SAND2023-05400C

Sandia National Laboratories

Exceptional service in the national interest

MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS (IDS) FOR WIND NETWORKS

George Fragkos, Sandia National Laboratories

AI for Wind Energy Workshop

June 27th & 28th

Boulder, CO

Joint project with:

INL Idaho National Laboratory

NREL

BACKGROUND: PROBLEM STATEMENT

- There are several locations in wind sites and turbines where network traffic could be analyzed
  - Provide high-fidelity information about adversary actions

- This source of data is rarely inspected on wind system. Commercial tools:
  - Not tailored to the wind environments
  - Rarely incorporate deep-packet inspection
  - Lack cyber-physical analysis technologies

BACKGROUND: POTENTIAL MALICOUS ACTIVITIES

- Reduced power production
  - Brake actuation
  - Wind / yaw-heading misalignment
- Causing damage
  - Overheating
  - Mechanical stress
  - Catastrophic failure
- Grid-level impacts
  - Entire wind plant shuts down unexpected
  - Entire wind plant produces more power (real or reactive) than authorized

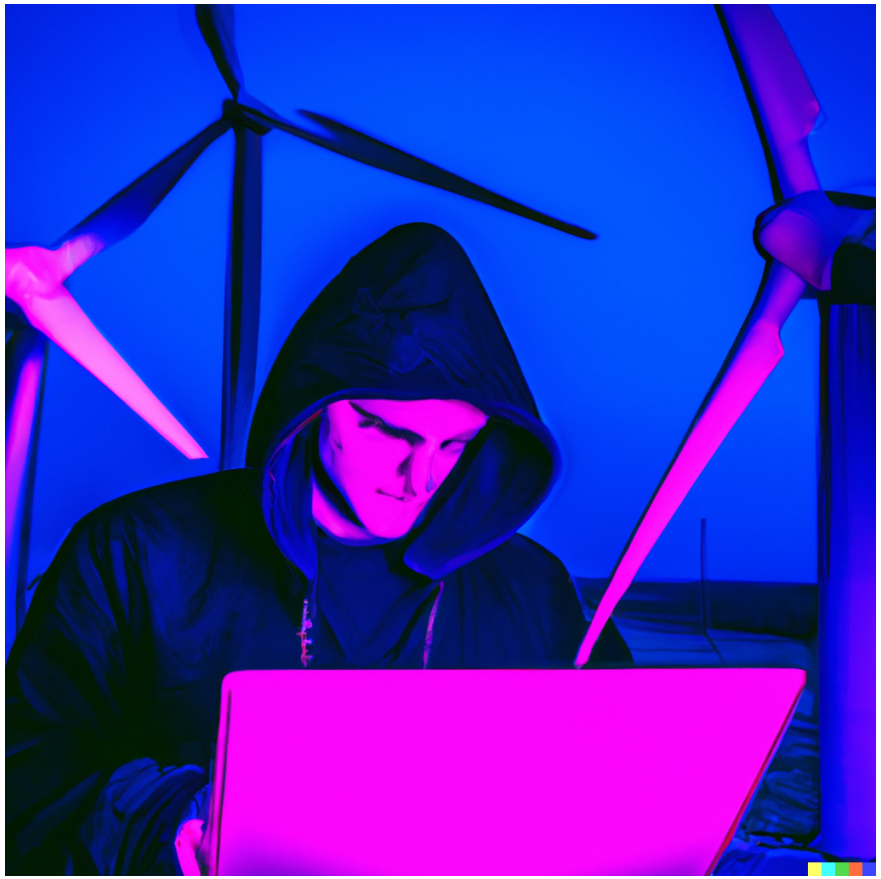


Image created with AI image generator “DALL-E”

BACKGROUND: NETWORK INTRUSION DETECTION

- What is a NIDS?
  - It is a security technology that monitors network traffic for potential security threats and intrusions
  - It analyzes network packets, identifies suspicious patterns, and generates alerts

- NIDS Functionality
  - Real-time monitoring and analysis of network traffic
  - Detection and identification of potential threats by using signatures, rules, and/or behavioral analysis
  - Generating alerts to security administrators and reports for post-incident analysis

- NIDS Benefits in Wind Networks
  - Early detection of network attacks and intrusions
  - Protection of critical wind network infrastructure
  - Prevention of unauthorized access and data breaches

BACKGROUND: NETWORK INTRUSION DETECTION

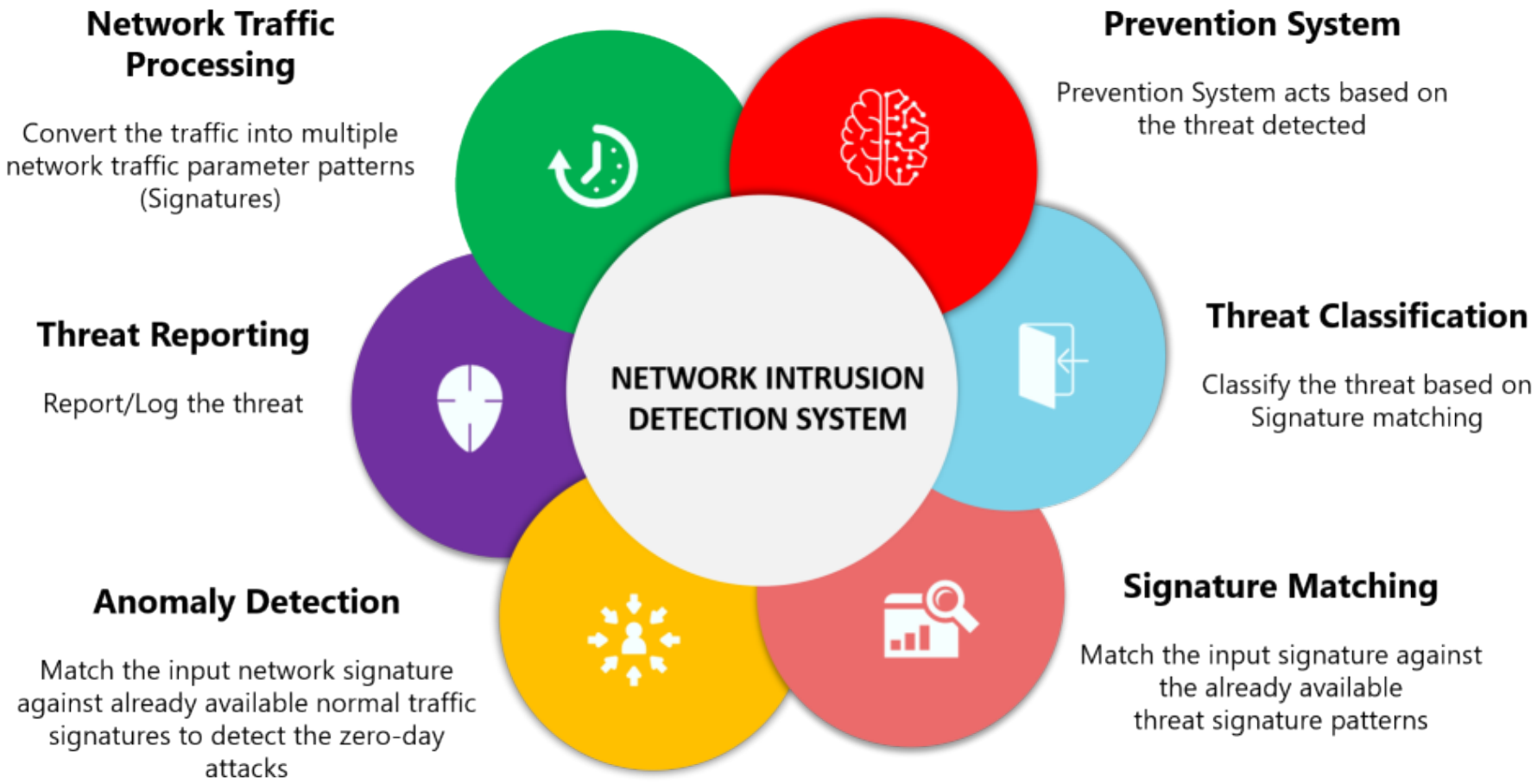


Image from: https://www.businessprocessincubator.com/content/securing-the-internet-of-things-with-intrusion-detection-systems/

OBJECTIVES

Our new research effort is called “Machine Learning-Based Intrusion Detection Systems (IDS) for Wind Networks”, funded by DOE Wind Energy Technology Office

- Perform Machine Learning (ML)-based cybersecurity classification on wind packets
- Aim to accurately identifying instances of suspicious wind network activity and raising alerts

Several state-of-the-art ML models will be studied

- Principal Component Analysis (PCA)
- Autoencoders (AE)

- Support Vector Machines (SVMs)
- Random Forest
- Gradient Boosting

- Offline Deep Reinforcement Learning

NIDS PLACEMENT

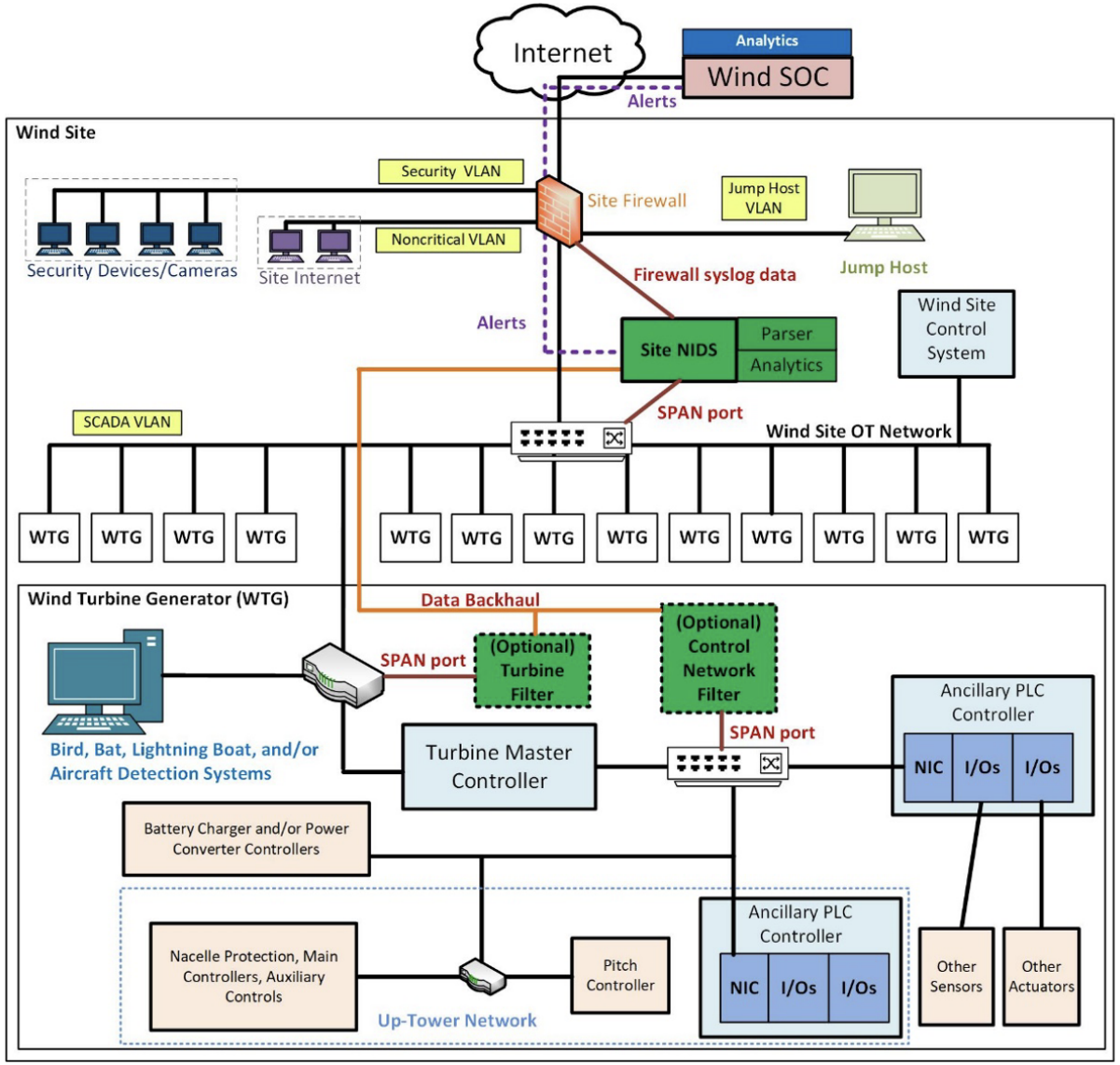
Less Expensive

Easier Deployment

Wider Visibility

Greater Data Granularity

More Difficult for Adversary To Evade Detection



Site level: Traffic to all turbines and the site controller is captured using a SPAN port

Switch at the wind turbine: See data associated with bird, bat, lightning, boat, aircraft, etc. detection systems

OT Control Network: Turbine protocols such as EtherCAT, Modbus, or S7 protocol

ML-BASED INTRUSION DETECTION SYSTEMS FOR WIND NETWORKS

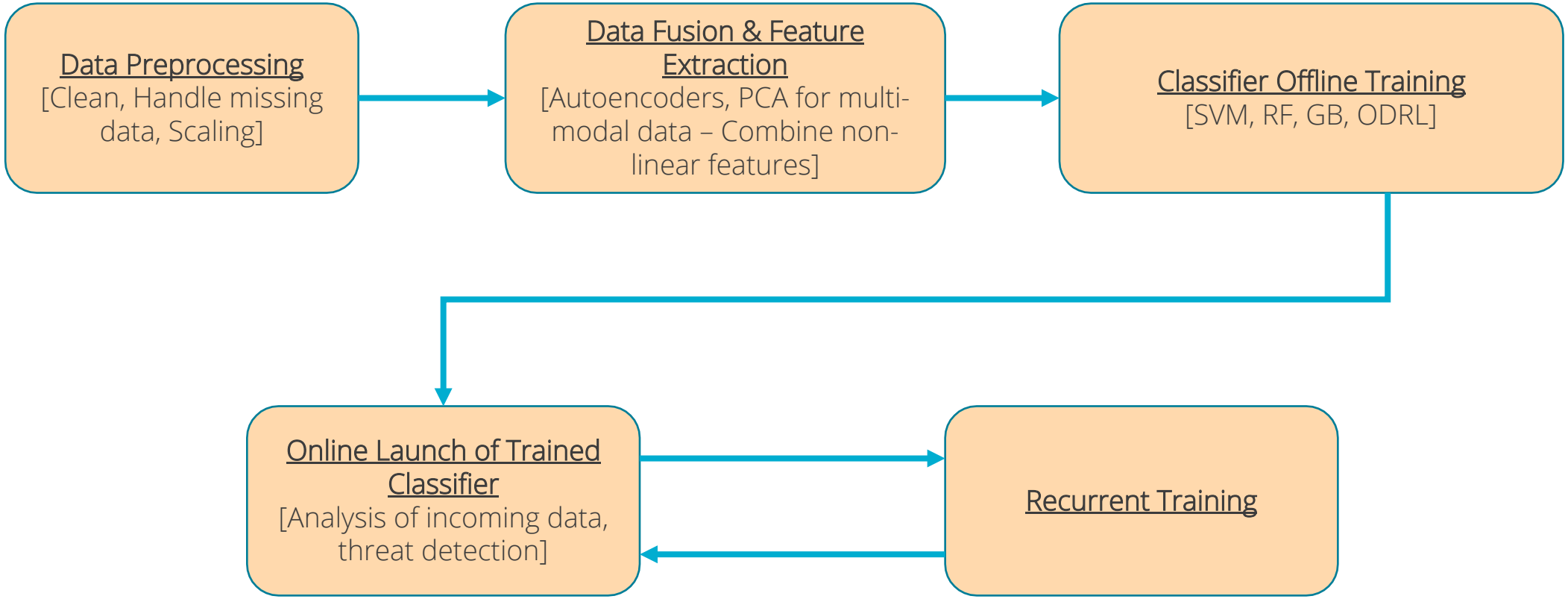
- Need for representative captured traffic/datasets
  - Performing classification operations with ML in such a complex scenario includes the construction of a balanced and representative dataset
  - Capture traffic from wind networks under both normal operation and simulated attack scenarios

- Data generation
  - Long-term data of normal operations: Wind turbine operations for a range of weather and operational conditions [“**Normal” Dataset**]
  - Malicious data: [**“Abnormal” Dataset**]
    - (a) Place the systems in unnatural or intentionally bad states, e.g., pitching a single blade
    - (b) Send attack data on the networks, e.g., denial of service attacks, brute force attacks, etc.

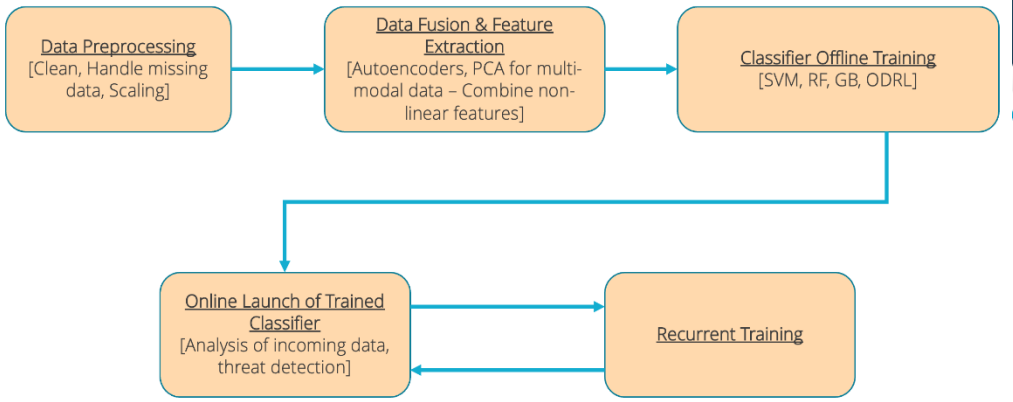
- Cyber-Physical Features
  - Cyber: RTT, IP and MAC addresses, packet length, packet protocol, and others.
  - Physical: voltage, current, temperature, pressure
  - Multimodal data

ML-BASED INTRUSION DETECTION SYSTEMS FOR WIND NETWORKS

ML Pipeline

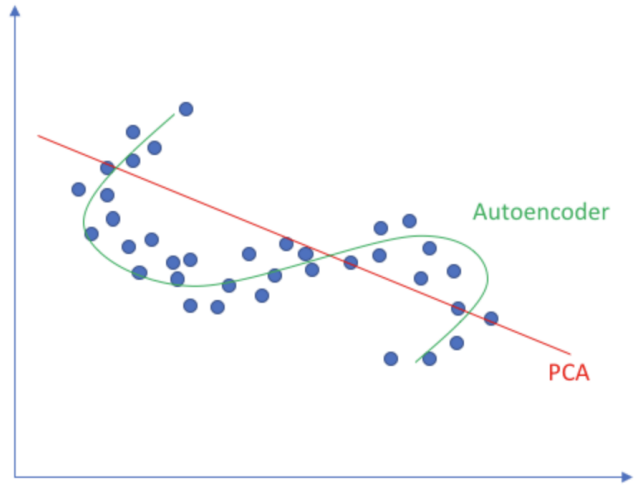


ML-BASED INTRUSION DETECTION SYSTEMS FOR WIND NETWORKS



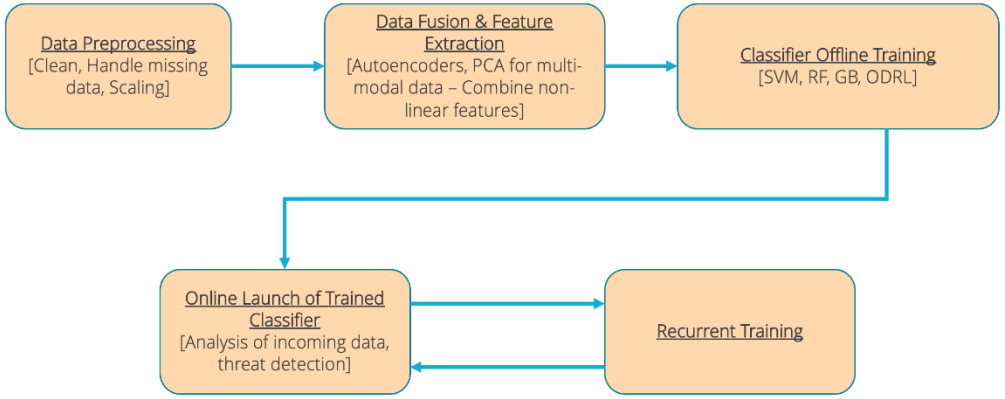
- Data Fusion & Feature Extraction
  - The predictive performance of classifiers is influenced by the number of input features utilized
  - Combine and integrate cyber-physical data to generate a lower-dimensional feature subspace
  - *PCA*: Identifies the most informative features by transforming them into a new set of uncorrelated variables
  - *Autoencoder*: Type of ANN that learns to encode and decode data, effectively compressing it

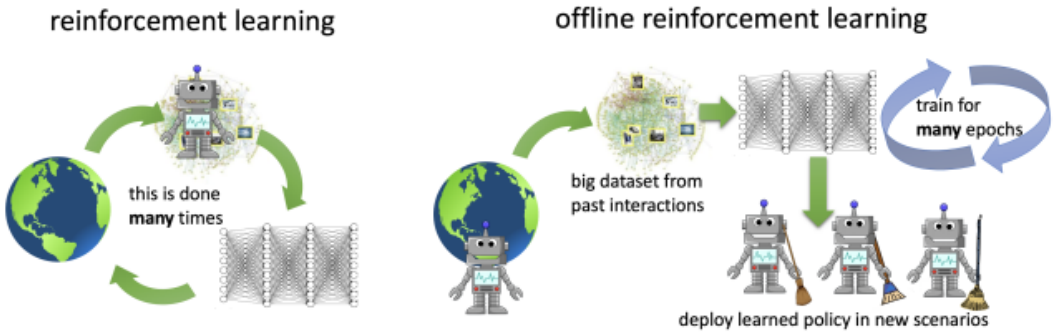
Linear vs nonlinear dimensionality reduction



ML-BASED INTRUSION DETECTION SYSTEMS FOR WIND NETWORKS

- Classifier Offline Training
  - SVMs: Find an optimal hyperplane in a high-dimensional feature space to separate different classes
  - RF: Ensemble learning algorithm that combines multiple decision trees for classification
  - *GB*: Ensemble learning technique that combines weak predictive models and optimizes loss function using gradient descent
  - *ODRL*: Sequential decision-making paradigm that learns only from pre-existing data without requiring any additional online interaction with the environment
- Recurrent Training
  - Distribution shift of the input data can cause the performance of the model to degrade
  - Warm-start re-training ensures the deployment integrity





COSTS AND BENEFITS

Benefits of using a ML-based IDS for Wind Networks

- Improved accuracy
  - Detect complex patterns and anomalies in network traffic
- Adaptability
  - Learn from new types of attacks or network behaviors
  - Evolving system
- Scalability
  - Can handle large volumes of wind network traffic

Cost of using a ML-based IDS for Wind Networks

- Training difficulties
  - Large training datasets required
  - Over/Under-fitting dangers
- Data distribution shift
  - Wind networks can experience changes in network traffic patterns

CONCLUSION

- Several locations in wind sites and turbines where network traffic could be analyzed to provide high-fidelity information on adversary actions.
- Commercial tools are
  - not tailored to wind environments
  - do not provide adequate deep-packet inspection (DPI) capabilities for some wind protocols
  - lack cyber-physical analysis technologies
- Machine Learning-based Network-Based Intrusion Detection Systems (NIDS) for the wind industry will identify real-time threats attempting to exploit wind site and turbine vulnerabilities.
  - Approach will provide asset owners the ability to identify malicious actions within the network and prioritize mitigations based on the current threat posture
- Stay tuned for cyber-physical, deep packet inspection IDS results from the labs shortly!

THANK YOU

QUESTIONS?

Let's talk:
gfragko@sandia.gov