Online, Context-aware Anomaly Detection, Causality and Consequence Analysis for SCADA Systems

Wenyu Ren, Timothy Yardley, Klara Nahrstedt

SCADA SYSTEMS ARE VULNERABLE

Supervisory Control and Data Acquisition (SCADA) systems are industrial control systems (ICSs) for large-scale distributed critical infrastructure systems, such as, power grids and oil/gas pipelines.

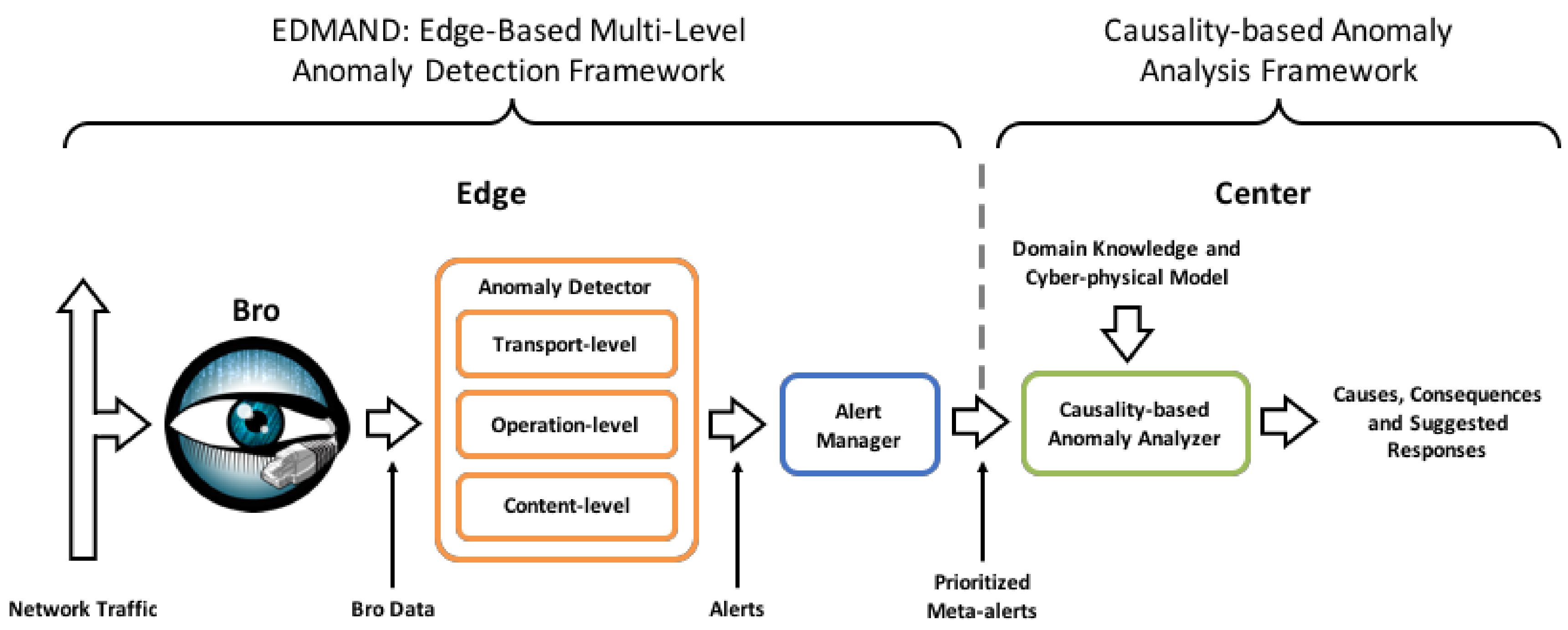
Critical as they are, SCADA systems are vulnerable to a wide range of serious threats due to the following reasons:

- The increasing complexity and interconnection of SCADA systems provides greater opportunity for attacks from malicious sources.
- Devices in SCADA systems are usually not built with consideration to cybersecurity and lack authentication or encryption mechanisms.
- Most ICS protocols lack authentication features and provide no protection for the network traffic.

RESEARCH VISION

We aim to develop an online, context-aware, intelligent framework for anomaly detection, anomalous data analysis, causal reasoning, consequence indication and response suggestion for SCADA networks.

RESEARCH ROADMAP


EDMAND: Edge-Based Multi-Level Anomaly Detection Framework
Causality-based Anomaly Analysis Framework
Edge
Center
Bro
Anomaly Detector
Transport-level
Operation-level
Content-level
Alert Manager
Domain Knowledge and Cyber-physical Model
Causality-based Anomaly Analyzer
Causes, Consequences and Suggested Responses
Network Traffic
Bro Data
Alerts
Prioritized Meta-alerts

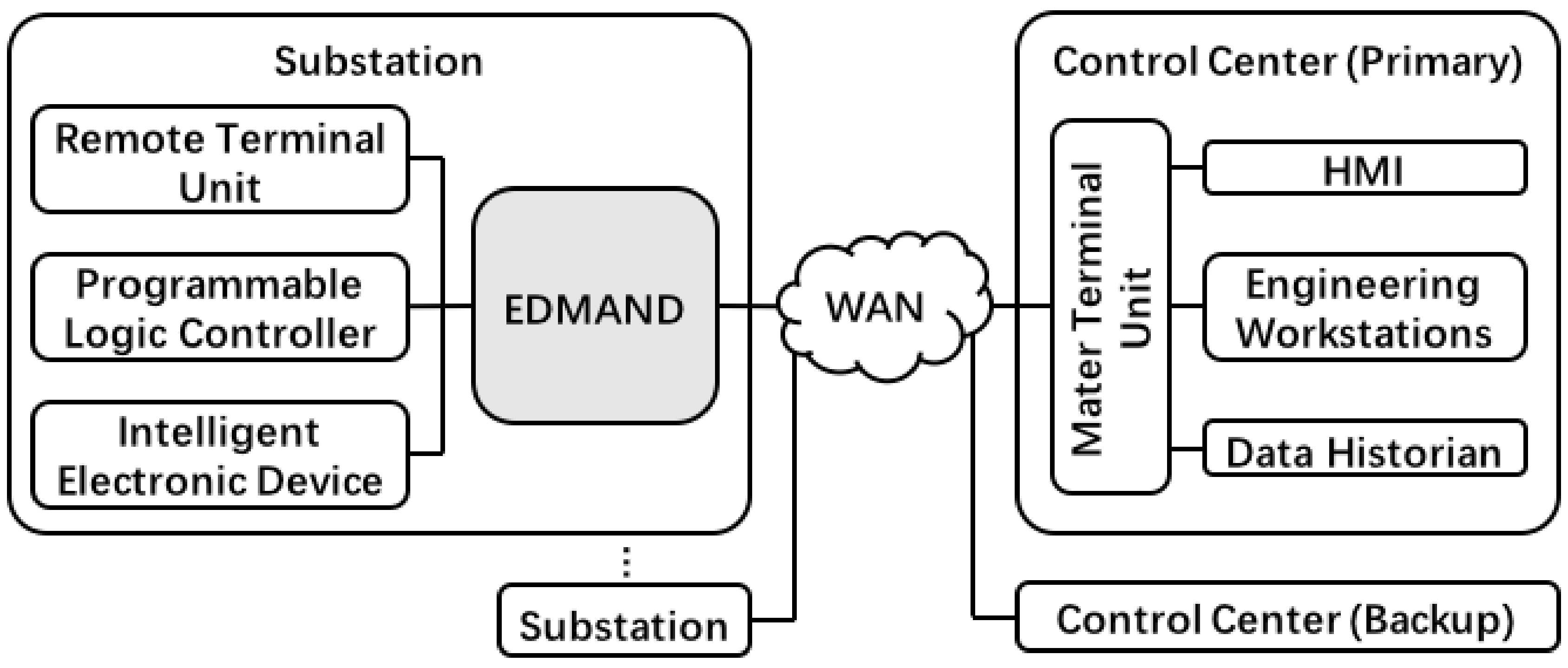
Our entire framework consists of two sub-frameworks:

- An edge-based multi-level anomaly detection framework named EDMAND
- A causality-based anomaly analysis framework

FRAMEWORK DESIGN

The anomaly detection framework (EDMAND) is located inside the remote substations, which are the edges of the SCADA network.

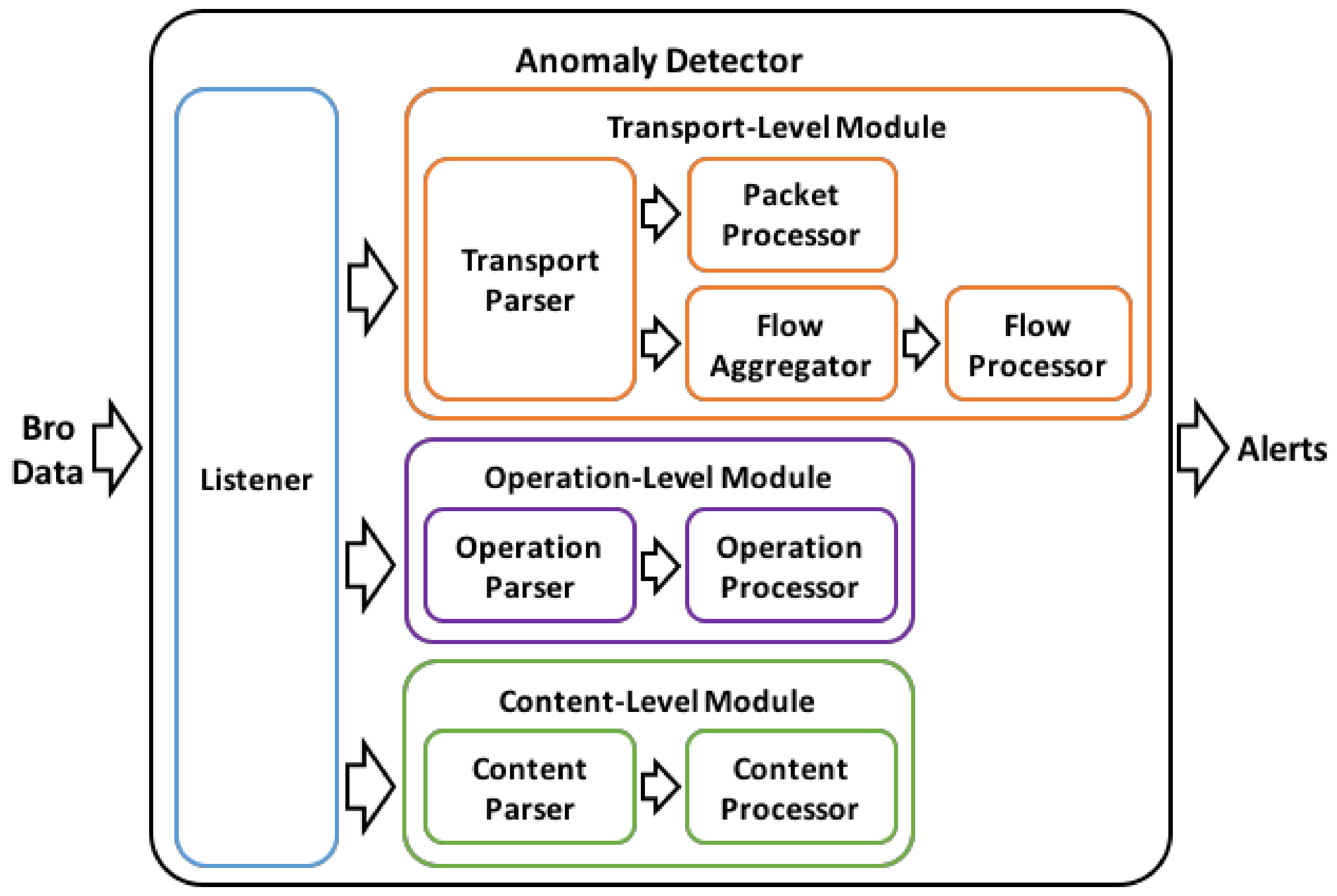
- It contains a multi-level anomaly detector to monitor all transport, operation and content levels of network traffic data passing by.
- Appropriate anomaly detection methods are applied based on the distinct characteristics of data in various levels.
- Alerts are aggregated and prioritized by an alert manager and sent back to control centers when anomalies are detected.



The anomaly analysis framework (future work) is located inside the central control centers.

- It contains a causality-based anomaly analyzer to analyze the alarms from substations.
- Domain knowledge and cyber-physical models of the system are utilized to aid the analysis of anomalies.
- Potential responses are analyzed and provided to the operator based on the analysis results.

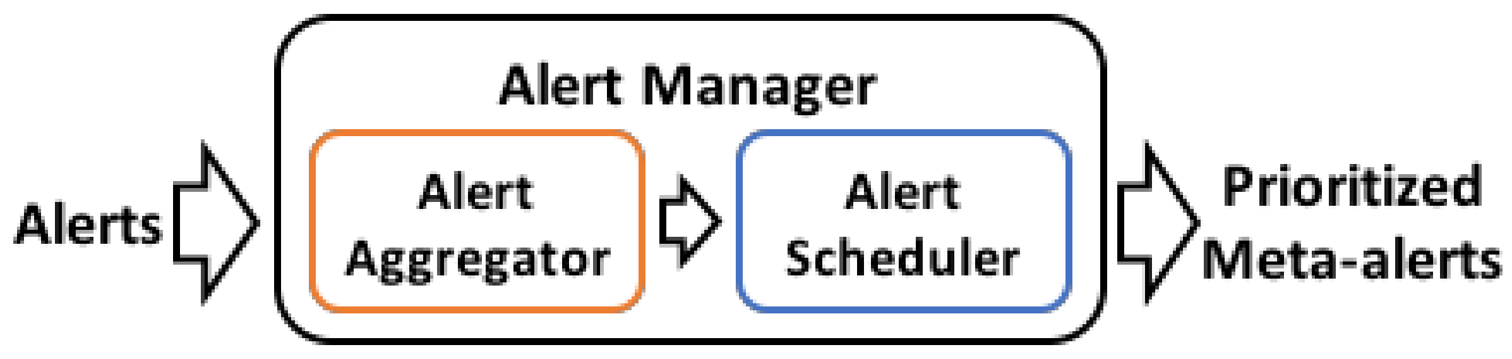
ANOMALY DETECTOR



We divide data in SCADA network traffic into three levels and apply appropriate anomaly detection methods respectively:

- Transport level: statistics in IP headers and transport protocol headers.
- Operation level: operation statistics in ICS protocols.
- Content level: measurement statistics from field devices.

ALERT MANAGER



The alert manager consists of two components:

- Alert aggregator: aggregates similar alerts to form meta-alerts.
- Alert scheduler: calculates priority scores of meta-alerts and decides their report frequencies.

PRELIMINARY RESULT

We inject various anomalies in the three levels:

- EDMAND is able to detect all the anomalies injected with a false positive rate of 0.007% .
- All the anomalies generate 12184 alerts in total, which are aggregated to 31 meta-alerts.

IMPACT ON INDUSTRIAL CONTROL SYSTEMS

What our framework provides for your system:

- Quick detection of anomalies on transport, operation, and content levels
- Potential causes and consequences of the detected anomalies
- Suggested responses to mitigate the anomalies

Business Benefit:

- Increased real-time situational awareness of your SCADA systems
- Actionable intelligence for your operators to react fast to attacks or failures

COLLABORATION OPPORTUNITIES

We are eagerly seeking cooperation, support, and guidance from industry partners in the following areas:

- Procedures the operators need to follow to deal with various failures in systems
- Dataset to better understand the traffic in SCADA systems and evaluate our framework

Contact: wren3@illinois.edu, yardley@illinois.edu, klara@illinois.edu

Activity webpage: https://cred-c.org/researchactivity/ContextAwareAD

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

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