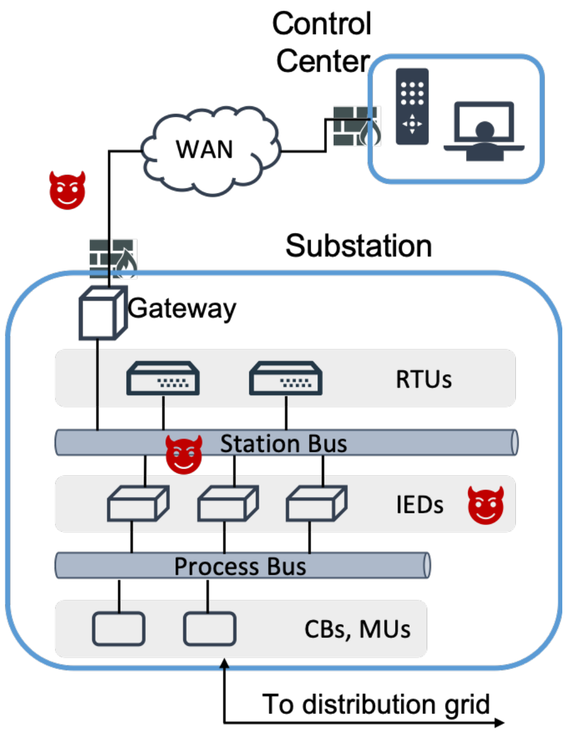
Secure SCADA Cloud for EDS

A. Bohara*, B. Feddersen*, A. Valdes*, K. Nahrstedt*, J. Ros-Giralt^, and W. H. Sanders*
* University of Illinois at Urbana-Champaign, ^ Reservoir Labs

THE SCADA NETWORKS ARE VULNERABLE

- A completely cyber-induced attack on the Ukrainian power grid left about 225,000 users without electricity
- Cyber espionage groups are active in SCADA systems and can disrupt the operations in both power grid and oil & gas EDS



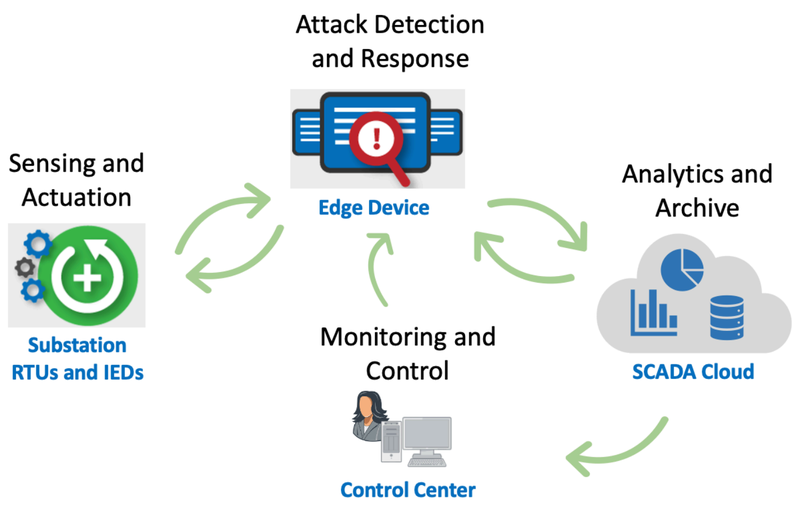
Cyber-physical attack examples
- Packet delay
- Man-in-the-middle (MITM)
- Data injection of erroneous commands/measurements
- Attacks that lead to instability of the system

- SCADA systems lack security protection
  - The growing number of heterogeneous programmable devices introduces new risks
  - Many devices and protocols are not designed with security in mind
  - Resource-constrained environments limit the application of security standards
- Attacker sophistication is increasing
  - Newer campaigns build upon past incidents
  - Attackers use standard OS/networking services to move laterally

RESEARCH VISION

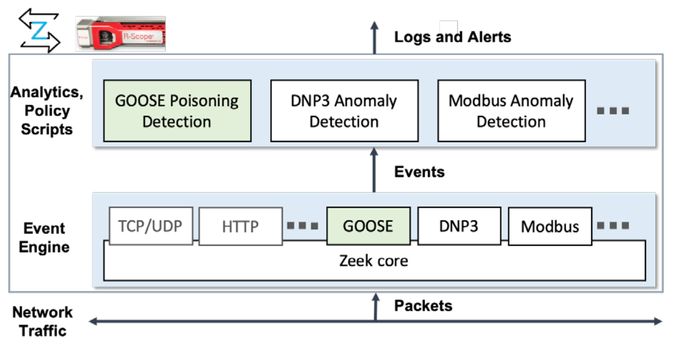
We are developing a SCADA edge-cloud framework for end-to-end security, from the field devices to the control center, by timely detection of both physical and digital anomalies.

RESEARCH ROADMAP



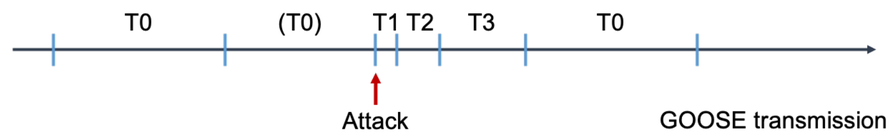
Edge-cloud framework moves the computation away from field devices
- Field Devices collect data only for state estimation
- Edge device performs attack detection and response
  - MAC address white-listing
  - Intrusion detection on within-substation GOOSE communication
  - Multi-level anomaly detection (packet, protocol, and content)
  - Secure communication with SCADA cloud and control center
- SCADA cloud server performs compute-intensive, but non-time-critical analytics
  - Analysis based on cyber-physical models to detect anomalies leading to instabilities or inconsistencies
  - Share the results and reports with the control center

ZEEK-BASED DETECTION ON SCADA EDGE



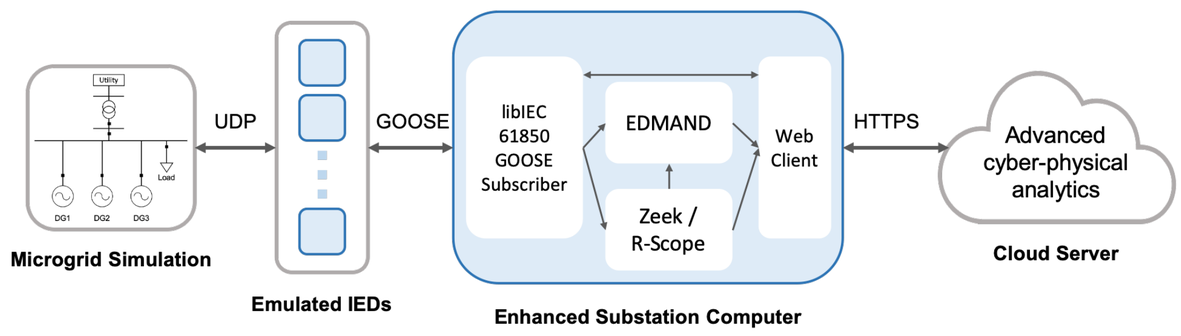
We utilize a network security monitor (e.g., Zeek / R-Scope) to extract essential features and detect attacks
- We have implemented an **analyzer for the GOOSE protocol**

- Example attack: MITM GOOSE poisoning attack
- Detection scheme: at each new event (new state number in the GOOSE message), detect the retransmissions of old events



+	time of transmission
T0	retransmission time in steady state
(T0)	steady state retransmission time, cut short by a new event
T1	shortest retransmission time after an event
T2, T3	retransmission times until achieving steady state time

EXPERIMENTAL SETUP



- We simulate three distributed energy resources (DERs), involving primary and secondary frequency controls in Simulink
- We adopt Zeek / R-Scope sensor for data extraction and protocol analysis
- EDMAND system implements traffic anomaly detection on packet, protocol, and content levels
- At the cloud server, we implement the alternating direction method of multipliers with Round-Robin technique (ADMM-RR) algorithm
  - ADMM-RR can continuously detect malicious DERs

IMPACT ON STATE OF GRID SECURITY

Impacts on Your System
- Detect cyber attacks and anomalies early at the edge
- Prevent unsafe and unstable conditions using advanced cloud-based analytics

Business Benefit
- Reduced outages and complex manual processes
- Increased data security and cyber resilience

INDUSTRY COLLABORATION

Current partners
- **Reservoir Labs:** enable technology-transfer using Zeek-based R-Scope® sensor
- **Duke Energy:** provide microgrid data (discussions underway)

We need your help
- Contribute Specifications concerning the security requirements of the SCADA networks
- Provide Datasets to better understand the systems and evaluate the detection techniques
- Contact: [abohara2, bfeddrsn, avaldes, klara] @illinois.edu
- Activity webpage: https://cred-c.org/researchactivity/secure-cloud-scada-eds

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY