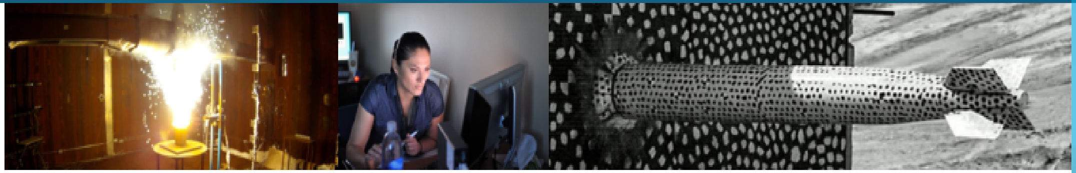
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2021-3547C

# Unsupervised Online Anomaly Detection to Identify Cyber-Attacks on Internet Connected Photovoltaic System Inverters



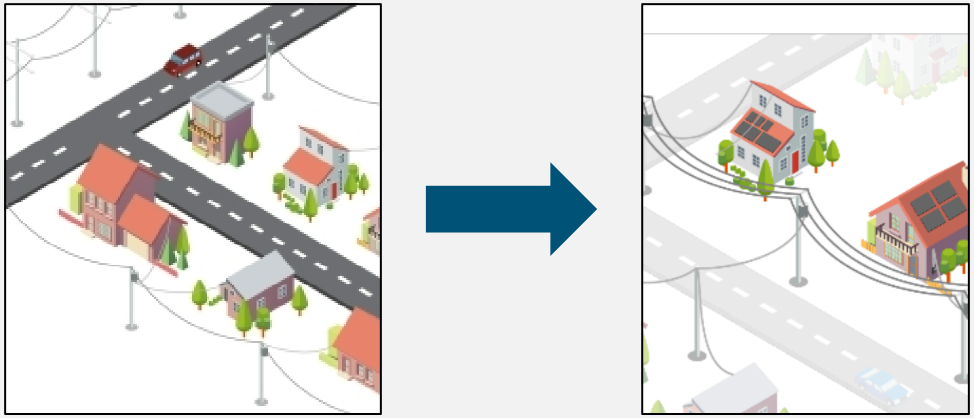
*C. Birk Jones, Ph.D.*

co-authors: Adrian Chavez, Shamina Hossain-McKenzie, Nicholas Jacobs, Adam Summers, and Brian Wright

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

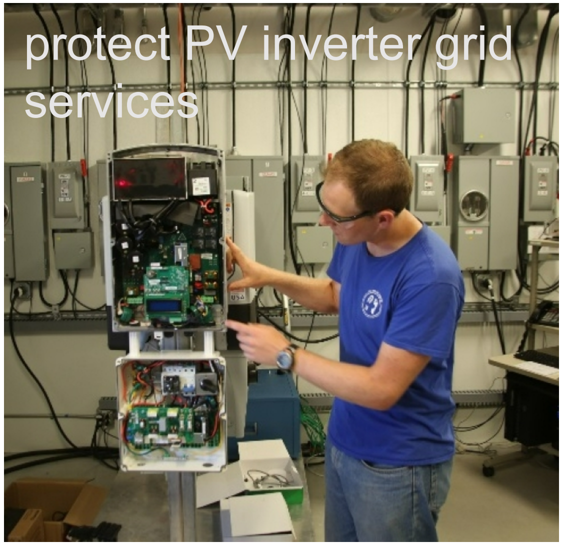
# Summary

1. Electric grid is changing to include centralized and distributed power generation
2. Roof-top Photovoltaic (PV) System Inverters
   - Internet connected
   - Provide grid services



Research Question:

➢ Can an online learning approach learn cyber network traffic while also detecting abnormal activity?

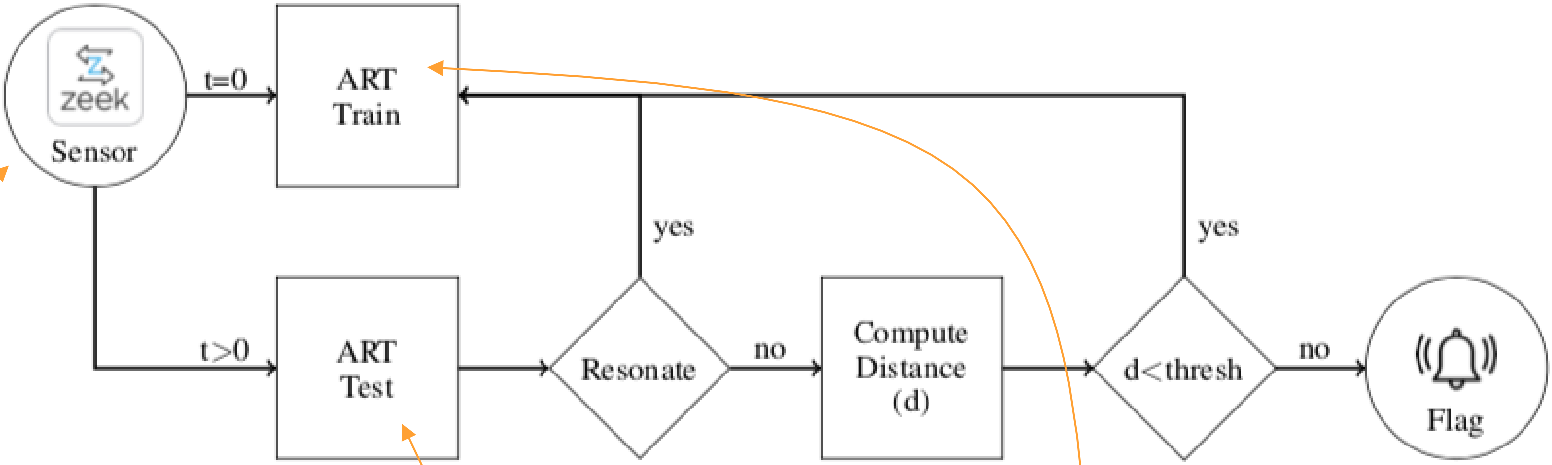


protect PV inverter grid services

Research Objectives:

1. Perform cyber monitoring & analysis experiment
2. Deploy and test unsupervised training and testing

# Unsupervised Training & Testing of Cyber Data (what?)



zeek

An Open Source Network Security Monitoring Tool

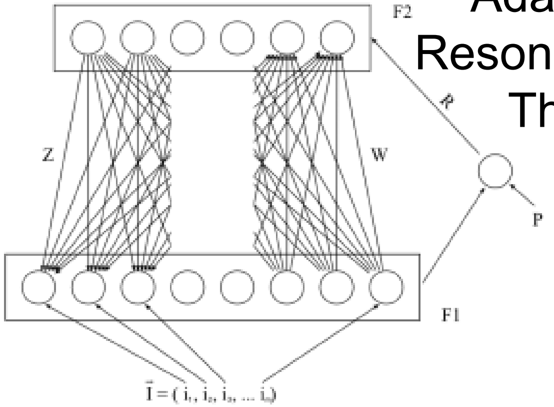
Zeek (formerly Bro) is the world's leading platform for network security monitoring.

Flexible, open source, and powered by defenders.

Get Zeek

ZEEK AND YE SHALL FIND

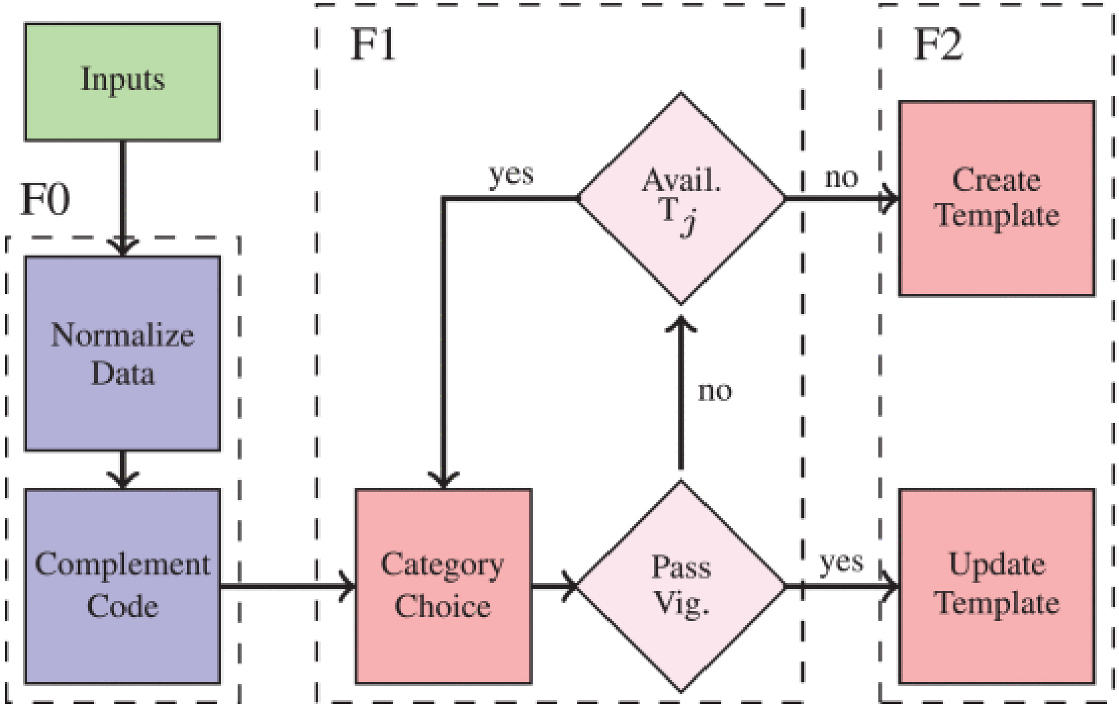
https://zeek.org/



Adaptive Resonance Theory

https://en.wikipedia.org/wiki/Adaptive_resonance_theory

# Adaptive Resonance Theory Artificial Neural Network (what?)



Normalize Data

$$X = \frac{X_i - min(X)}{max(X) - min(X)}$$

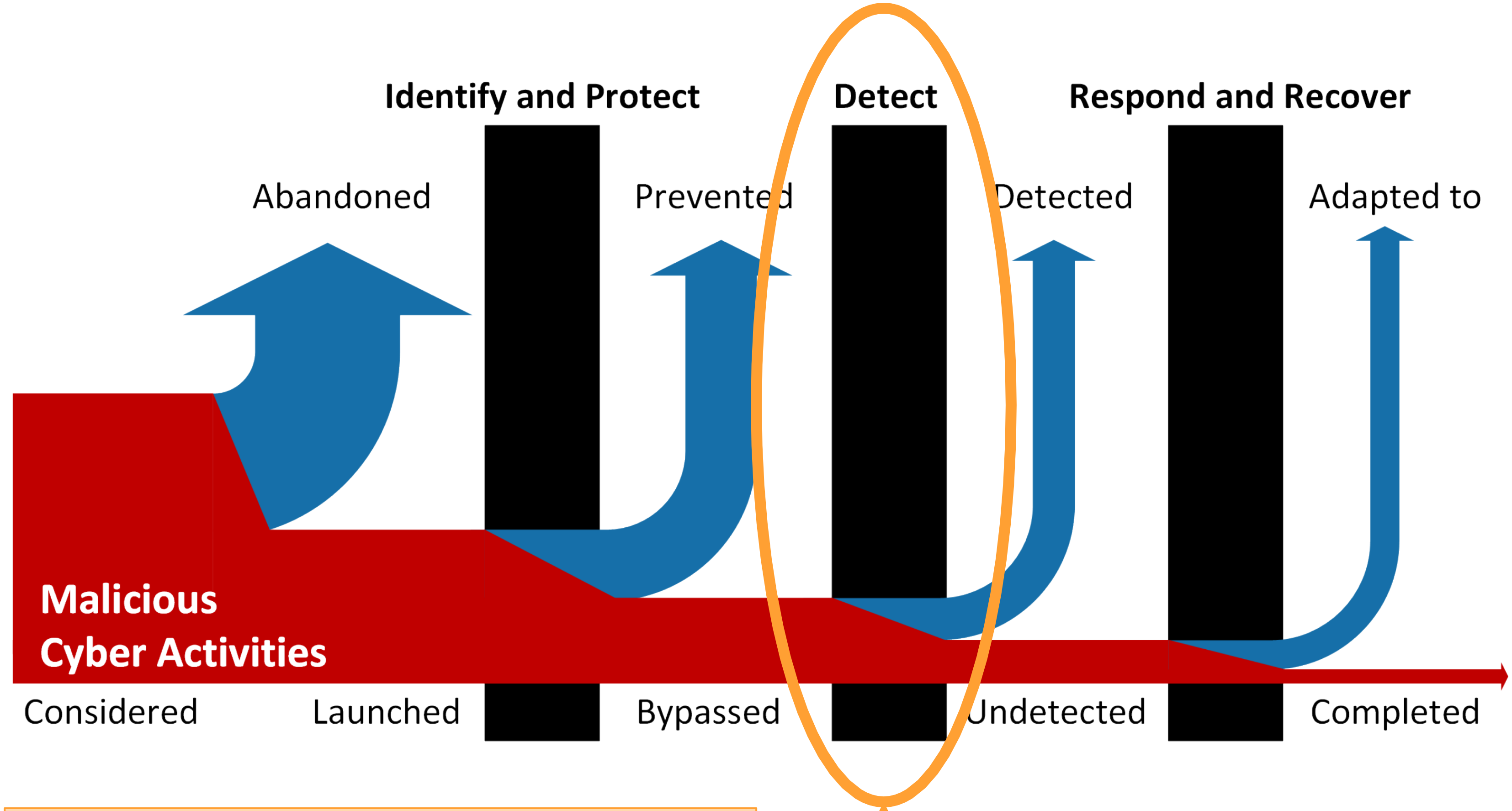
Category Choice

$$c = \frac{|X \wedge T_j|}{\alpha + |T_j|}$$

Vigilance Test

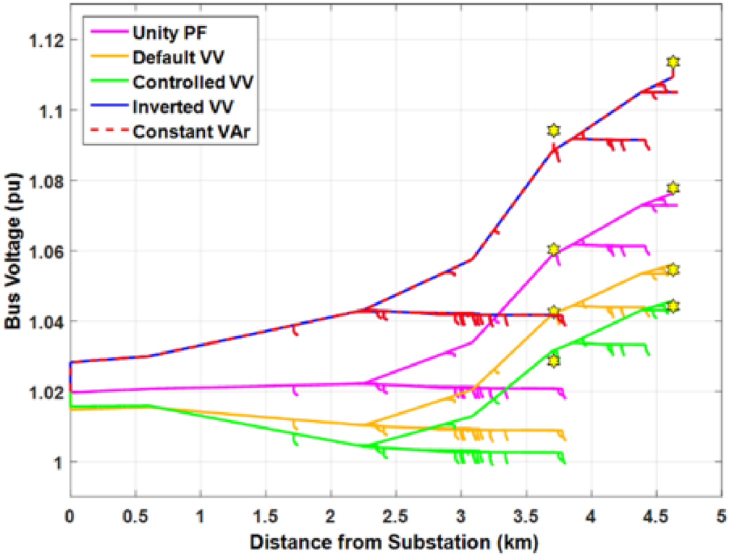
$$\frac{|X \wedge T_j|}{|T_j|} \geq \rho$$

# Cybersecurity Concerns (why?)



- Assume adversary can access network of PV inverter
- Algorithm intends to detect malicious traffic

# PV Inverter Manipulation Impacts (why?) *



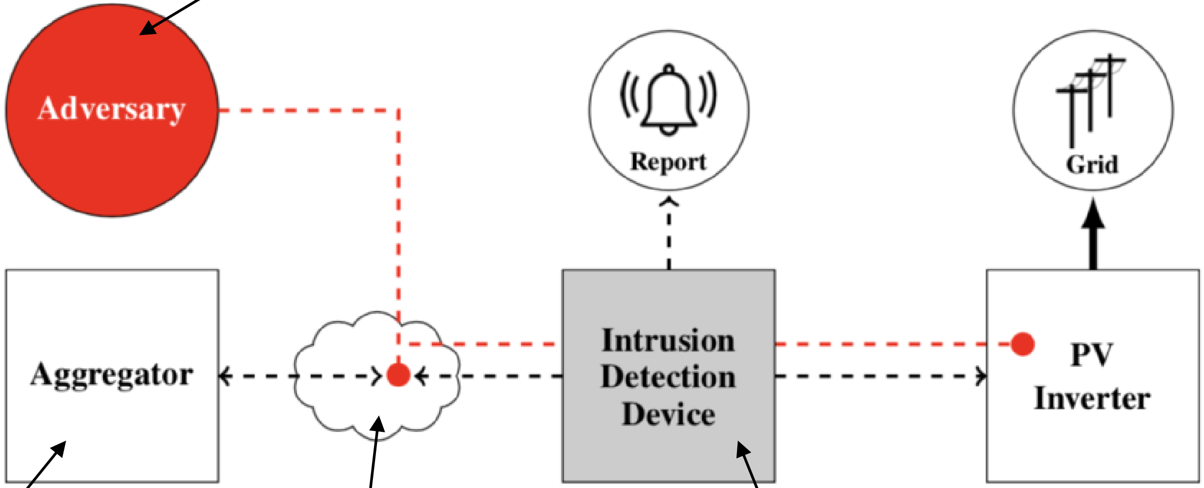
## Voltage Profile (single instance)

1. No Control:
   - ➢ Voltage >1.08 p.u.
2. w/ VVC:
   - ➢ Voltage <1.05 p.u.
3. Modified VVC (adversary)
   - ➢ Voltage > 1.1 p.u.

* J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, M. Reno, “Power system effects and mitigation recommendations for DER cyberattacks”, IET Cyber Phys. Syst. Theory Appl. 2019, 4, 240 -249.

# Cyber Monitoring & Analysis Experiment (how?)

Gains access, assesses the network/devices, and performs a denial of service attack



Centralized Control

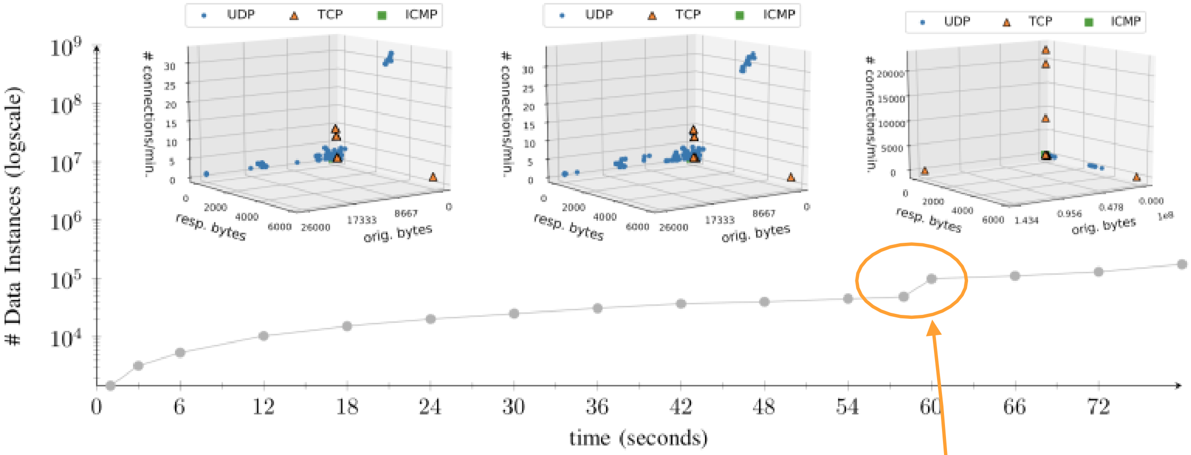
Local Area Network

On-board Monitoring & Analytics

# Cyber Data – Normal & Abnormal Traffic (how?)

1. Monitor actual network traffic
2. Emulate adversary reconnaissance using nmap tool
3. Perform denial-of-service (DoS)

NMAP



Reconnaissance:

```
nmap -sn < subnet address/prefix >
```

```
nmap -p0- -v -A -T4 < ip address >
```

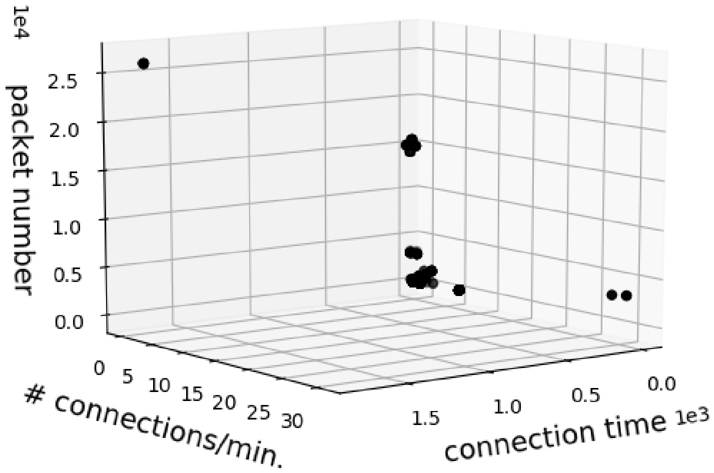
```
nmap -sX < ip address >
```

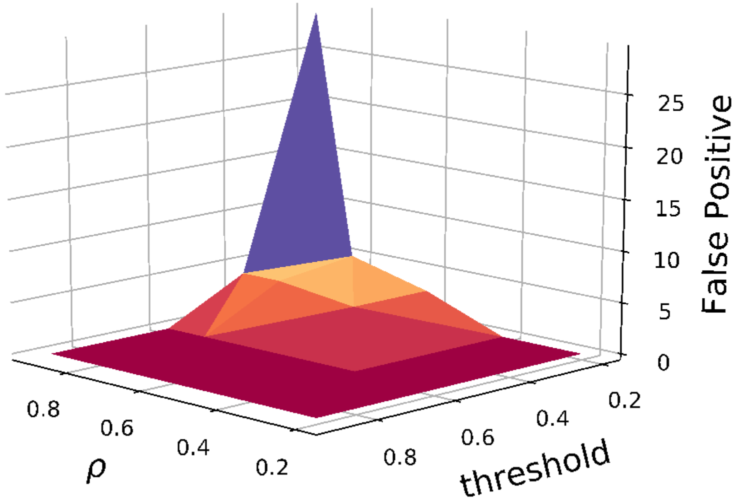
Denial-of-Service:

```
hping3 -c 100 -d 120 -S -p 502 -flood -V < ip address >
```

# Results

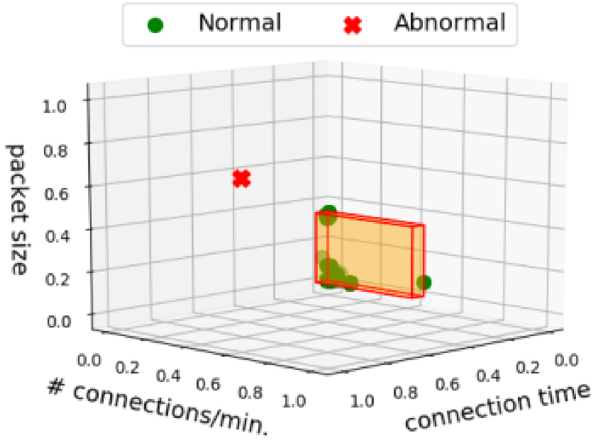
# Initialize Analysis: Define Free Parameter & Threshold



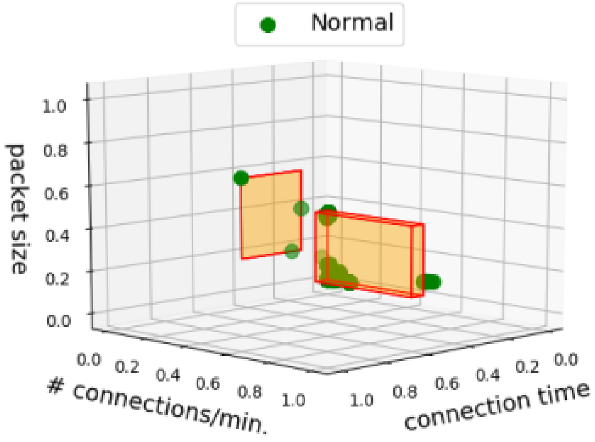


1. Features:
   - Packet Number
   - Connections/min.
   - Connection Time
2. Review first hour of data
   1. Define min & max for normalization – plot data
   2. Define free parameters – sensitivity analysis
3. Free parameter & threshold used:
   1. Threshold – 0.3
   2. ART rho – 0.7

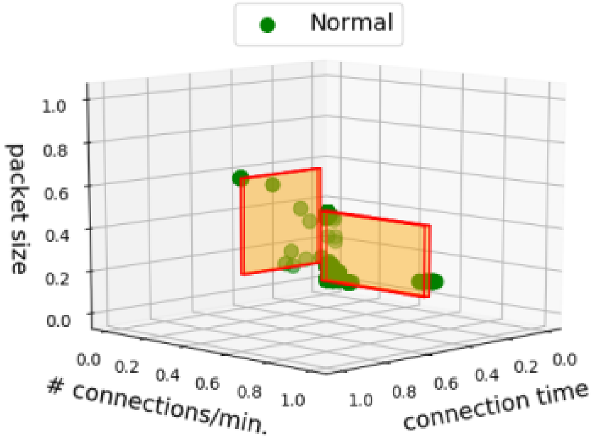
# Analysis: Learning w/ Normal Network Behavior Only



At hour 8



At hour 16



At hour 48

ART Learning:

- ➢ One Template

Abnormal Behavior

- ➢ Repetitive action that occurred every hour

ART Learning:

- ➢ Two Templates

Abnormal Behavior

- ➢ No abnormal data
- ➢ Repetitive action that occurred every hour considered to be ok and learned

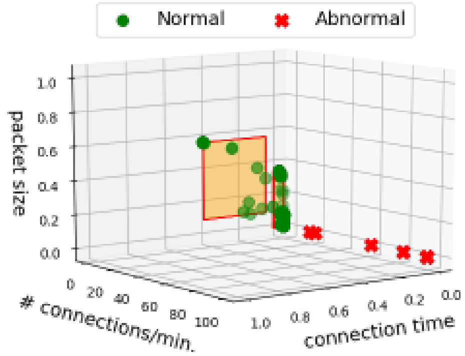
ART Learning:

- ➢ Two Templates (expanded in size)

Abnormal Behavior

- ➢ No abnormal data

# Analysis: Learning w/ Normal & Abnormal Conditions



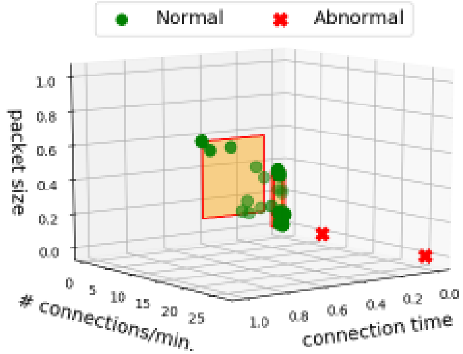
Aggressive Scan

ART Learning:

- ➢ No new templates

Abnormal Behavior

- ➢ Exceed connections/min feature template limits



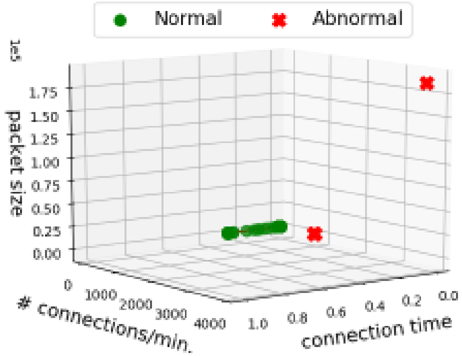
Stealthy Scan

ART Learning:

- ➢ No new templates

Abnormal Behavior

- ➢ Exceed connections/min feature template limits



Denial-of-Service

ART Learning:

- ➢ No new templates

Abnormal Behavior

- ➢ Exceed connections/min and packet size feature template limits

# Conclusion

Created cyber monitoring & analysis experiment:

- Generate and capture actual network traffic to and from a PV inverter

Emulate adversary actions

- Create and implement nmap and DoS actions

Deploy and test Adaptive Resonance Theory Online Learning Methodology

- Perform simultaneous learning and anomaly detection
- Provide evidence that method could work – future studies needed to provide proof of its effectiveness

Thank you for listening!

Contact Information:

C. Birk Jones

cbjones@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories