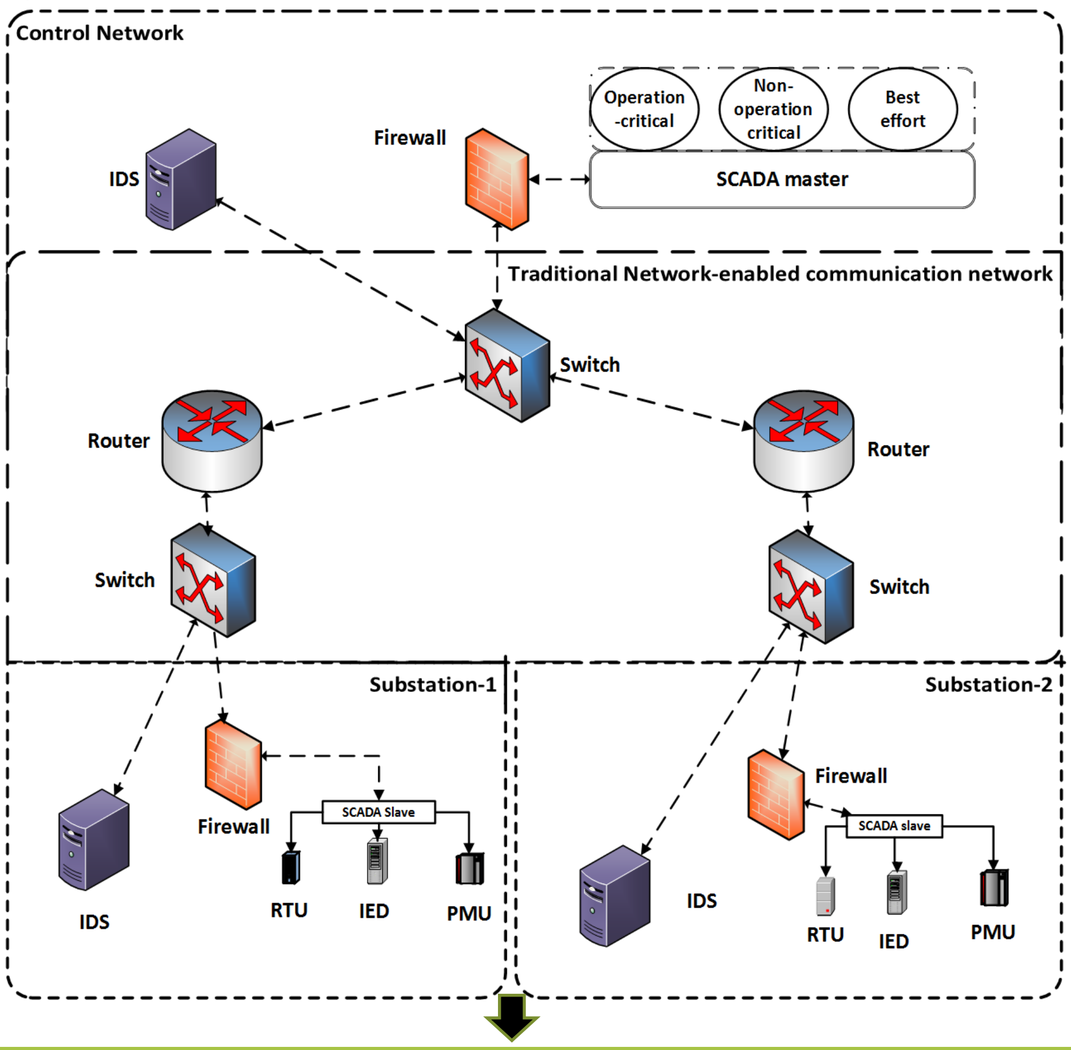
Modeling Cost of Countermeasures in Software Defined Networking (*SDN*)-Enabled Energy Delivery System (*EDS*)

Kamrul Hasan, Sachin Shetty, Amin Hassanzadeh, Malek Ben Salem, Jay Chen

EDS OPERATIONAL RESILIENCE

- Countermeasures deployed to mitigate cyber attacks in EDS may reduce the cyber risk at the cost of degrading operator resilience
- Need to maintain EDS QoS when countermeasure are applied to an operational EDS.

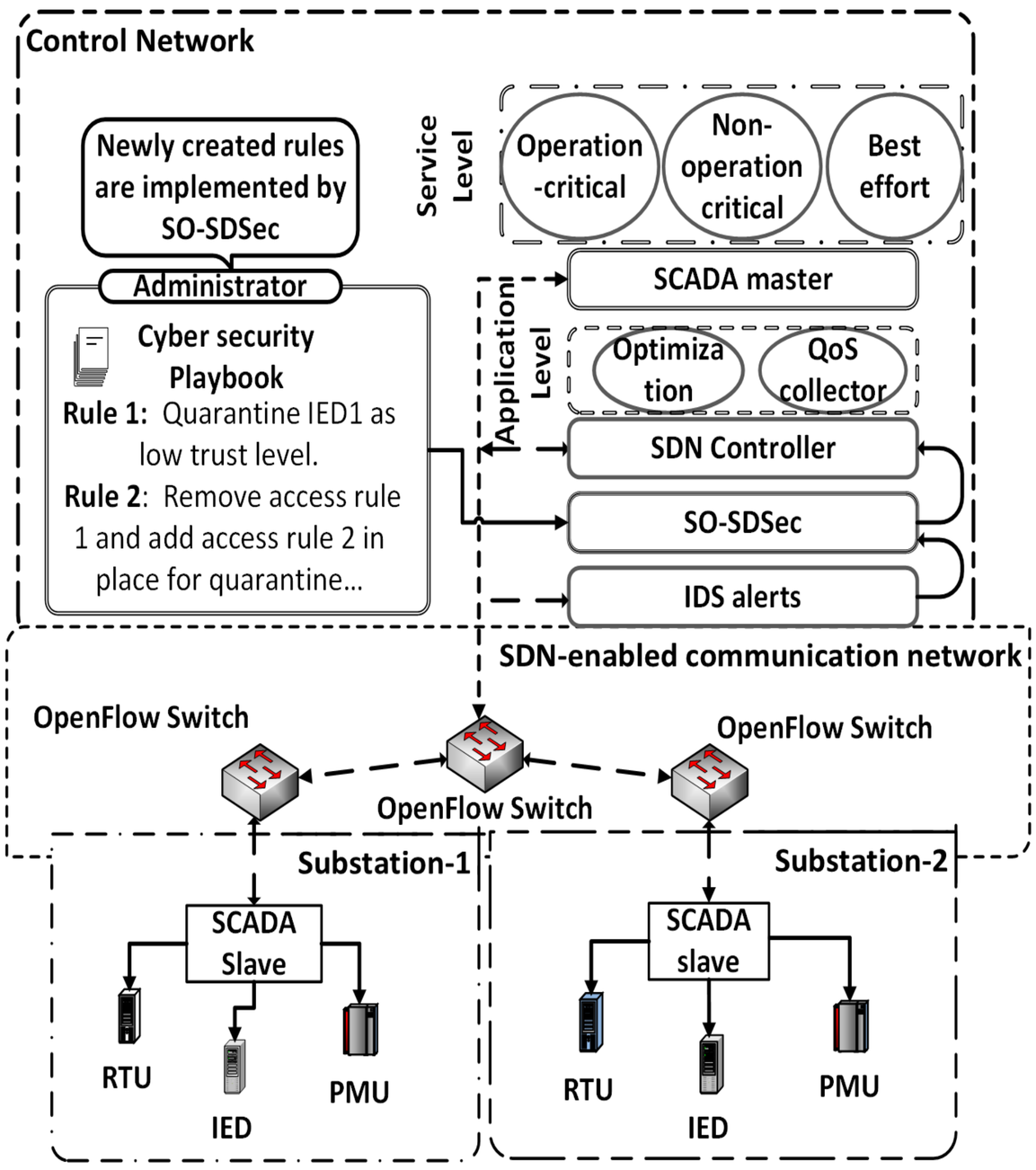


RESEARCH VISION

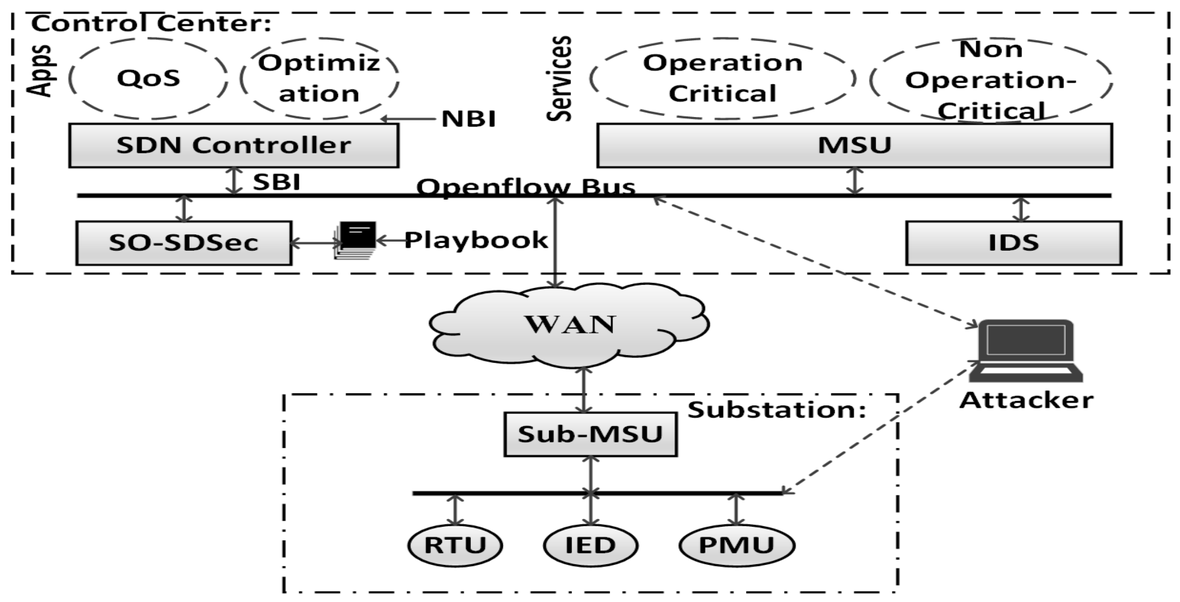
- Optimal selection of countermeasure which balances the tradeoff between security risk and quality of service .

RESEARCH APPROACH

- SDN-based architecture for autonomous attack containment which dynamically modifies access control rules based on configurable trust levels.
- Playbook which keeps a collection of work flow rules that define an OT organization's strategy to respond to certain cyber security events.
- Cost model to select the countermeasure which balances the tradeoff between security risk and quality of service.

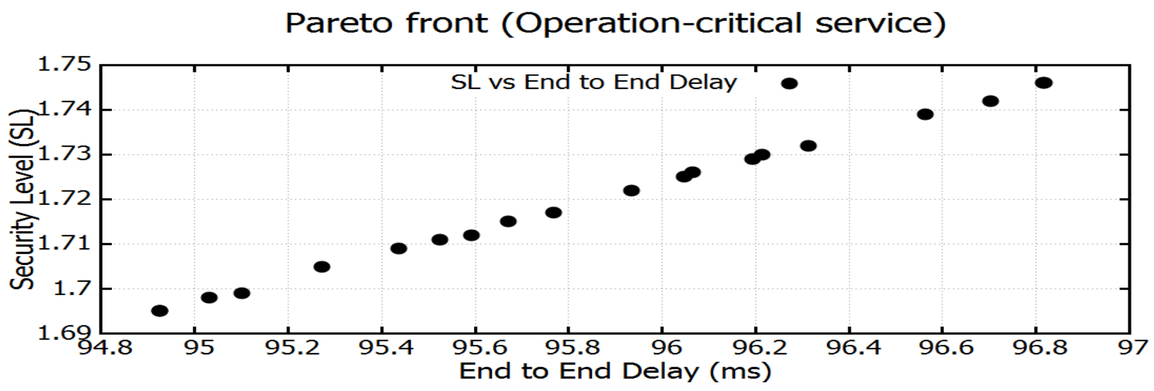


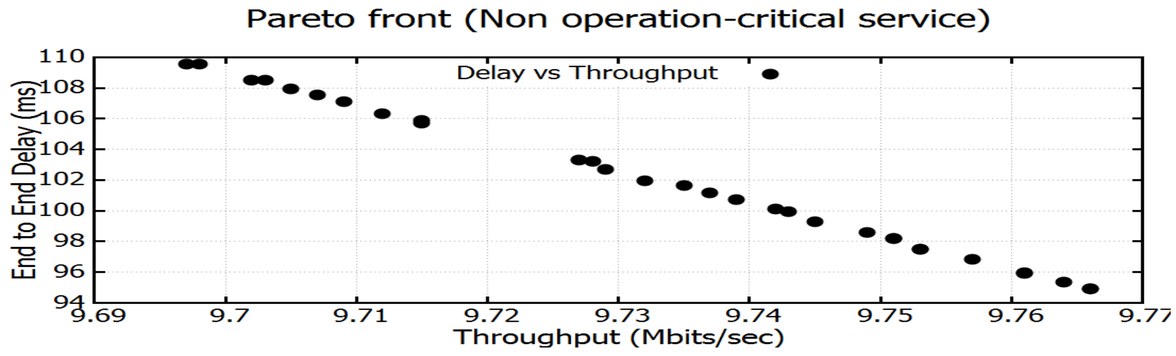
SYSTEM MODEL



- Alert → Playbook → Optimization → Apply Security Settings
- Message Authentication Code (MAC) and Key length represent cryptographic parameters that determine security risk and QoS settings.
- MAC and Key Length increase Security Level (SL) and impact packet delay and throughput in SCADA communication network.

SOME RESULTS FROM OUR WORK





- Substation automation control and monitoring and alarm/fault processing (**operation-critical services**) needs strict time constraint (≤ 100 ms) along with desired SL.
- Non-power system equipment monitoring and power quality monitoring, customer metering (**Non operation-critical service**) demands strict throughput ($\geq 97\%$).

IMPACTS ON GRID RESILIENCE

System Resilience Impact

- Optimal selection of countermeasures provides following benefits
  - Autonomous attack containment
  - Operational Resilience in presence of attacks
  - Runtime network orchestration automates response to attacks

Business Impact

- Reduce spread of impact of attacks
- Informs security investment by providing countermeasures that balance security risk and quality of service

COLLABORATION OPPORTUNITIES

Seeking collaborative opportunities from industry partners:

- Scenarios where SDN can play an effective role in automatically changing the network configuration to limit the impact of cyber attack
- Identifying required operational quality of service.
- Identifying parameters for determining operational resilience?

✓ Contact: sshetty@odu.edu

✓ Activity webpage: https://cred-c.org/researchactivity/modeling-security-risk-and-resiliency-eds-using-software-defined-networks-and

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