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

Wenyu Ren, **Tim Yardley**, Klara Nahrstedt

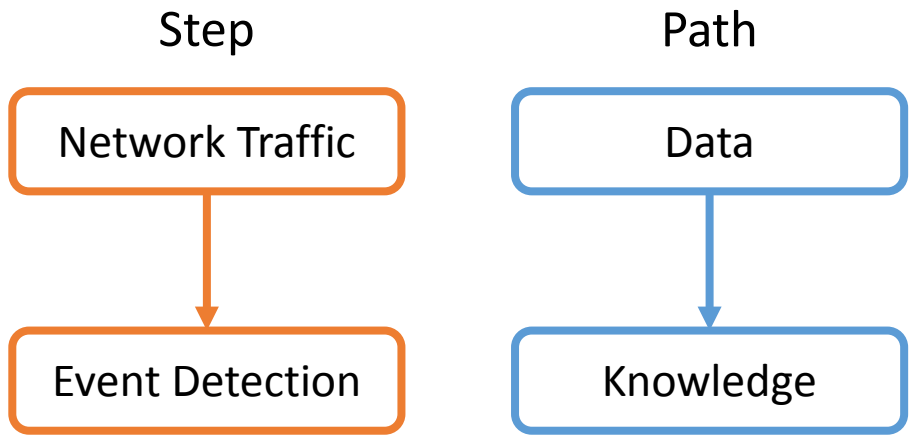
University of Illinois Urbana-Champaign, Urbana, Illinois, USA

Motivation

- SCADA (Supervisory Control and Data Acquisition)
  - Widely used in EDS to gather measurement data from field devices and send control commands to them
  - Vulnerable to various cyberattacks
    - Heterogenous resource-constrained end devices
    - legacy control protocols

Motivation

- Gap
  - Most of existing solutions only focus on monitoring and event detection of network state at the transport layer and perform flow-level analysis
  - Even solutions which parse the application protocol can usually detect the event only but fail to provide any causes and consequences of the event.

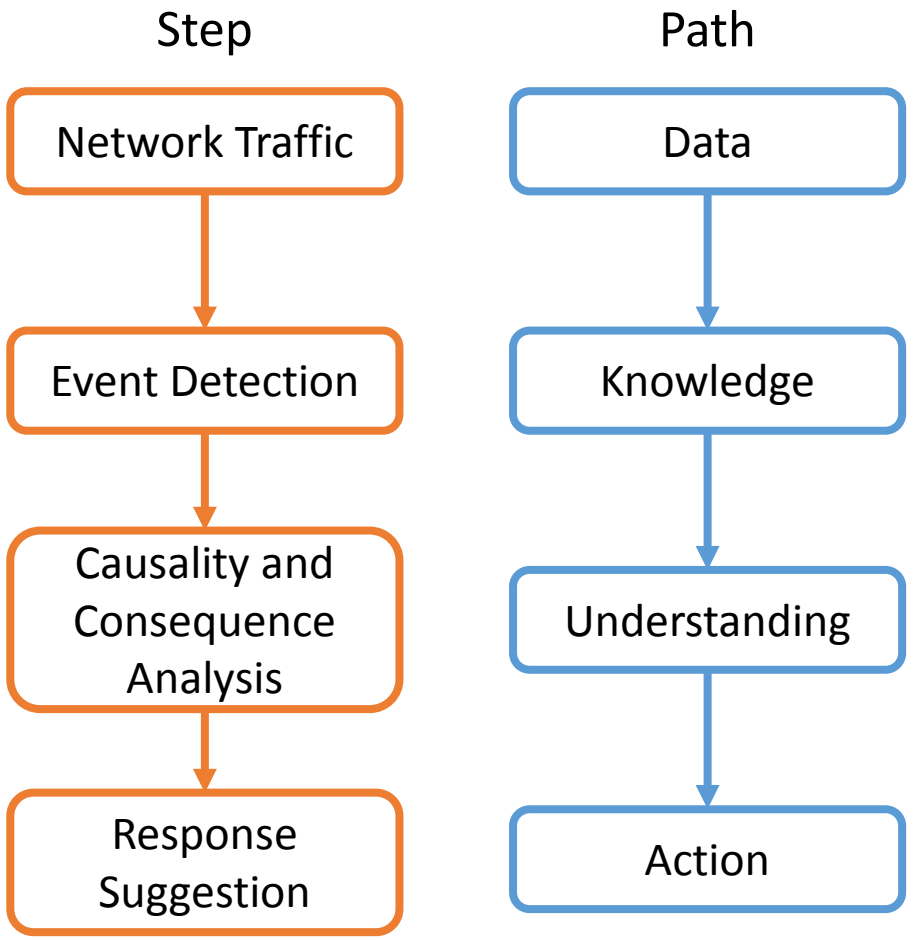


Our Approach

- Objective

  An online, context-aware, intelligent framework for anomaly detection, anomalous event analysis, causal reasoning, consequence indication and response suggestion for SCADA networks

- Feature
  - Utilizes not only transport-layer statistics but also application-layer statistics
  - Analyzes potential causes and consequences
  - Provides valuable response and recovery plan



Framework Architecture