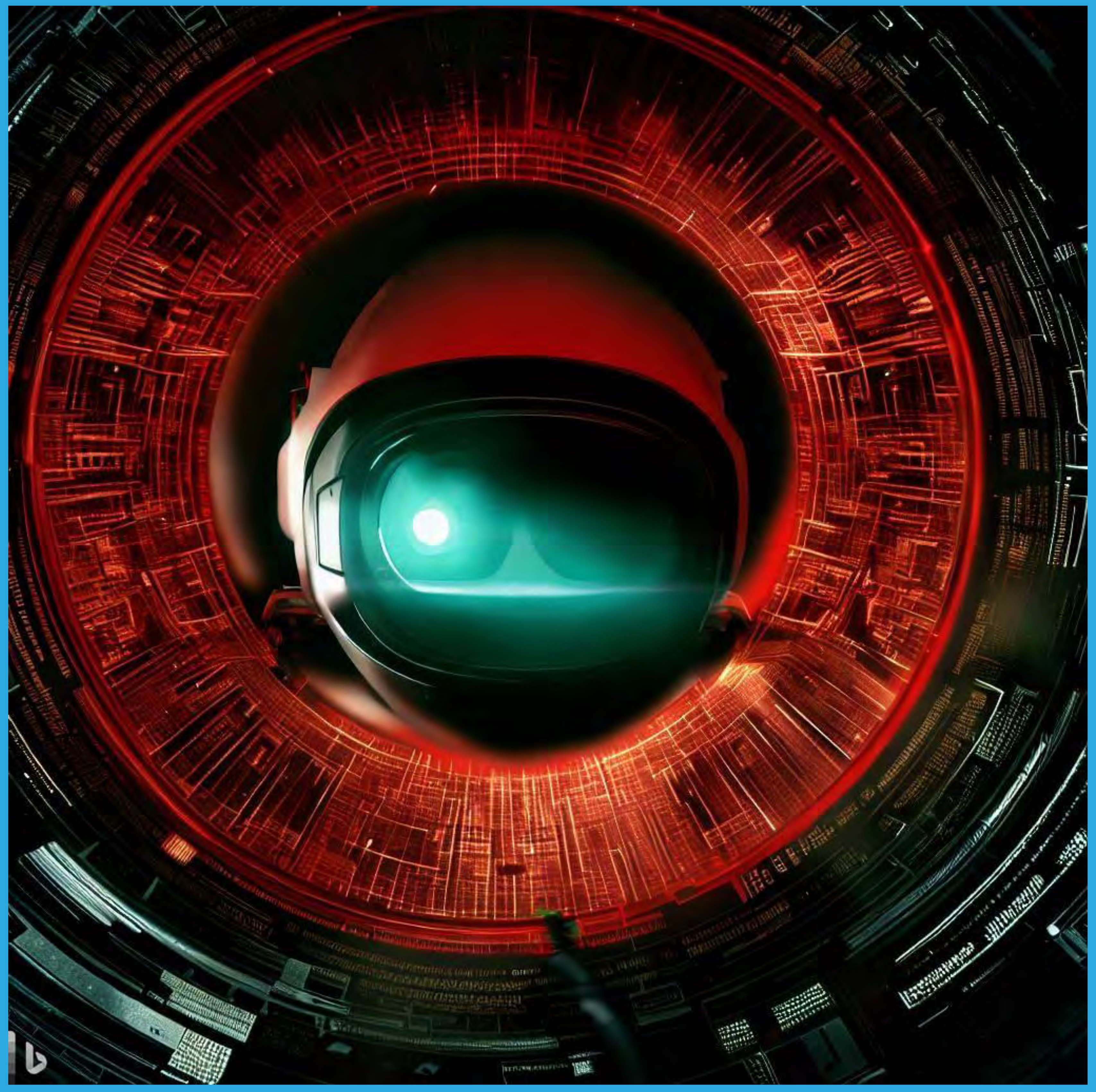
Project Number: 22A1059-031FP

LRS Number: INL/MIS-23-74197

Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

Red Teaming Artificial Intelligence:

Investigating the utility of red team security audits on machine learning



Jed Haile, Idaho National Lab
Dr Mike Borowczak, University of Wyoming

Method:

- Identify commonly used AI/ML toolkits, application programming interfaces
- Investigate deployment scenarios and technologies
- Search for reported vulnerabilities and exploits
- Determine if tactics and techniques used in red team attacks on Enterprise systems are applicable and sufficient
- Research the difficulty, expense and impact of novel vulnerability research on the most used tools and models

Outcomes:

- Rapidly changing target environment and rapid rates of development have led to short time frames between vulnerability disclosure and mitigation
- The trend is moving from self hosting to using cloud providers such as OpenAI and Azure
- Popular machine learning frameworks do not include functionality to expose the model on a network, direct access to the model is in process only
- Typical deployment scenario is a simple REST API providing a prediction or generation endpoint resulting in a small attack surface
- Models are trained on large corpora of diverse origin, meaning input validation is strong by necessity
- Machine learning programming uses specialized tools and techniques which are uncommon in general programming
- Fuzzing and static code analysis were not productive, indicating developers use these techniques
- Student researchers with knowledge of vulnerabilities and machine learning are not available
- Experienced vulnerability researchers found it challenging to audit these systems due to the highly specialized nature of machine learning code
- Effective red team assessment of requires the development of knowledge, tools and techniques specific to the domain

Code metrics of popular machine learning frameworks

Framework	Files	All Lines	Lines of Code
Caffe	576	107,928	80,256
Tensorflow	11,219	3,310,964	2,465,296
PyTorch	5,451	1,141,599	903,967

Historic CVE trends for CUDA enabled hardware

Year	Matches	Total	Percentage
2006	2	6608	0.03%
2007	1	6516	0.02%
2008	0	5632	0.00%
2009	0	5732	0.00%
2010	0	4639	0.00%
2011	4	4150	0.10%
2012	2	5288	0.04%
2013	4	5187	0.08%
2014	3	7937	0.04%
2015	8	6487	0.12%
2016	43	6447	0.67%
2017	60	14643	0.41%
2018	24	16509	0.15%
2019	43	17305	0.25%
2020	48	18350	0.26%
2021	107	20158	0.53%
2022	92	25101	0.37%
2023	73	18443	0.40%

Project Number: 21A1050-088FP
LRS Number: INL/MIS-23-74386 Rev:000

www.inl.gov

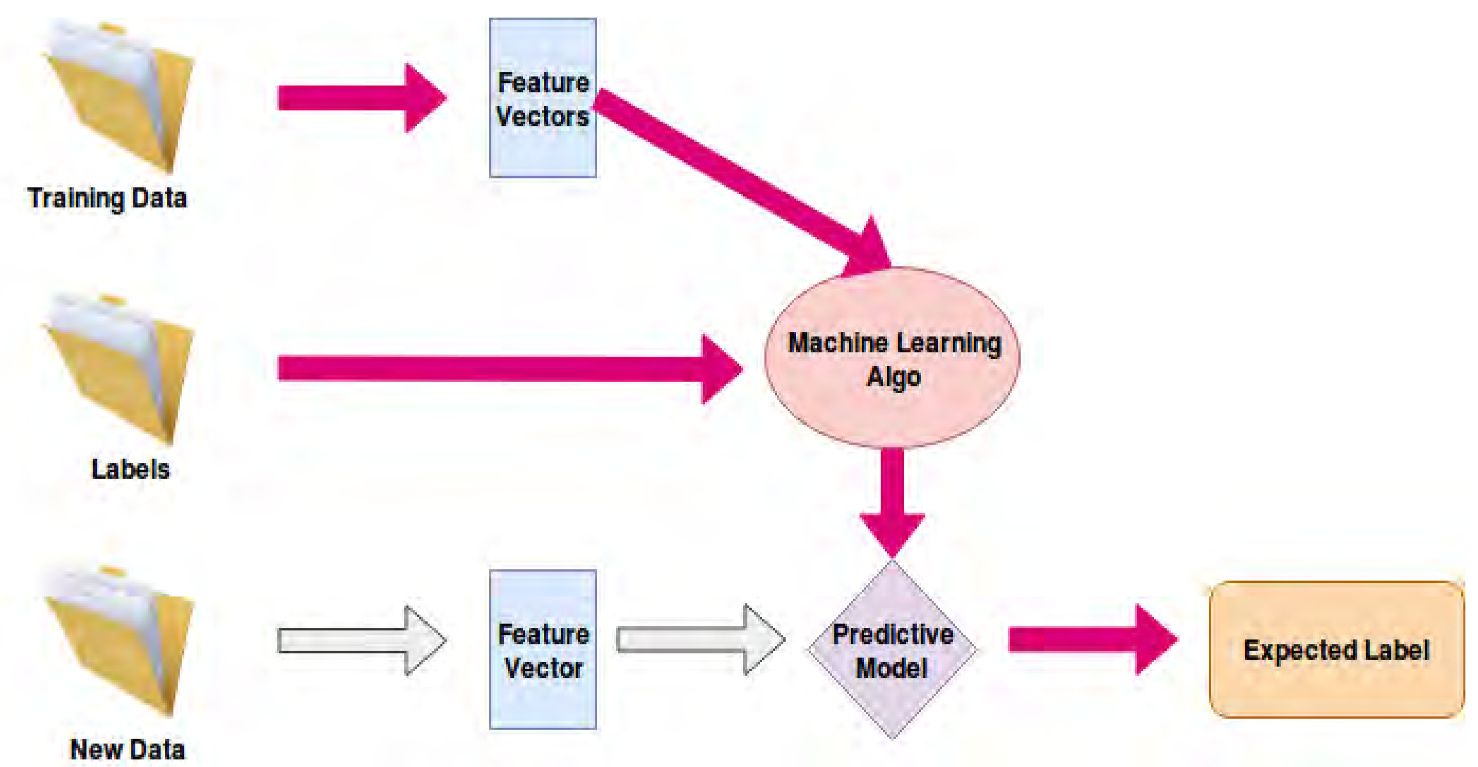
Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517."

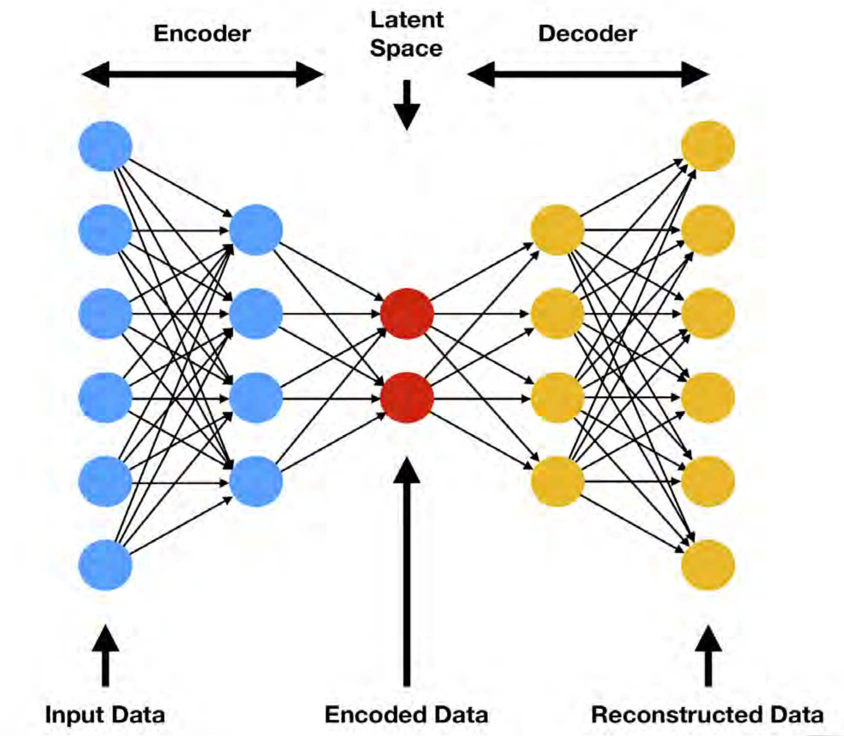
Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Secure and Resilient Machine Learning System for Detecting 5G Attacks including Zero-day attacks
22A1059-018FP PI: Matthew Anderson INL/MIS-23-74183

Identifying anomalies in 5G networks via deep packet inspection of the payload with the use of machine learning deployed on a FPGA.





Objective 1: Analyze

As the packets move across the network, they are inspected by the machine learning program. The header is ignored because the program focuses on the payload.

Objective 2: Detect

Based on the training of the autoencoder and classifier, the program will be able to detect if there is anomalous data in packets. Anomalous data includes malware and unusual network traffic.

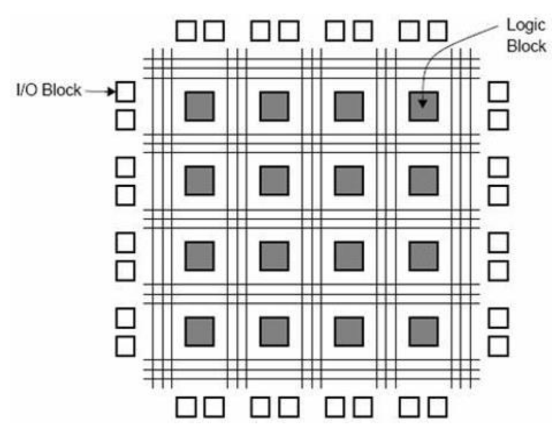
Objective 3: Visualize

Each packet is plotted on a graph in the cluster that they belong to spatially.
The packets are also classified into different categories and visualized in different colors.

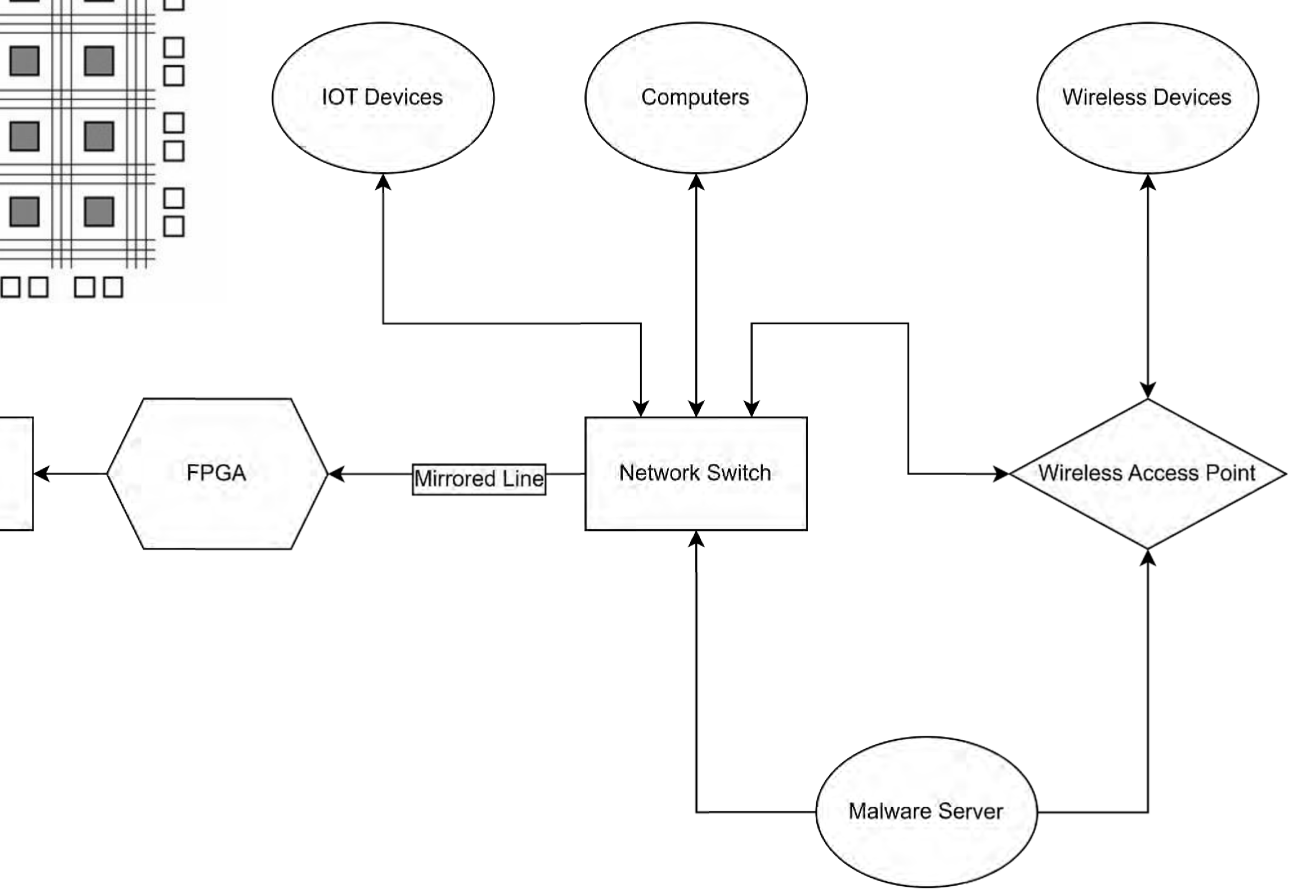
Viruses Tested

- Nonstop_Virus
- Backdoor_payload
- Lokibot
- Putingods
- Sandworm
- Vawtrak
- Trickbot

FPGA Diagram



Test Bed Diagram

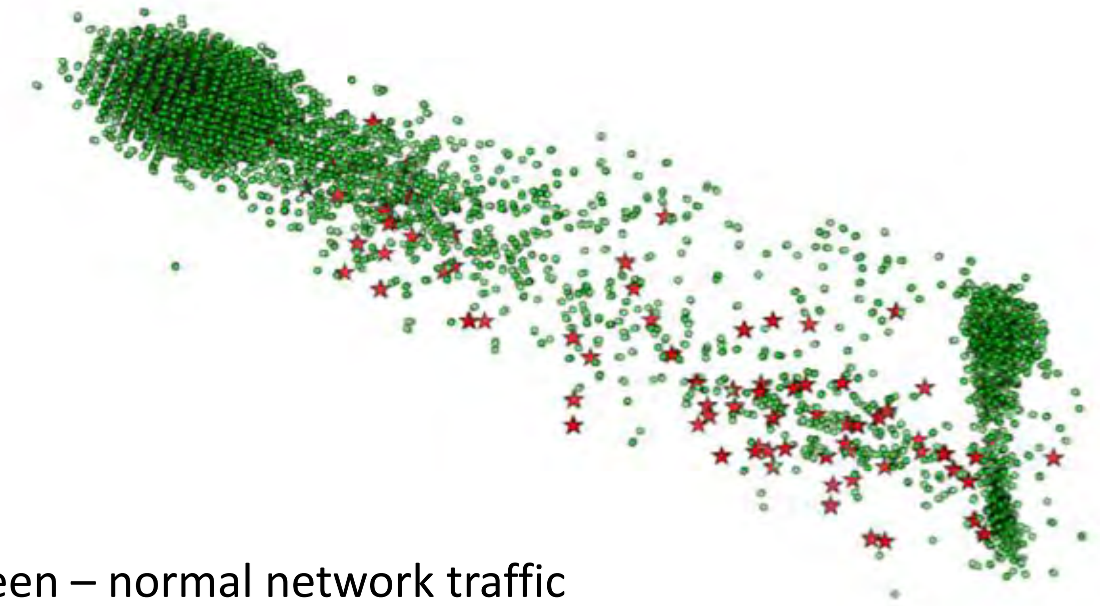


FPGA

- Field Programmable Gate Arrays(FPGA) are integrated circuits designed to be customized after manufacturing.
- This design is capable of handling large amounts of incoming data through parallelism.
- We then use our AI to detect anomalous data and visualize it with very little latency, or delay.
- The FPGA we used, the Xilinx ZCU104, currently uses around 10W of power compared to the power draw of the Nvidia A100, at 400W.

Machine Learning

- The model combines a Variational Autoencoder (VAE) with classifiers for real-time anomaly detection in 5G network traffic, optimized for FPGA.
- Through a delicate balance between throughput and accuracy, the model ensures live operation on FPGA and meeting 5G's speed requirements.
- A custom VAE architecture is adapted for network traffic analysis, its latent space trained with Maximum Mean Discrepancy(MMD) for interpretability and identification of malicious traffic.



Green – normal network traffic
Red – anomalous network traffic

Patents: 17/663,883
BA-1503
Software Disclosures: CW-23-34
Gitlab.com/IdahoLabResearch/5GAD
Publications: "Machine Learning 5G Attack Detection in Programmable Logic", 2022 IEEE Globecom doi:10.11578/dc.20220811.1
"Machine learning models for network traffic classification in Programmable Logic", 2022 IEEE HST doi:10.1109/HST56032.2022.10025442

PI: Matthew Anderson
www.inl.gov
Ben Mahoney
Brian Allen
Brighton Roskelley
Denver Conger
Keaton Roberts

Automated Malware Analysis

Via Dynamic Sandboxes

Presenter: Michael Cutshaw

BACKGROUND:

Manual malware analysis:

- Requires specialized labor
- Time consuming
- Does not scale

Analysis through sandboxes:

- Captures behaviors:
  - IP addresses
  - Domain names
  - Files modified or read
  - System calls
- Rapid analysis
- Highly scalable

Current state of the art (sandboxes):

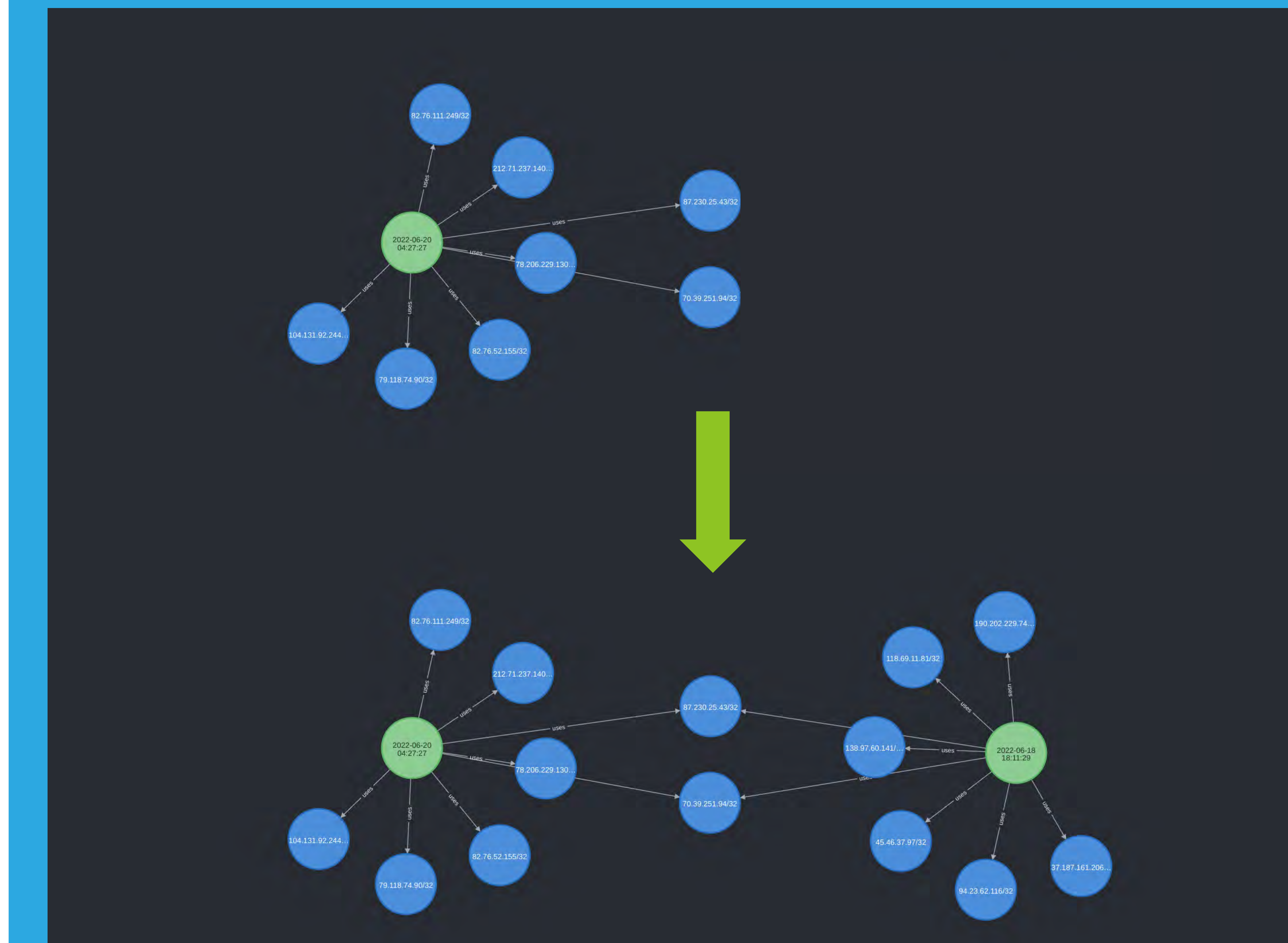
- Unaggregated results
- focuses on malicious/benign classification
- Sandbox specific output

Our Solution:

- Translates individual results into STIX:
  - Interoperable
  - Graph enables aggregated analysis
- Leverages virtualization for:
  - Wide range of processor architectures
  - ICS/Embedded emulation

https://github.com/idaholab/cape2stix

Scalable dynamic malware analysis framework. In a shareable, graph format.



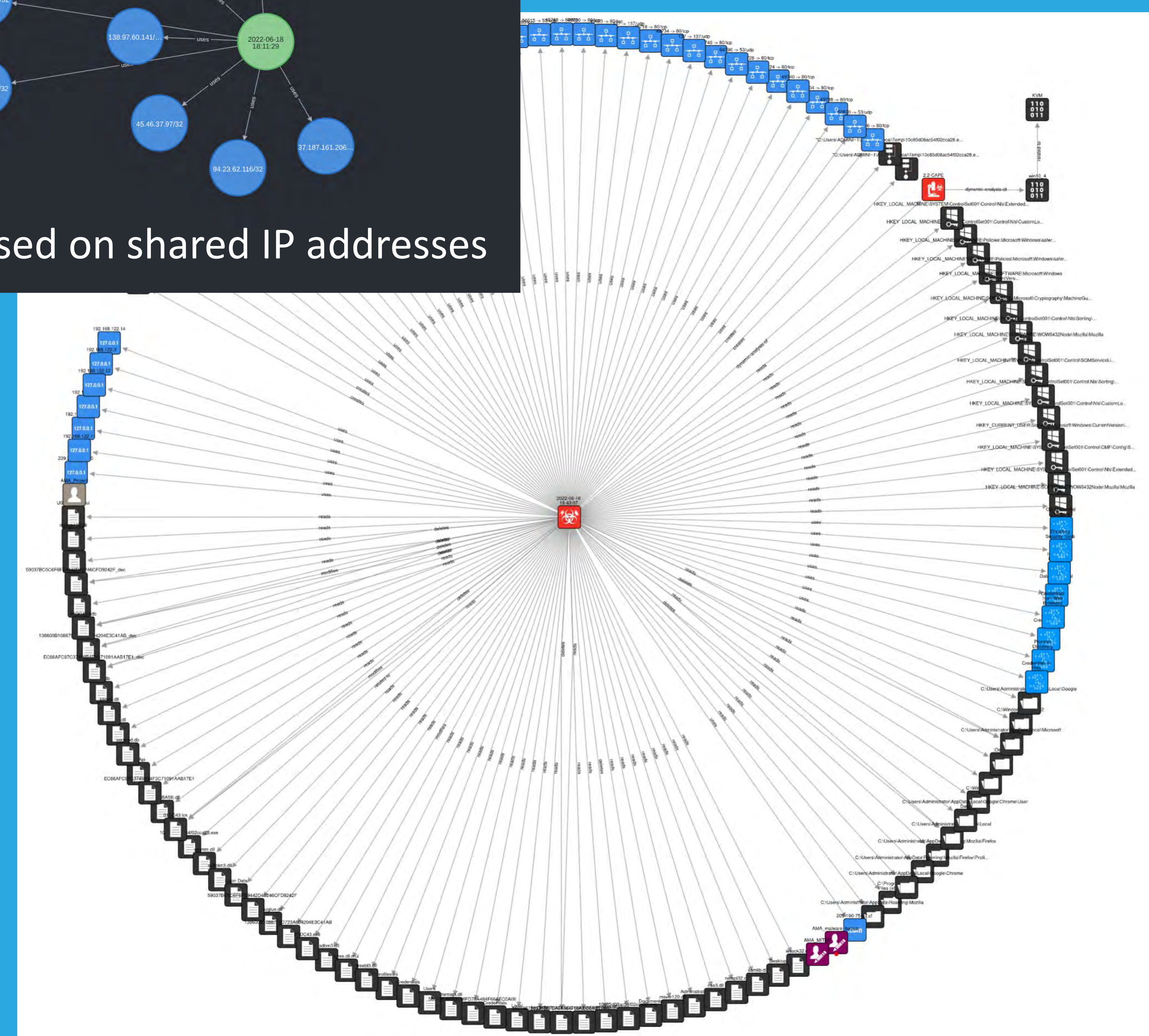
Emotet malware being linked based on shared IP addresses

Determine similarities through shared behavior

Automatic linking based on behavior hashing

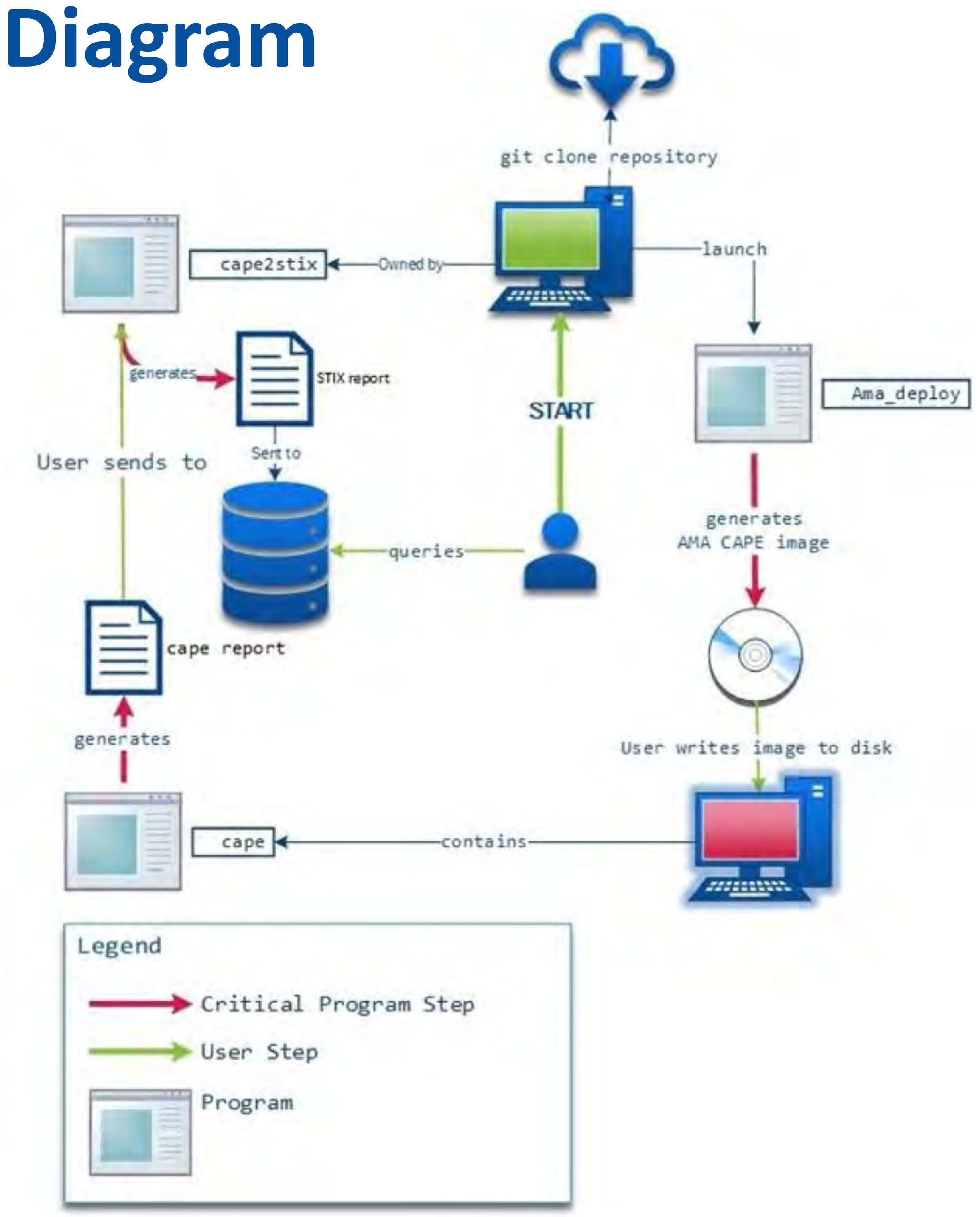
~90,000 executed samples

Over 600,000 samples collected total



Single malware sample with all behaviors (shown in STIG)

Architecture Usage Diagram



Samples	681,573
Total Size	465 GB
Unique Attack Patterns *	57
Nodes *	747,728
Edges *	12,117,818
Shared Nodes *	8,715,527

*Represents results from first 20,000 samples analyzed

Michael Cutshaw, Will Brant, Zachary Priest, Bryan Beckman, Micah Flack, Taylor McCampbell

Project Number: 22A1059-060FP   LRS Number: INL/EXP-23-74295

www.inl.gov

Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517."

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

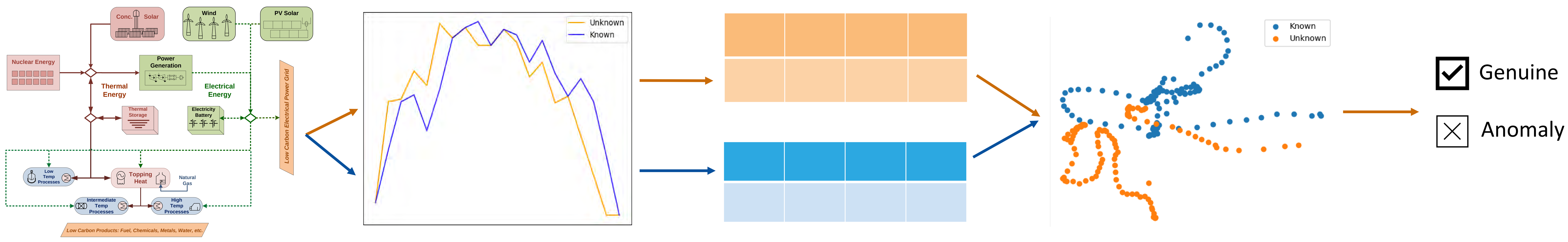
Idaho National Laboratory

Signal Decomposition for Intrusion Detection

in Reliability Assessment in Cyber Resilience

Paul Talbot, Dylan McDowell, Bri Rolston, Xingyue Yang, Luis Nunez, Blaine Bockholt, Idaho National Laboratory
Hany Abdel-Khalik, Yeni Li, Tyler Lewis, Purdue University

Background and Motivations



Complex Systems

Securing cyber resilience for systems with complex physical process interactions becomes challenging as the system becomes more interconnected, such as in nuclear-hydrogen-renewable energy grids.

Signals

An intruding entity with malicious intent may gain access to a system and cause damage by "spoofing" signals coming from installed sensors.

Characterization

We can identify subtle changes to the signal by using a toolbox of different characterization methods that will compare characteristics from a known signal with an incoming unknown signal.

Visualization

Detection of these changes might be invisible to the naked eye but are much more apparent when the signal is transformed into a different characterization space.

Results

We can numerically assess the difference between our known and unknown signals by applying a distance metric that will categorize the signal as "Genuine" or "Anomaly."

Implementation

- Novel software: Signal Oriented Network Anomaly Recognition (SONAR)
- Built on Risk Analysis Virtual ENvironment (RAVEN) framework
- SONAR is accessible to Purdue and INL researchers for training and detecting anomalies in digital-physical signals
- Enables automated formatting, construction, and analysis of signal anomaly detection scenarios with comprehensive documentation and data visualization tools

Summary

- Identifies anomalies in datasets using distance metrics and data-based decomposition techniques
- Particularly adept at detecting subtle and distant anomalies, such as identifying adversarial attacks in sensor data for critical infrastructure protection
- Demonstrates versatility in many applications, such as nuclear reactor simulations, seismic events, and 3D printing temperature monitoring
- Showcases broad usability across diverse data types and settings

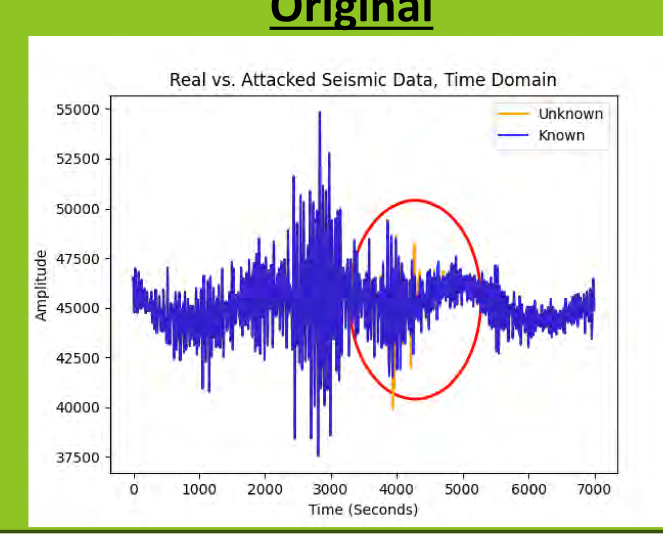
What's Next?

- Enhanced application through multi-signal correlation and regime detection, yielding significant detection improvement
- Future research potential in refining software usability for non-developer experts and exploring new directions
- Building on established research foundation to seize opportunities in advancing SONAR capabilities

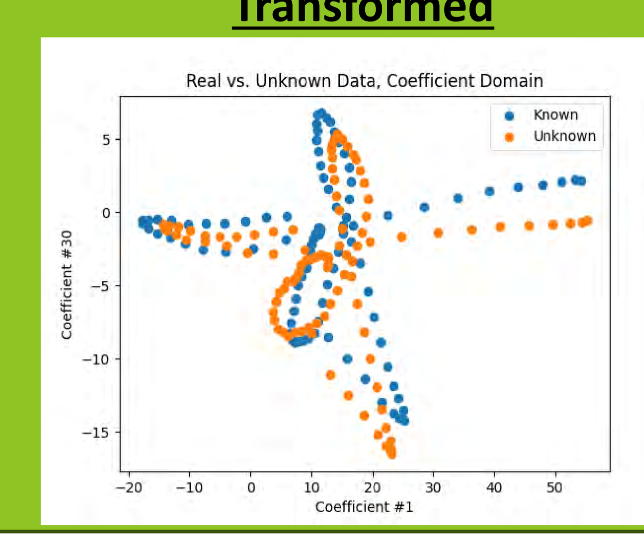
Case study: Seismic Event

Safe nuclear reactor systems monitor seismic activity to respond to significant events. SONAR demonstrates detecting anomalous false data injections that are too subtle to be seen by the eye, but are clearly different in characterization space

Original



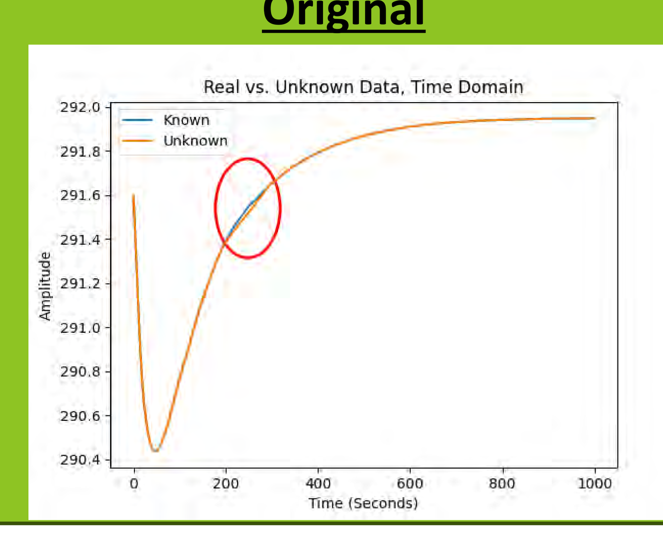
Transformed



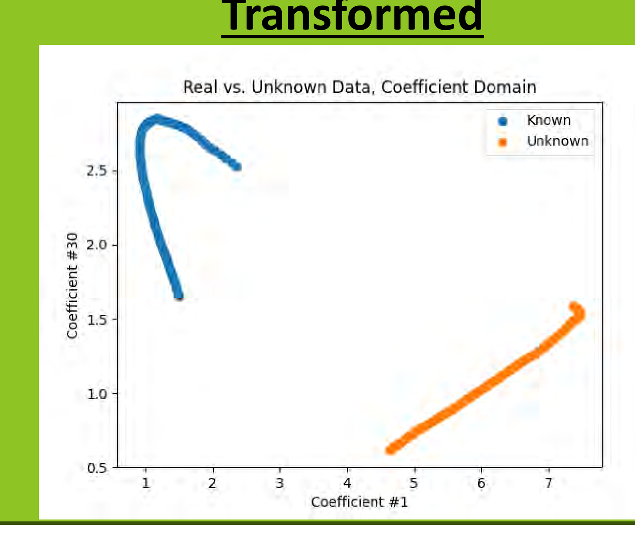
Case study: RELAP5 Simulation

SONAR can also be used in digital twin applications, such as using RELAP to monitor system thermal hydraulics. This example case considers coolant temperature at reactor core inlet of a nuclear reactor, and a subtle perturbation injected to the signal.

Original



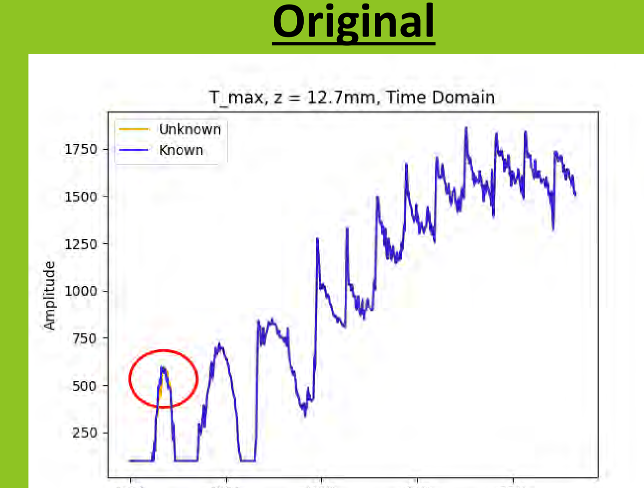
Transformed



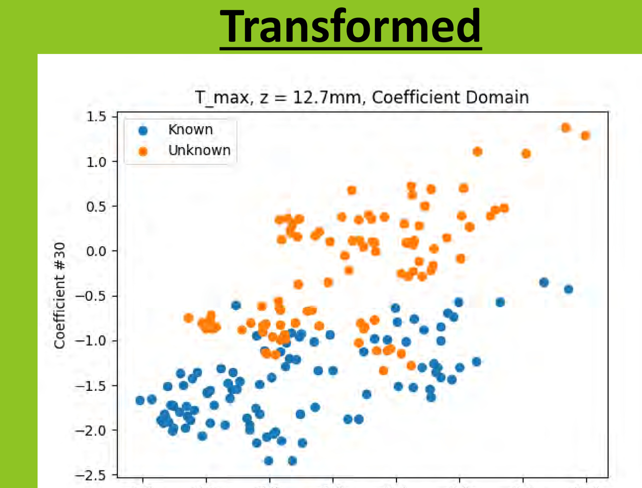
Case study: 3D Printing

In 3D printing for complex materials, temperature pools are measured to ensure correct behavior. SONAR detects even subtle data changes to the measured temperatures. Injecting data into an additive manufacturing process may result in compromised components downstream.

Original



Transformed



Project Number: 21A1050-024FP LRS Number: INL/EXP-23-74091

Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517

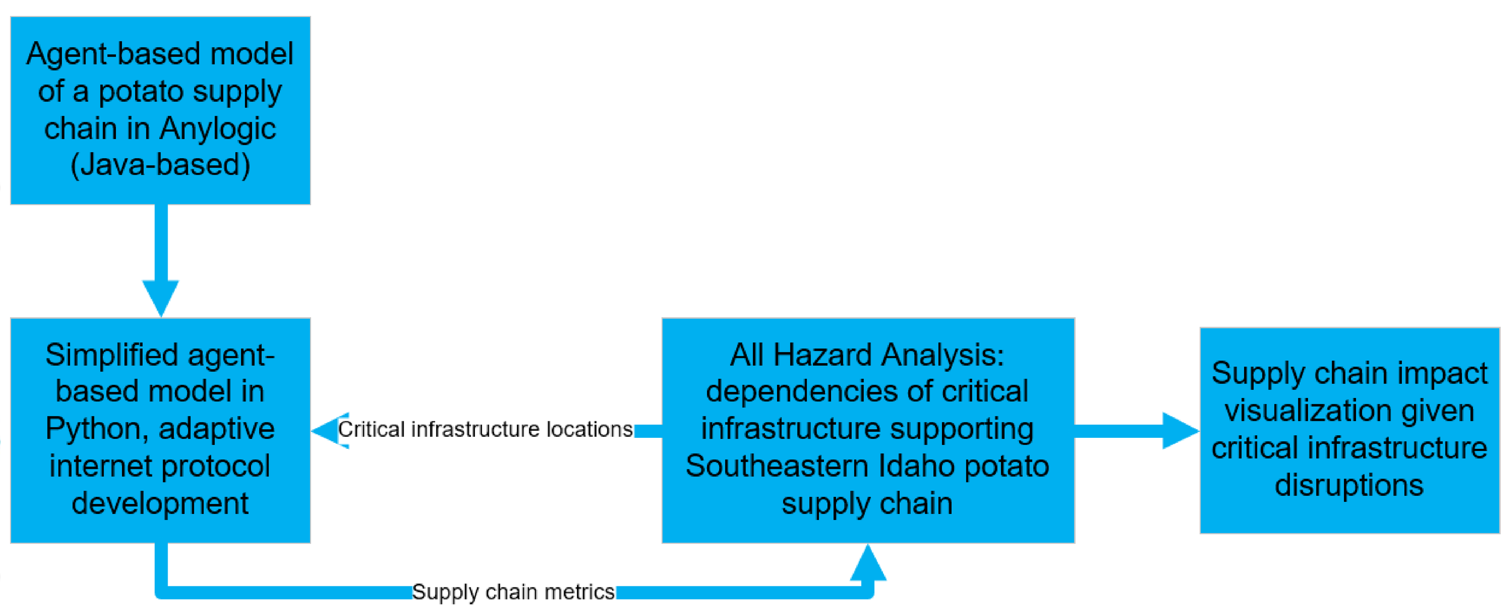
A quantitative approach to multiple critical supply chain resilience assessment

PRESENTERS: **Julia Morgan & Ruby Nguyen**

BACKGROUND

Food & Agriculture is one of 16 critical infrastructure sectors. This supply chain is subjected to both supply and demand disruptions. Quantifying disruption impacts would help improve this supply chain's resilience.

METHODS



RESULTS

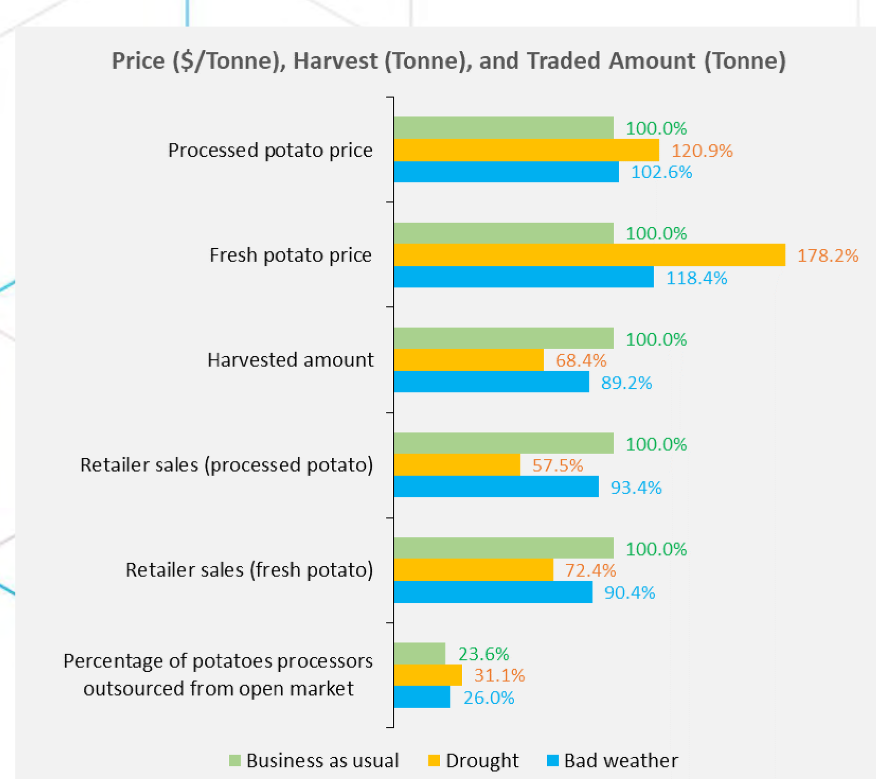


Figure 1: Comparative impacts of drought and early frost on prices and quantity

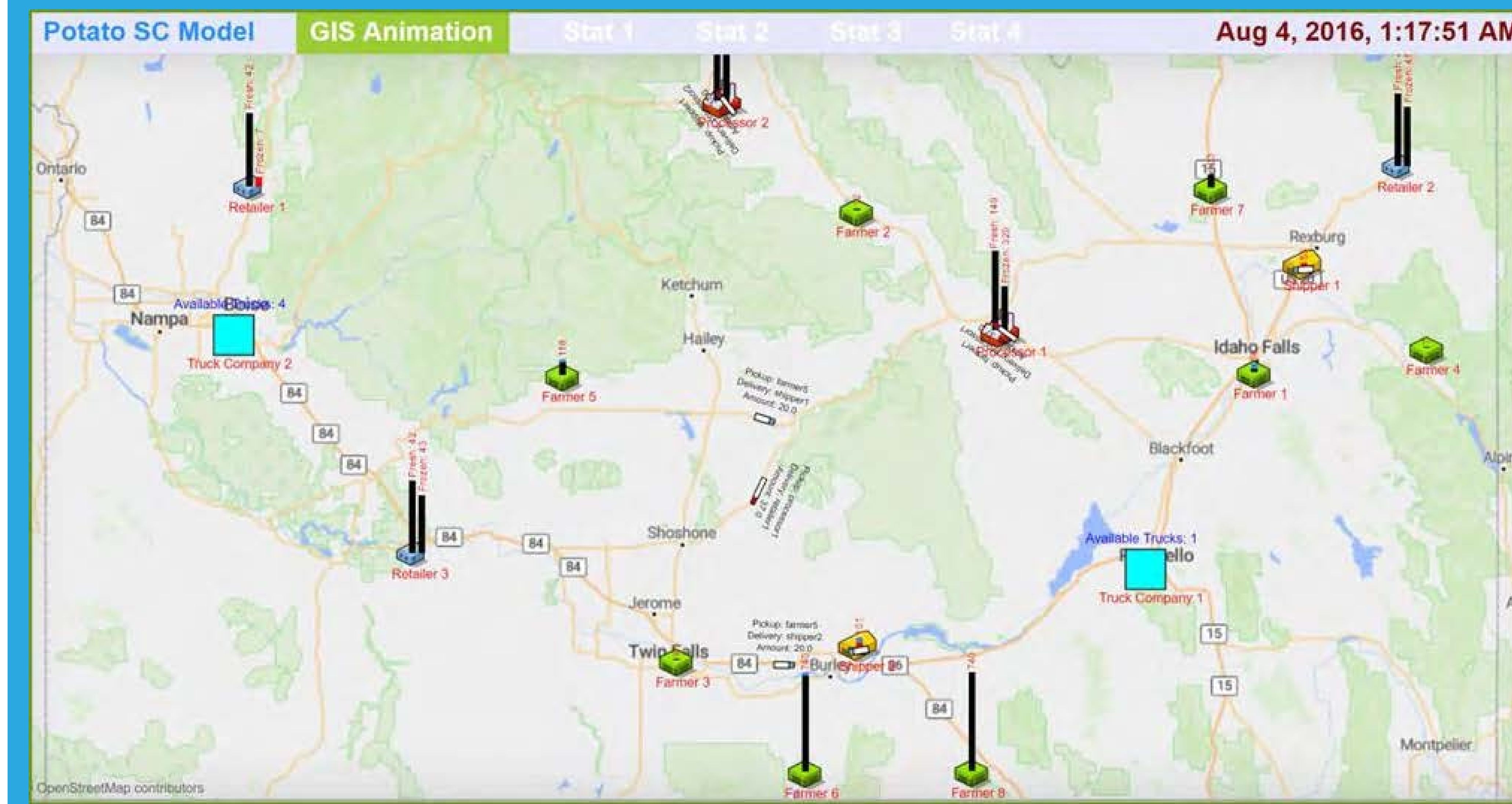


Figure 2: Simulation model snapshot

Transportation disruptions have minimal impacts. Climate change disruptions such as drought have the most impacts on the Food & Agriculture supply chain.

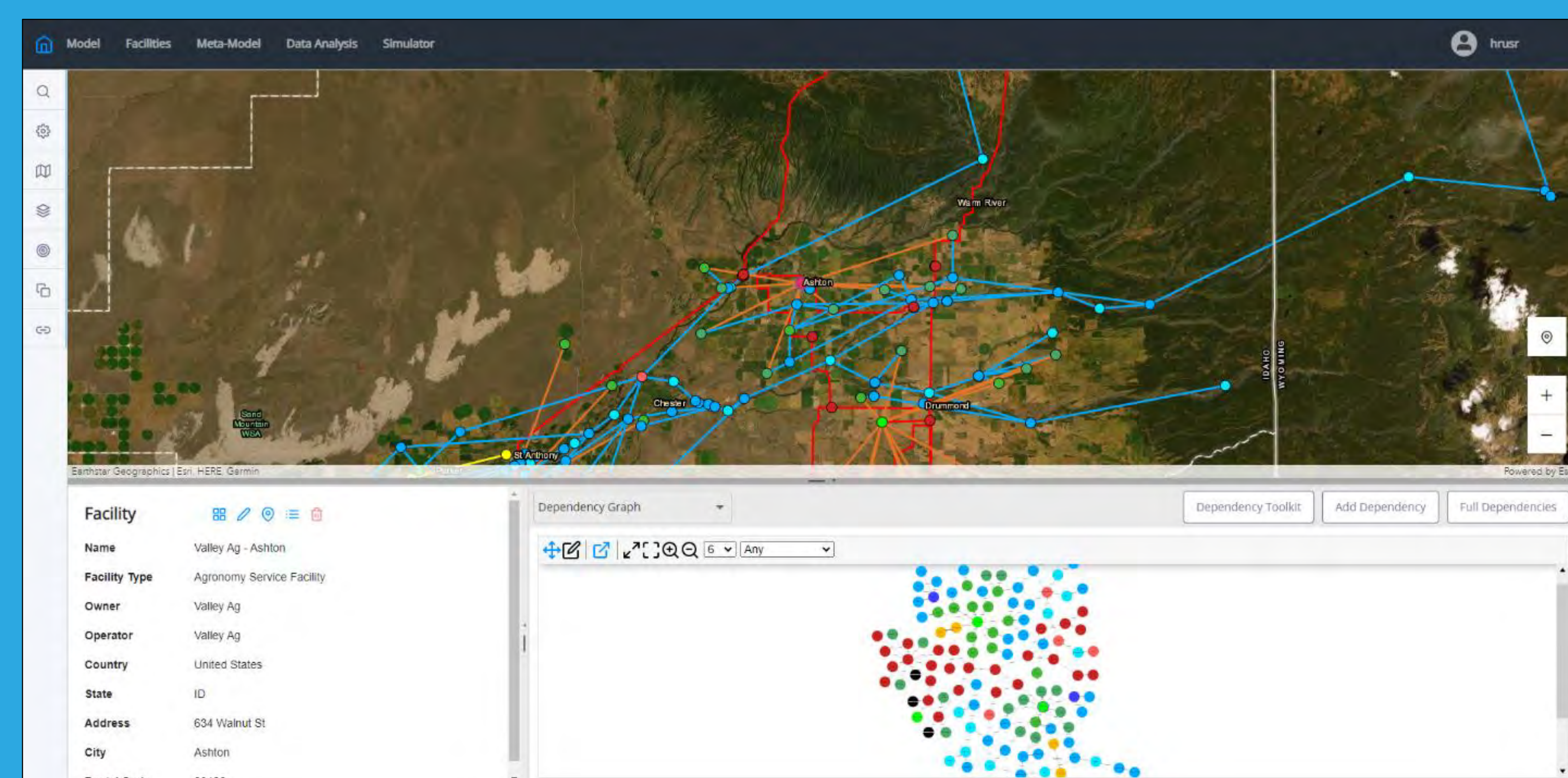


Figure 3: Visualization of the irrigation network and cascading impacts from disruptions

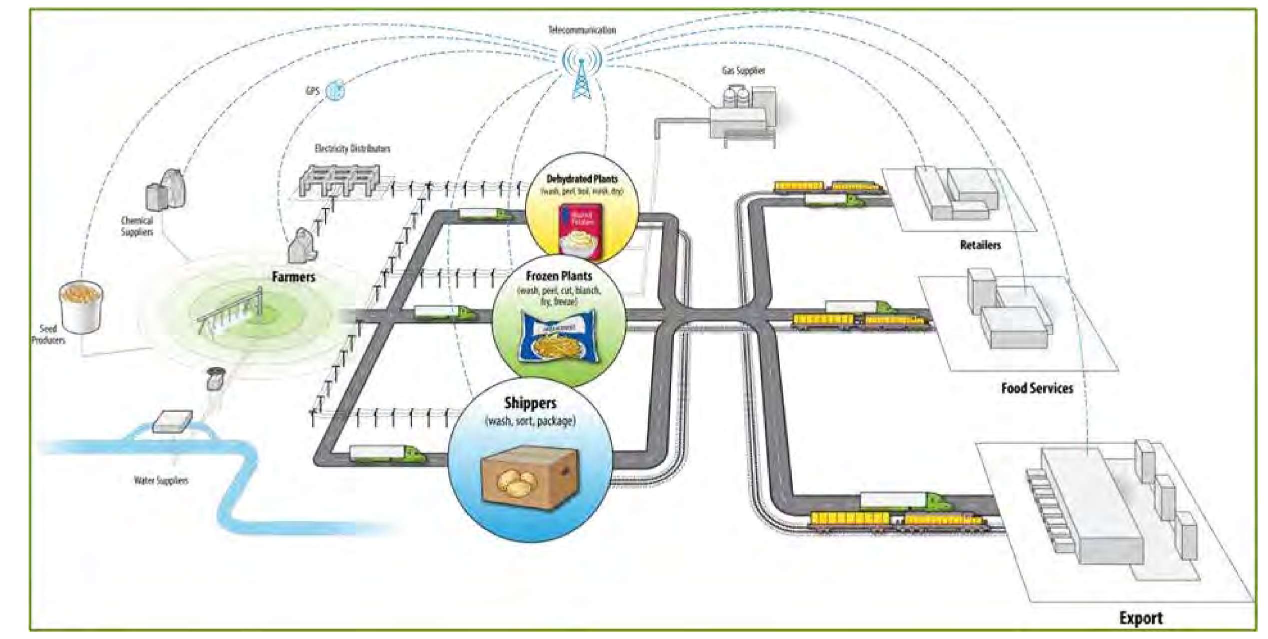


Figure 4: Overview of the potato supply chain

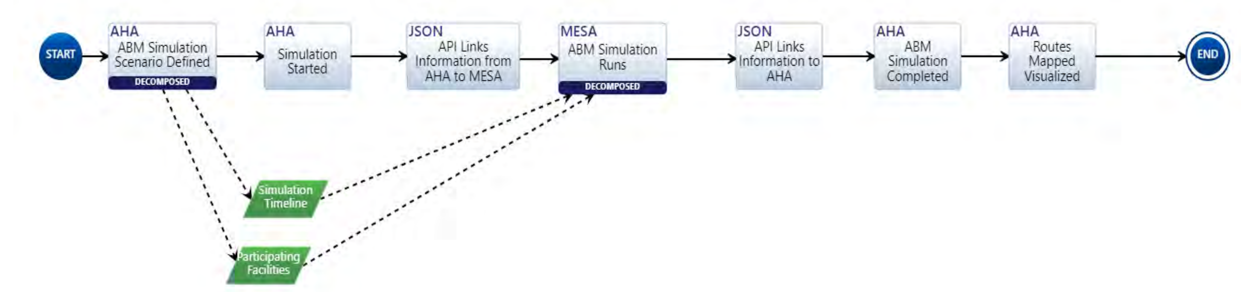


Figure 5: Flow of information for agent-based modeling simulation

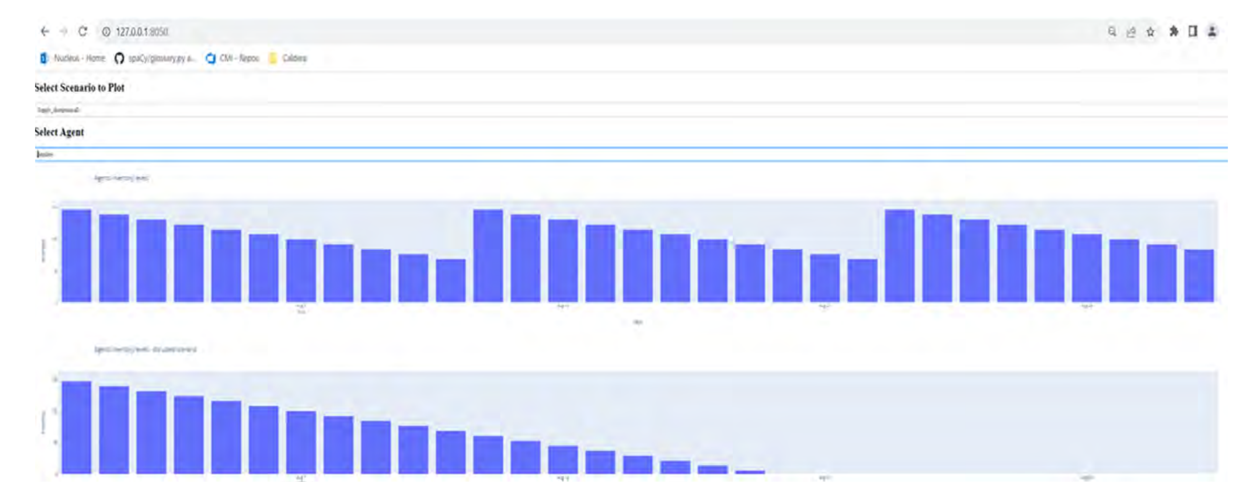
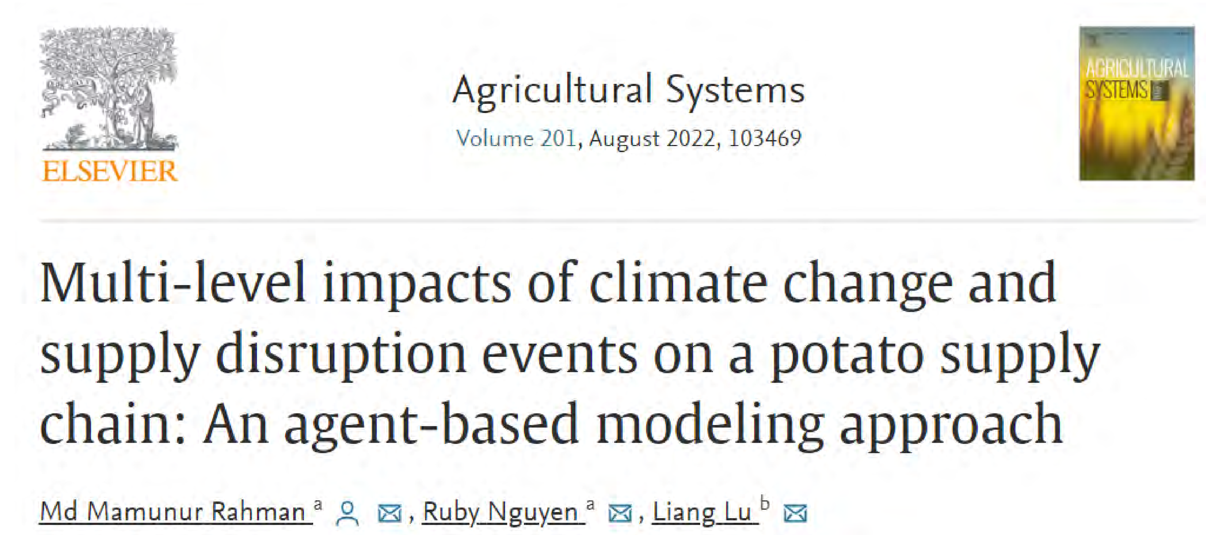


Figure 6: Visualization of inventory level fluctuation throughout the agent-based model simulation


Agricultural Systems
Volume 201, August 2022, 103469

Multi-level impacts of climate change and supply disruption events on a potato supply chain: An agent-based modeling approach

Md Mamunur Rahman [a], Ruby Nguyen [a], Liang Lu [b]

Ruby Nguyen, Ryan Hruska, Steven Hall, Julia Morgan, Trevor Baker, Mamunur Rahman, Wael Khallouli, Liang Lu, Yuan-Yuan Lee, Barry Ezell

Project Number: 21A1050-082FP LRS Number: INL/EXP-23-74229

www.inl.gov

Work supported through the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517."

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory