Research Spotlight Forum

8.6.19 Cybersecurity

Security@Edge: A smart grid and ML perspective

PRESENTED BY:

Jay Misra, CS@NMSU, misra@cs.nmsu.edu

Director, Networks and Systems Optimization Laboratory

Sandia National Laboratories | Georgia Institute of Technology | The University of New Mexico | Illinois | NM State University | Purdue University | New Mexico Tech | The University of Texas at Austin

SAND2018-14303 O

ABOUT YOURSELF

Associate Professor in CS since 2015, over 85 journal/conference papers, over 4600 citations, *h-index 21, i-10 index 30* published in CCS, TDSC, CODASPY, ICN, etc.

- Research areas: Scalable Security, Privacy, and Access Control in Future Internet Architectures, such as smart grid, IoT, internet, …
- Research group interests: Solving real-world problems with techniques, such as configurable crypto, zero knowledge proofs, blockchains, machine learning, and AI.
- **Size:** 6 PhD, 3 MS, and 3 UG students, with two postdocs. Four domestic and two women students.
- Belong to the Communication Security and Resilience Group
- Director, BS in Cybersecurity Program (starting Fall 2020)

Keywords:

Smart grid, IoT, IIoT, distributed ledger, provable security, trust management, adversarial AI.

About Us (Communication Security and Resilience Group)

Hardware Security

Wenjie Che

Reliable and Resilient Communication

David Mitchell

Cryptography, Privacy, Security

Roopa Vishwanathan

Secure and Trusted Networking, Resilience, Adversarial Machine Learning

Jay Misra

My General Research Interests

Internet of Things Cyber-physical Systems

Wireless Networks

High Performance Computing

Online Social Networks

Future Internet Architecture

Cybersecurity, Privacy, Reliability, Scalability, Access Control, Optimization, Network Analysis, System Modeling - Theory, Practice, Application

Publication Venues: ACM CCS, IEEE TDSC, ACM CODASPY, IEEE Internet of Things, IEEE Comm. Mag, IEEE SmartgridComm, ACM ICN, IEEE TWC, IEEE ComST.

Current Research Interests

Using Blockchains to enable:

- Distributed Credit Networks (CODASPY '19)
- Auditable Surveillance Processes (CCS '19)
- GDPR based data storage and post-disaster rescue

Security, privacy, and access control @ edge

- Verifiable computing by redundancy
- Trust management and reputation
- Data utilization with preservation of privacy and sustainable economic model
- Machine Learning and Security as a serice (ML-aaS, S-aaS) at the edge

Creating a resilient and scalable network architecture for cyber-threats aware solar smart grid distribution system

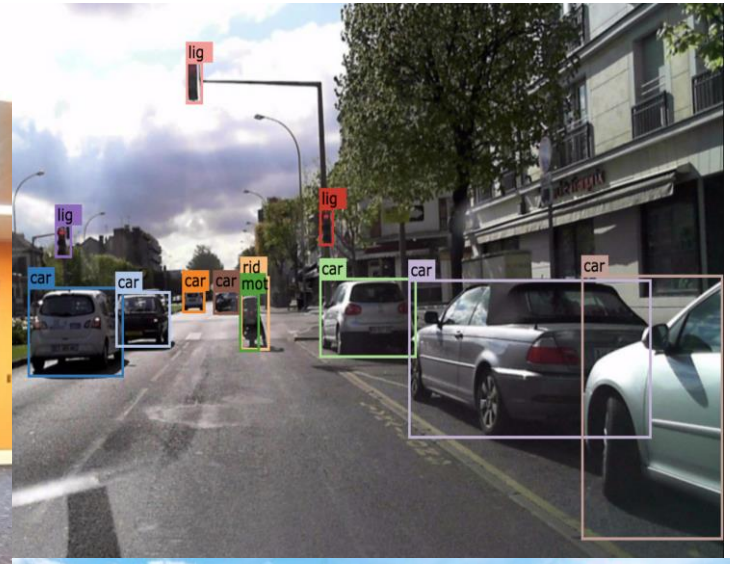
- Secure communications
- Threat assessment, mitigation, and reduction of impact of mitigation (recently funded by DoE)

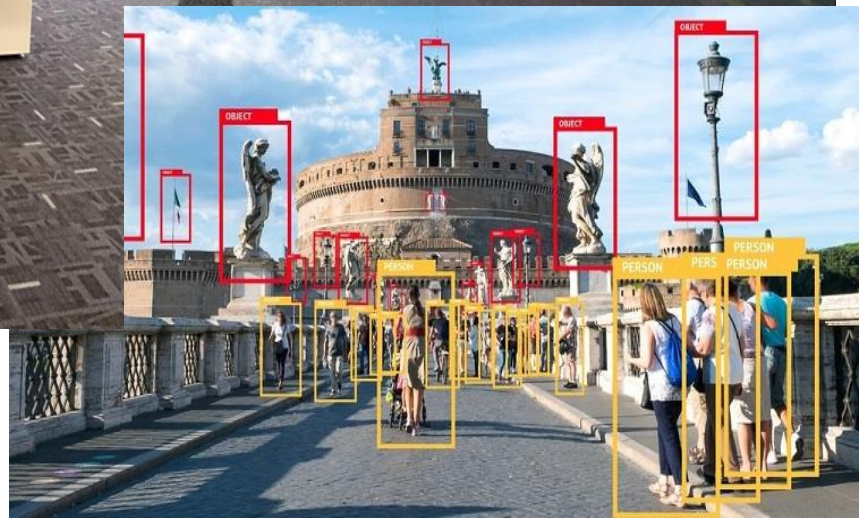
Quantum Computing and Post-Quantum Security

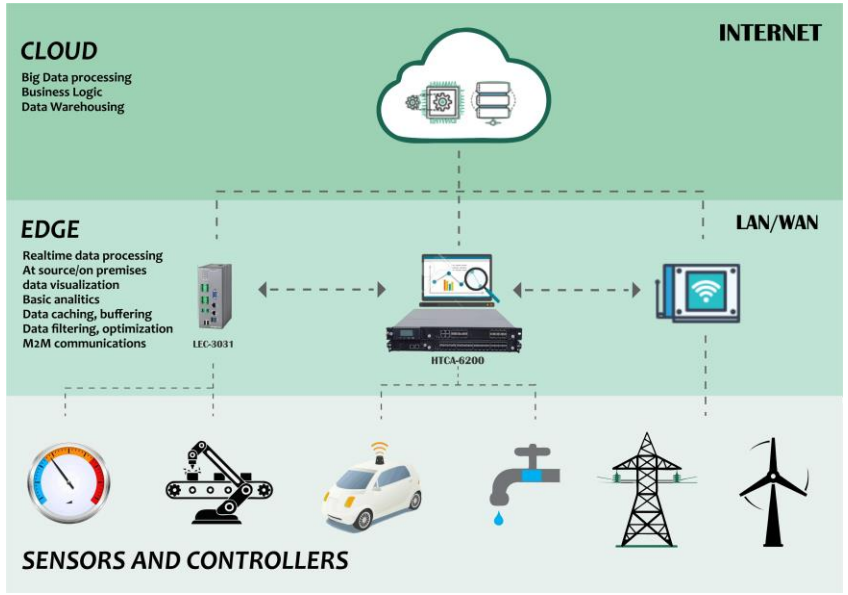
Blockchains use as a distributed ledger and messaging board

More from Roopa on this.

Edge Computing: Potential and Security and Privacy







Verifiable Computing

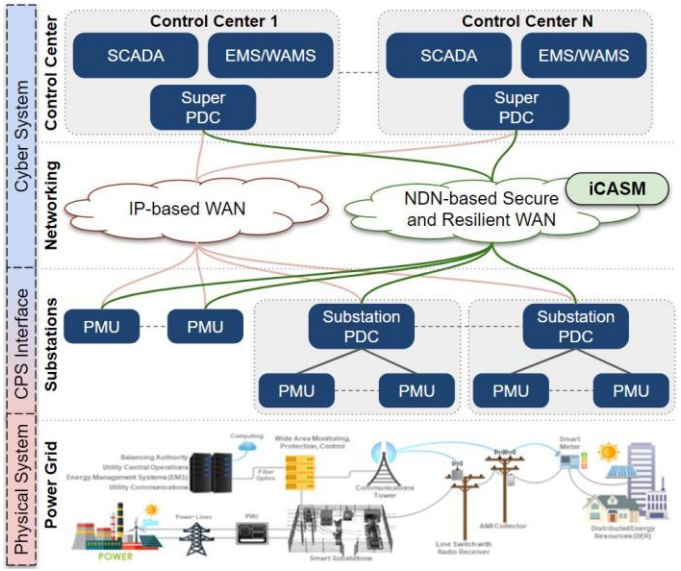
Service Discovery

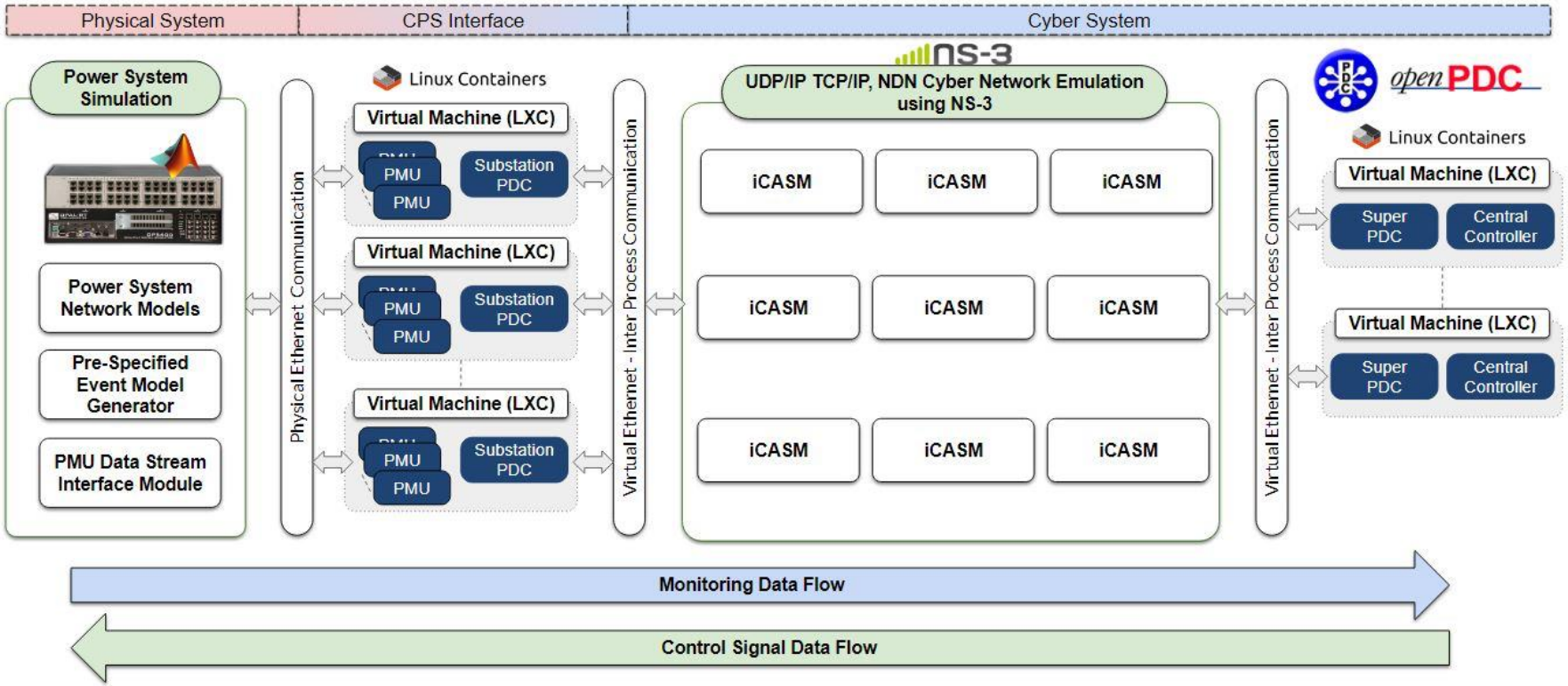
Compute Reuse

User and Data Privacy

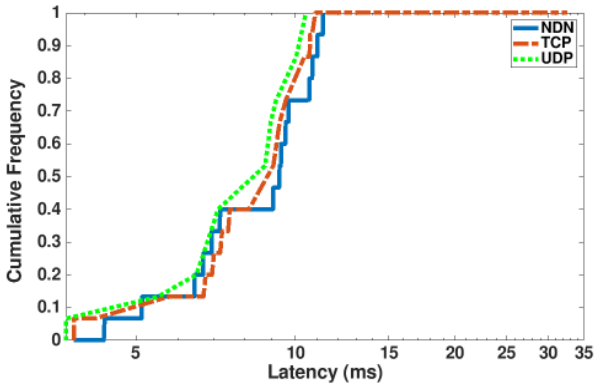
Distributed, Resilient ML

Cybersecurity for the Smart Grid: Resilient Networking and Configurable Security

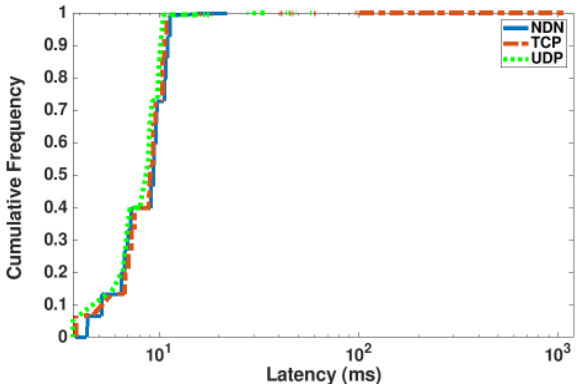




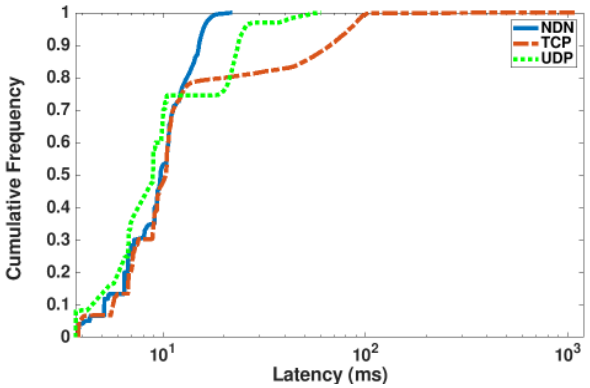
Initial Results



(a) 0% of Simulation Time

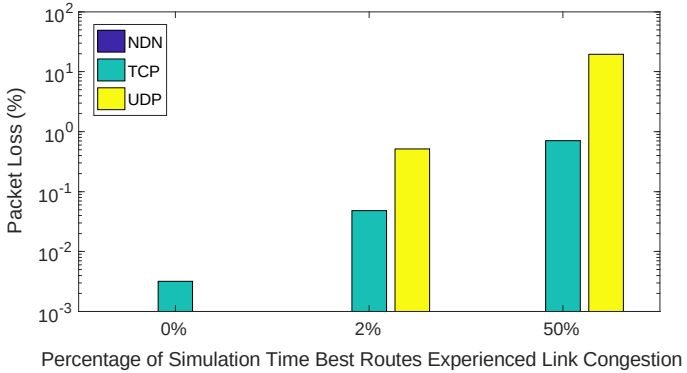


(b) 20% of Simulation Time

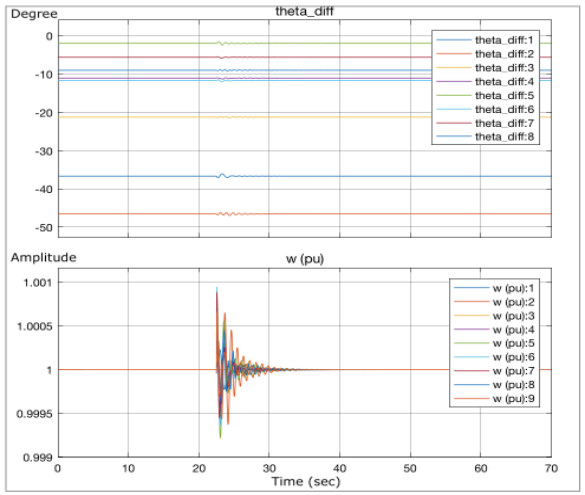


(c) 50% of Simulation Time

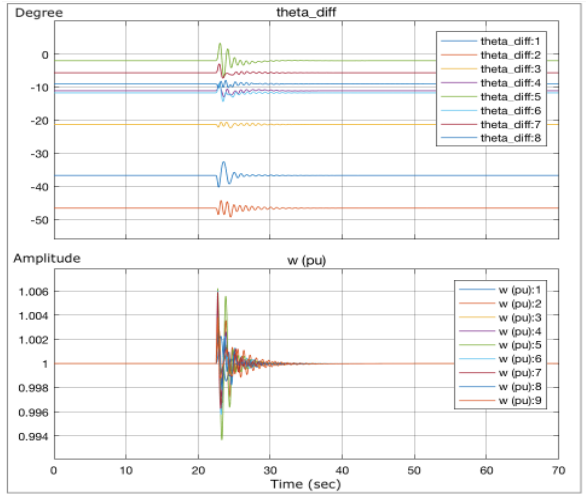
Performance in the face of congestion/jamming



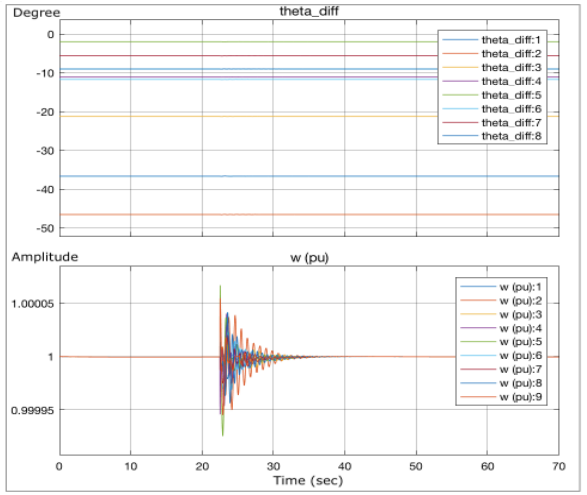
Pkt loss w/ congestion



(a) TCP



(b) UDP



(c) NDN

Faster Convergence

Future Work on this front…

Identify and model the communication, networking, and attack vectors and latency challenges; categorize them based on priorities.

Model different attacks (DDoS/DoS, jamming, blackhole, sinkhole attacks) and build solutions to mitigate the impact; also quantify the impact of the attacks.

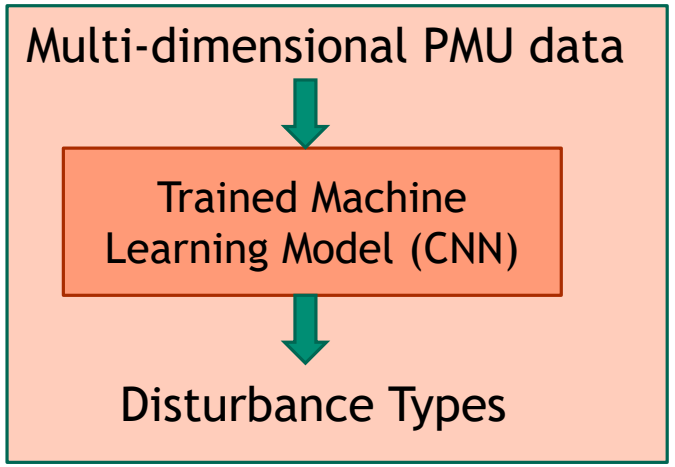
Create a rulebook for the utility operators to follow for security and privacy needs.

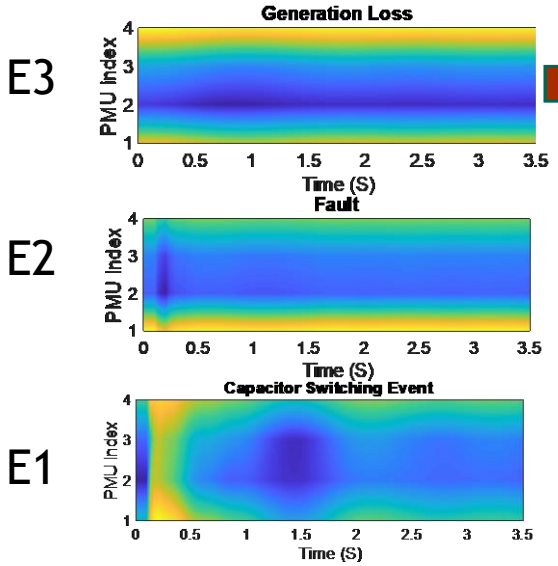
ML in the Smart Grid

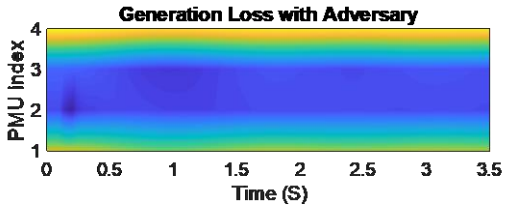
TrojanAI: Adversarial sample crafting to selectively alter outcomes of machine learning models. e. g, mis-classification of critical events by minimal perturbation of data from input sensors.

Machine learning models promising for monitoring, supervisory protection and control DSS.

Our preliminary work crafts coordinated adversaries which minimally alter the measurements sensed by a small set of selective PMUs to fool the AI-based wide area monitoring, protection and control systems (WAMPCS).







The Model predicts the event as Capacitor Switching (E1)

We also focus on the defense mechanisms that could potentially minimize adversary crafting.
Extend to data driven microgrid management / control, and smart meter data analytics.

FUNDING SOURCES

List funding sources of current projects, if applicable- especially joint work with Sandia, other NM Universities, or other Sandia Academic Alliance Universities (UT Austin, Georgia Tech, UIUC, or Purdue).

- CREST: Interdisciplinary Center for Research Excellence in Design of Intelligent Technologies for Smartgrids Phase II, Co-PI, total amount ~$5M, lead security and resilience subproject. (NSF)
- Optimal Reconfiguration and Resilient Control Framework for Real-Time Photovoltaic Dispatch to Manage Critical Infrastructure (ReDis-PV) $3.6M (UNCC, Clemson, Michigan Tech, INL). (DoE)
- ICN-WEN: Collaborative Research: ICN-Enabled Secure Edge Networking with Augmented Reality, NSF/Intel funded, Co-leading with UCLA, $2M. (NSF/Intel)
- EPSCoR grant – RII Track-1: The New Mexico SMART Grid Center: Sustainable, Modular, Adaptive, Resilient, and Transactive, ~$24M, (NMSU, UNM, NM Tech, …), co-lead networking and security subproject. (NSF)

RESEARCH NEEDS

Describe any gaps or new directions that would benefit from collaboration.

- Smart grid security and resilience (and critical infrastructure by translation)
- Adversarial machine learning and impact on critical infrastructure
- Quantum-safe computing and security