Internet of Battlefield Things

COLLABORATIVE RESEARCH ALLIANCE

Task 2.3: Fast and Adaptive Learning in Self-Aware IoBTs

B. Jalaian - ARL
S. Jha – SRI
P. Tabuada – UCLA
P. Thomas – U. Massachusetts
V. Veeravalli – UIUC
G. Verma – ARL
S. You – ARL
J. Smith - ARL

ILLINOIS · USC University of Southern California · UCLA · UMassAmherst · SRI International · Georgetown University

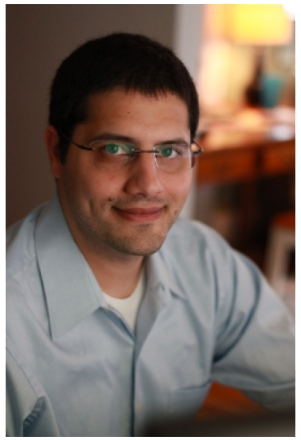
Team Members

Jalaian, ARL

Adversarial Machine Learning, Uncertainty Quantification for Machine Learning

Jha, SRI

Adversarial machine learning, formal methods



Thomas, UMass

Reinforcement Learning

Tabuada, UCLA

Cyber-physical systems, control, formal methods, security

Veeravalli, UIUC

Statistical inference, stochastic optimization, information theory

Verma, ARL

statistics, wireless networks, machine learning

You, *ARL*

Deep learning, image and signal processing

Smith, ARL

Mathematical Modeling

Task Goal

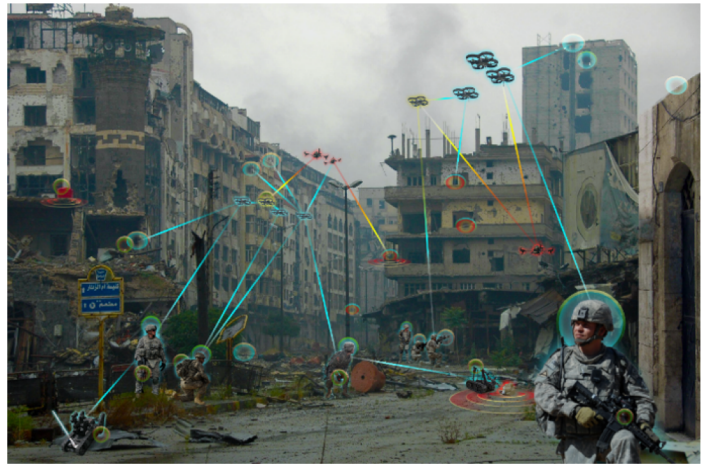
Goal:

- Enable improved intelligent interoperability, reliability,and survivability of IoBTs through a

  "principled fast and safe change detection and adaptation".

- Supporting "command-by-intent", "situational awareness", and "timely, decisive action".

- Relevant to Network C3I for Expeditionary Operations in line with Army's Modernization Priorities



Notional Example:
Contested urban environment with multimodal sensing (cameras, road sensors, mobile sensing drones) with network communication to obtain situational awareness for achieving mission goal.

Technical Approach

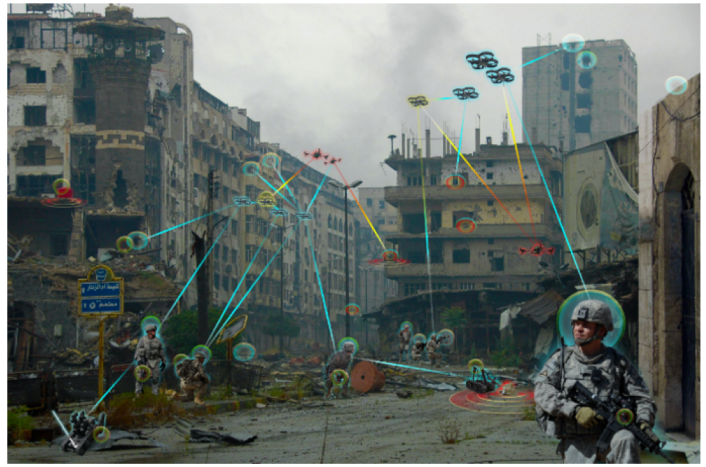
Goal: Develop safe autonomic reflexes in network that can quickly detect and adapt to uncertainty and adversarial perturbations

IoBT Challenges:

- Scale and heterogeneity of IoBT
- Rapidly evolving fast-tempo environment
- Need to operate in uncertainty and risk-sensitive decision-making
- Adversarial cyber and physical perturbations in operationally-contested environment
- Need to ensure safety of adaptation decisions

Approach:

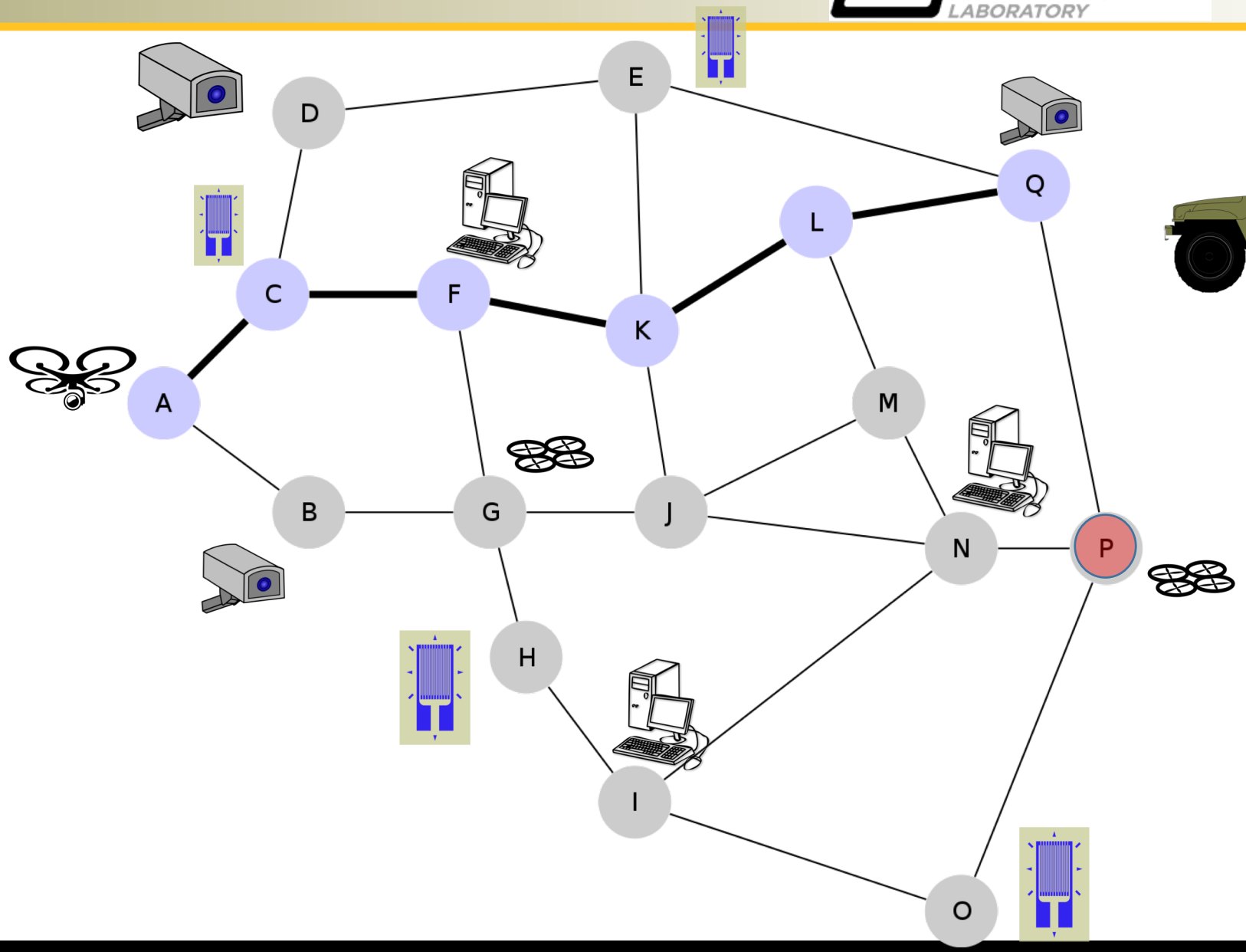
- Quick detection of concept drift and sudden changes
- Detection of adversarial and out-of-distribution data
- Robust state estimation in presence of adversaries
- Safe reinforcement learning for adaptation

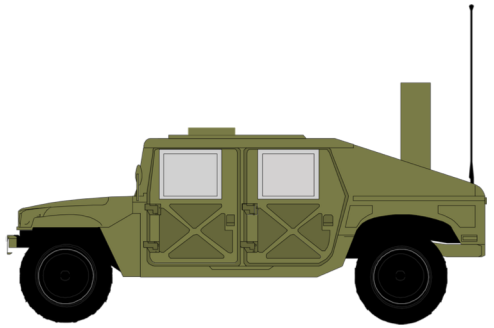


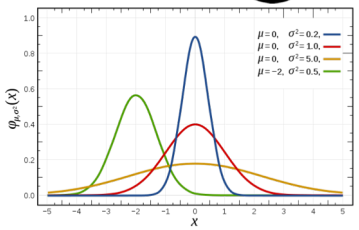
Notional Example:

Contested urban environment with multimodal sensing (cameras, road sensors, mobile sensing drones) with network communication to obtain situational awareness for achieving mission goal.

Task 2.3: Fast and Adaptive Learning







Model-based change detection

Concept Drift

Model Change

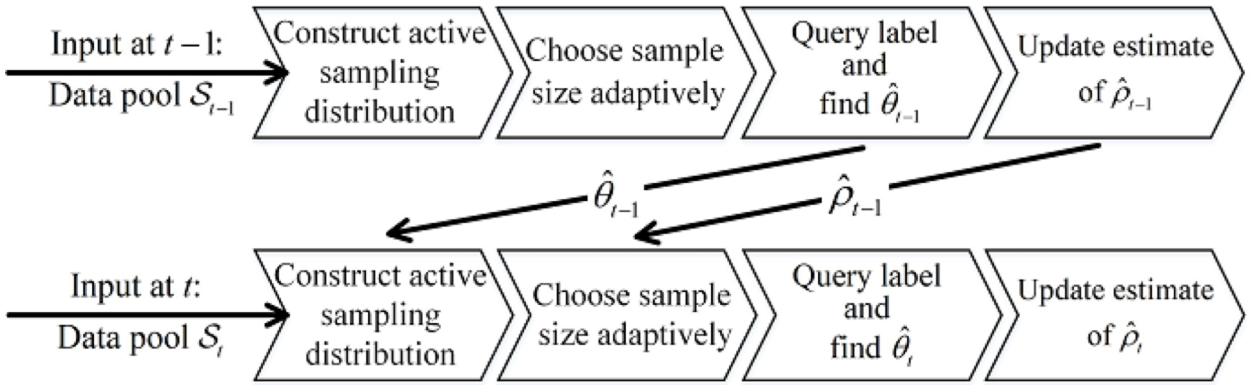
Task 2.3: Fast and Adaptive Learning

Addressed Army Need: Supporting machine learning functions in rapidly changing battlefield environments

- Active and adaptive sequential learning strategies for learning tasks that change in a bounded manner:

$$\ell(y|x,\theta) \triangleq -\log p(y|x,\theta)$$

$$L_{U_t}(\theta) \triangleq \mathbb{E}_{X\sim U_t, Y\sim p(Y|X,\theta_t^*)}[\ell(Y|X,\theta)]$$

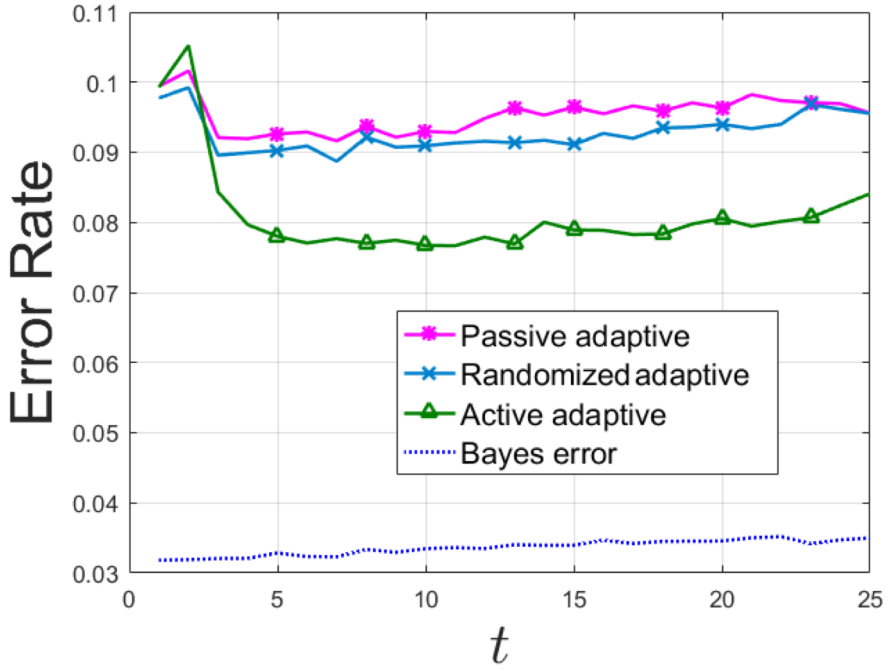


Passive means drawing new samples using a uniform distribution

Random means replacing the estimate of θ_{t-1} with a random point from Θ

Active and adaptive learning framework can significantly improve accuracy while being efficient in the use of training samples

$$\|\theta_t^* - \theta_{t-1}^*\|_2 \leq \rho_t$$



Tracking user preferences (Yelp 2017 dataset)

Task 2.3: Fast and Adaptive Learning

Addressed Army Need: Supporting machine learning functions in rapidly changing battlefield environments

- Model change detection strategies for detecting abrupt changes in tasks:
  - Generalized likelihood ratio test, test based on Jensen-Shannon divergence, and test based on maximum mean discrepancy (MMD)

$$\ell(y|x,\theta) \triangleq -\log p(y|x,\theta)$$

$$L_{U_t}(\theta) \triangleq \mathbb{E}_{X\sim U_t, Y\sim p(Y|X,\theta_t^*)}[\ell(Y|X,\theta)] \qquad \|\theta_t^* - \theta_{t-1}^*\|_2 \leq \rho$$

$$H_0 : (\theta,\theta') \in \chi_0 \triangleq \{(\theta,\theta') | \, \|\theta-\theta'\|_2 \leq \rho\},$$
$$H_1 : (\theta,\theta') \in \chi_1 \triangleq \{(\theta,\theta') | \, \|\theta-\theta'\|_2 > \rho\},$$

$$2JS(P,P') \triangleq D(P\|\overline{P}) + D(P'\|\overline{P}),$$

where $\overline{P} = \frac{P+P'}{2}$ and $D(\cdot\|\cdot)$ denotes the KL divergence.

$$\delta_{\mathrm{ED}} = \begin{cases} 1, & \text{if } \hat{JS}(\mathcal{S},\mathcal{S}') \geq \eta \\ 0, & \text{if } \hat{JS}(\mathcal{S},\mathcal{S}') < \eta \end{cases}$$

$$\hat{JS}(\mathcal{S},\mathcal{S}') = \sum_{i=1}^{n} \log \frac{2f_{\hat{w}_{ERM}}(x_i,y_i)}{f_{\hat{w}_{ERM}}(x_i,y_i) + f_{\hat{w}'_{ERM}}(x_i,y_i)} + \sum_{i=1}^{n} \log \frac{2f_{\hat{w}'_{ERM}}(x'_i,y'_i)}{f_{\hat{w}_{ERM}}(x'_i,y'_i) + f_{\hat{w}'_{ERM}}(x'_i,y'_i)}$$

$$\hat{w}_{\mathrm{ERM}} \triangleq \arg\min L(w), \qquad \hat{w}'_{\mathrm{ERM}} \triangleq \arg\min L'(w)$$

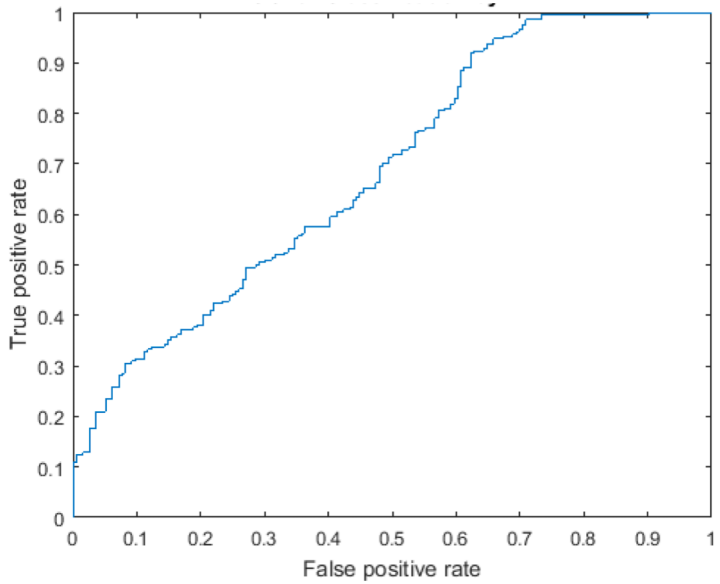
$$L(w) \triangleq -\sum_{i=1}^{n} \log f_w(X_i,Y_i), \qquad L'(w) \triangleq -\sum_{i=1}^{n'} \log f_w(X'_i,Y'_i).$$

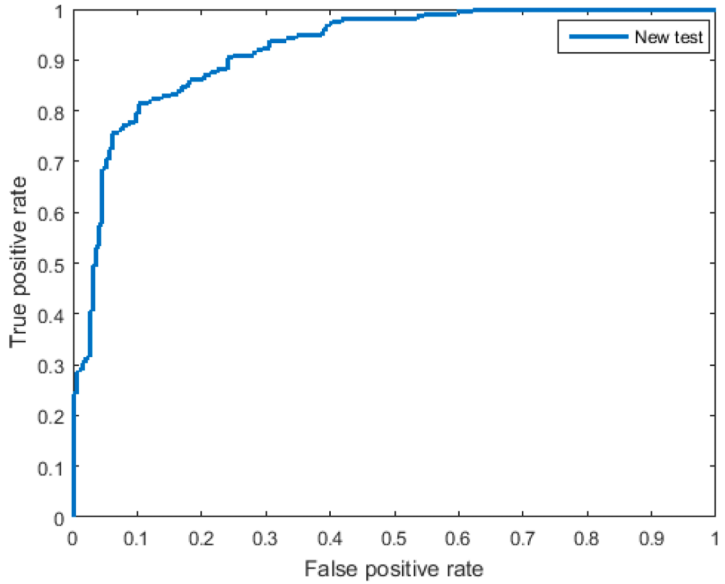
Task 2.3: Fast and Adaptive Learning

Addressed Army Need: Supporting machine learning functions in rapidly changing battlefield environments

Experiments and Results:

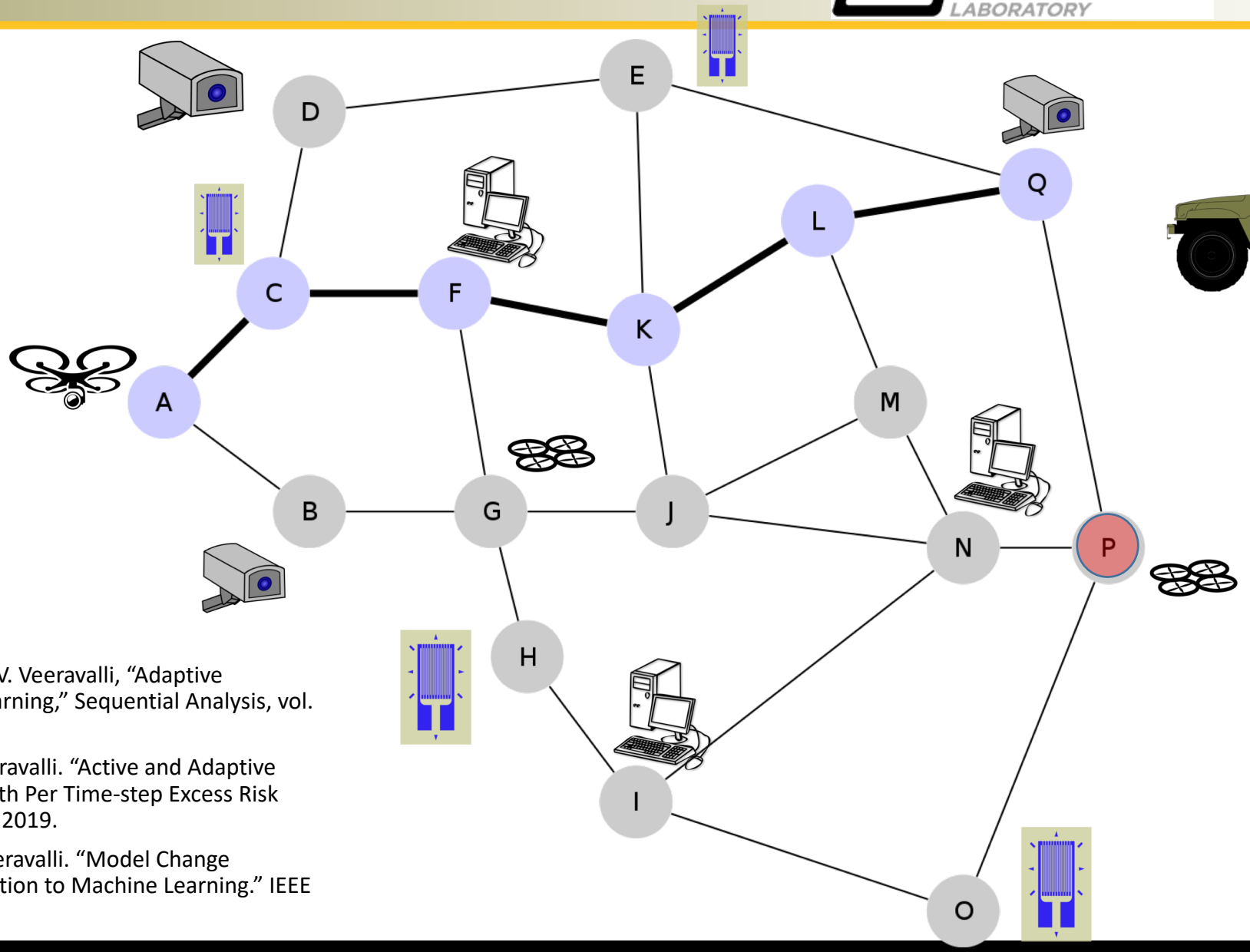
- Model change detection: **Landmines dataset**
  - The goal is to detect landmines in specific regions. Overall 29 binary classification tasks
  - Each datum is a 9-dimensional feature vector from radar images that capture a single region of landmine fields
  - Tasks 1-15 correspond to regions that are relatively highly foliated. Other 14 tasks are bare earth or desert
  - $^{29}C_2 = 406$ number of pairs to test whether the distribution is same.

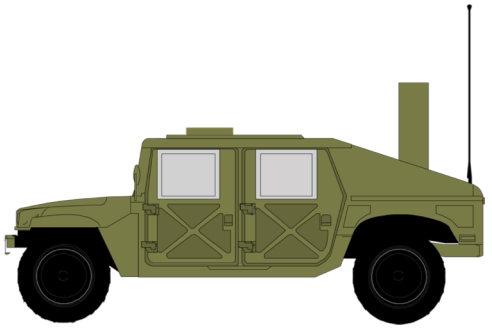


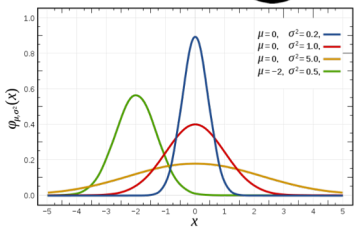


Tests based on Jensen-Shannon divergence and MMD effective in detecting model changes

Task 2.3: Fast and Adaptive Learning







Model-based change detection

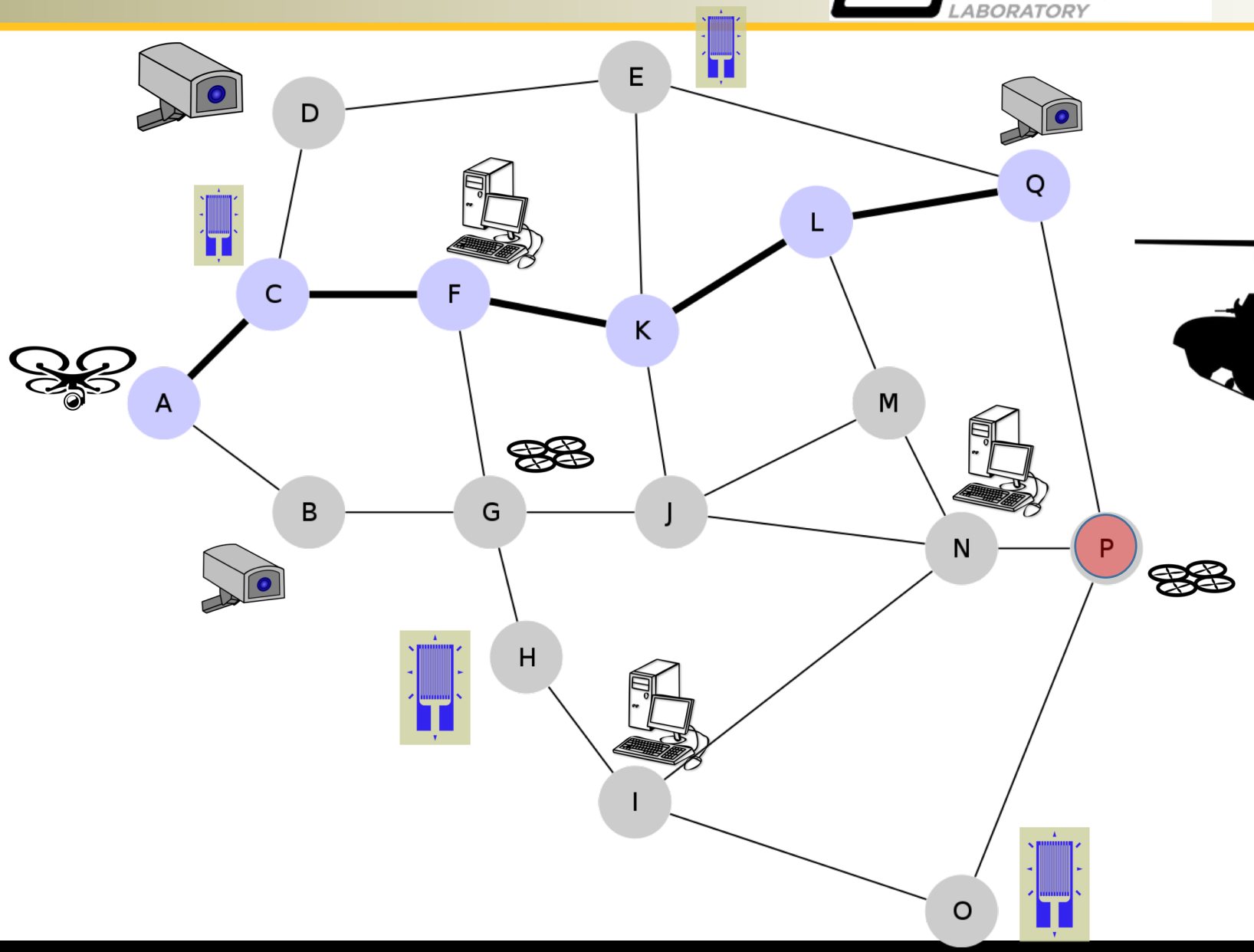
Concept Drift

Model Change

Key Publications:

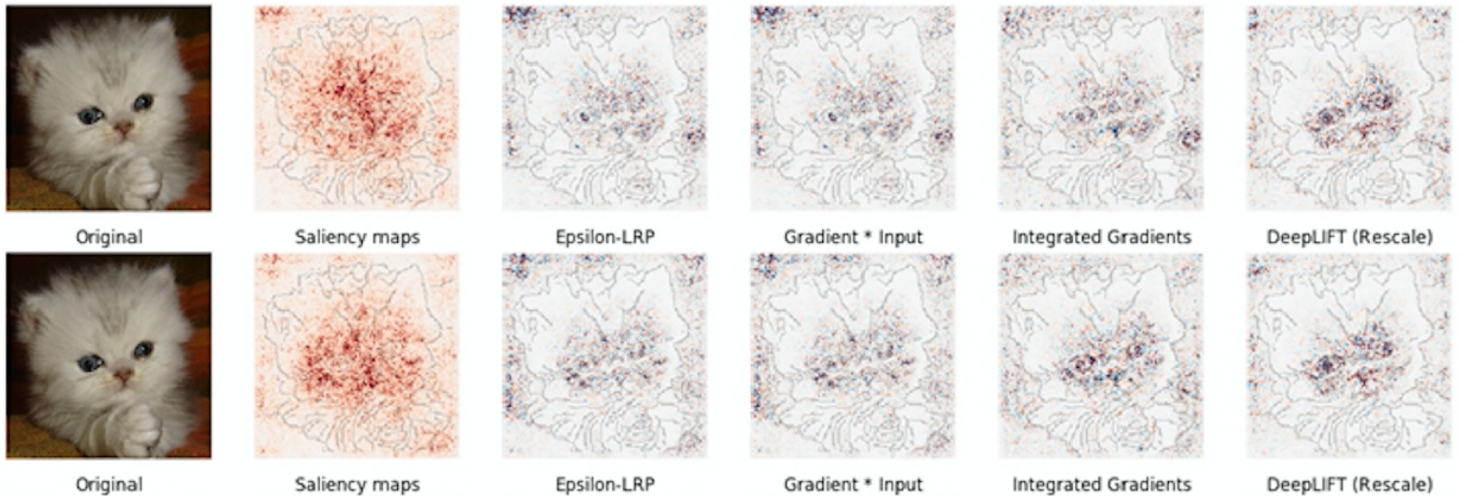
- C. Wilson, Y. Bu, and V.V. Veeravalli, “Adaptive sequential machine learning,” Sequential Analysis, vol. (to appear), 2020
- Y. Bu, J. Lu and V.V. Veeravalli. “Active and Adaptive Sequential Learning with Per Time-step Excess Risk Guarantees,” Asilomar 2019.
- Y. Bu, J. Lu, and V.V. Veeravalli. “Model Change Detection with Application to Machine Learning.” IEEE ICASSP 2019.

Task 2.3: Fast and Adaptive Learning



Adversarial Attack

Digital Physical



Young (1985) demonstrated that Shapley values are the only set of values that satisfy these properties.

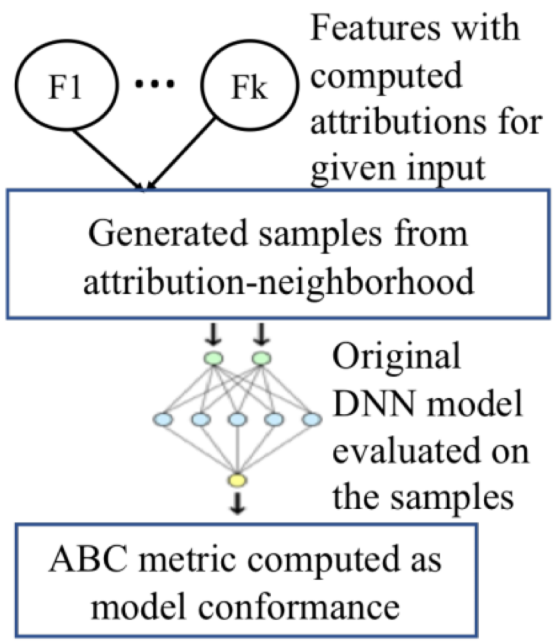
$$a_i = \sum_{z \subseteq x} \frac{|z|!\,(M - |z| - 1)!}{M!} \left[f_x(z) - f_x(z' \setminus \{x^i\}) \right]$$

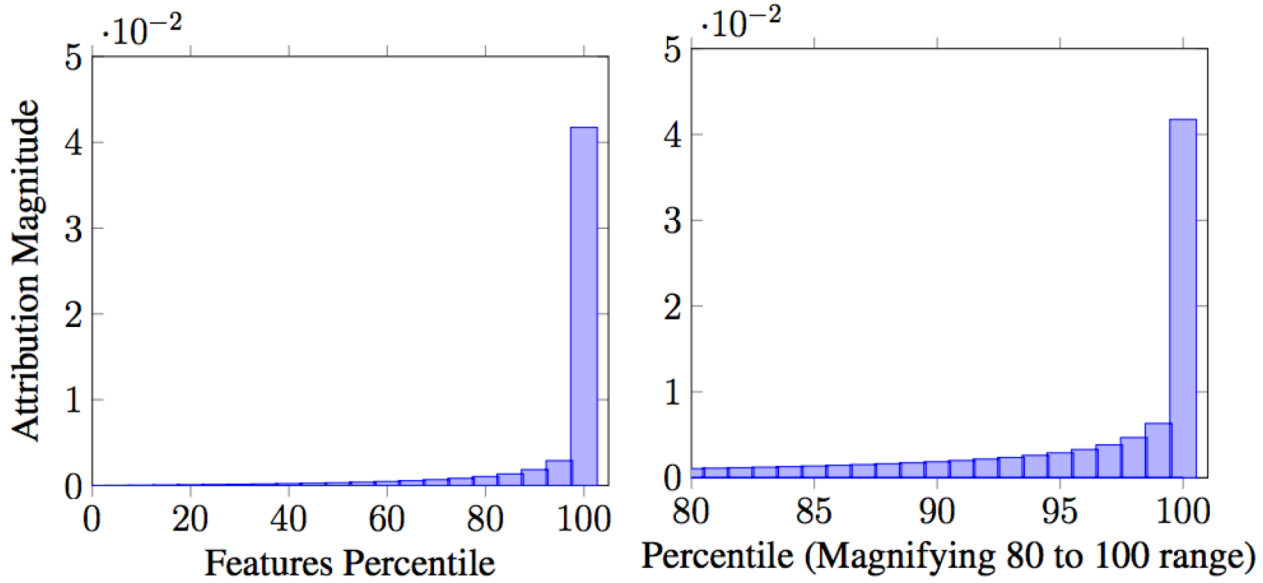
Apply sampling approximations to above equation and approximate the effect of removing a variable from the model by integrating over samples.

Baseline and path based methods.

Friedman, Eric J. Paths and consistency in additive cost sharing. International Journal of Game Theory, 32(4): 501–518, 2004.

Given $\gamma = (\gamma_1, \ldots, \gamma_n)$: $[0,1] \rightarrow R^n$ be a smooth function specifying a path in R^n from baseline x^b to input x, that is, $\gamma(0) = x^b, \gamma(1) = x$.

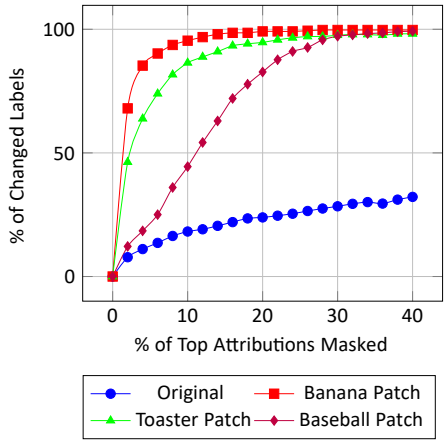




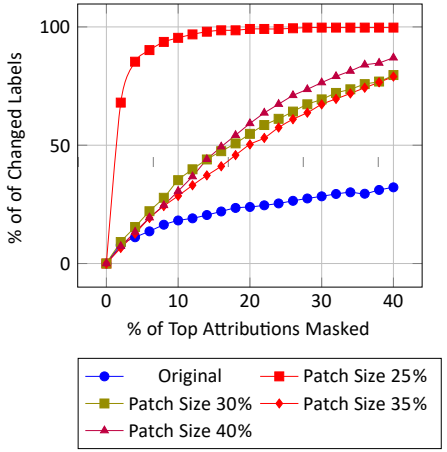
Feature Concentration in well-trained models

Theorem 1. *The sensitivity of the output* $\mathcal{F}(\mathbf{x})$ *with respect to an input feature* $\mathbf{x}_j$ *in the neighborhood of* $\mathbf{x}$ *is approximately the ratio of the attribution* $\mathcal{A}_j(\mathbf{x})$ *to the value of that feature* $\mathbf{x}_j$*, that is,* $\frac{\mathcal{A}_j(\mathbf{x})}{\mathbf{x}_j}$.

Task 2.3: Fast and Adaptive Learning



Dropping 0.4% of the attribution causes 99.71% of the attacks based on banana patches, 98.14% of the attacks based on toaster patches, and 99.20% of the attacks based on baseball patches to be detected.

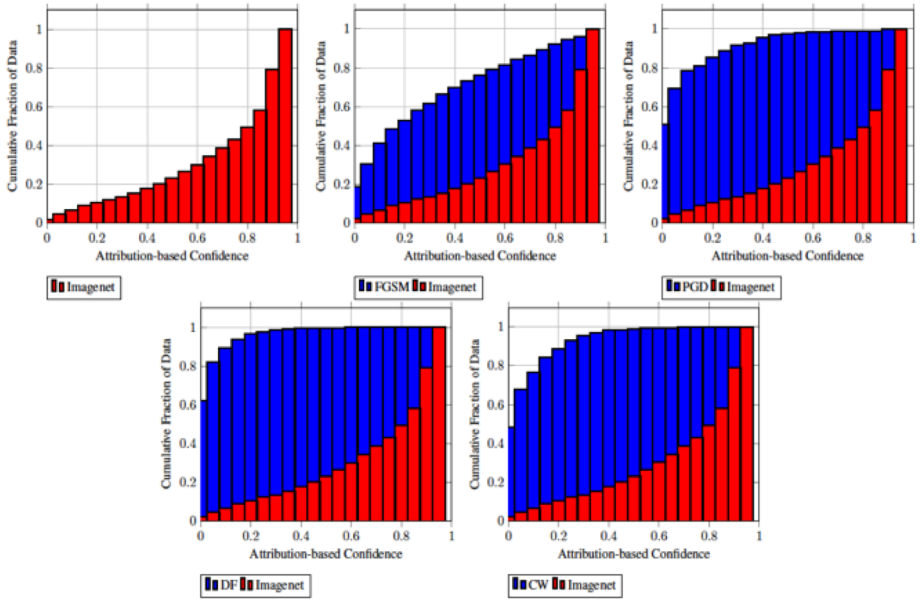


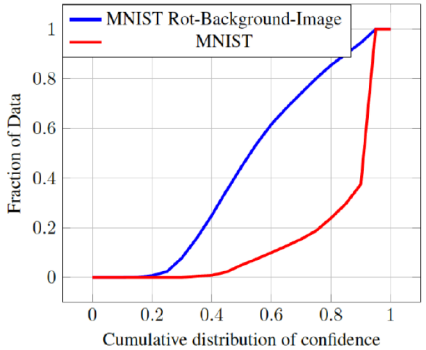
Masking 0.4% of attributions caused nearly 80% of labels to change for images with adversarial patches.

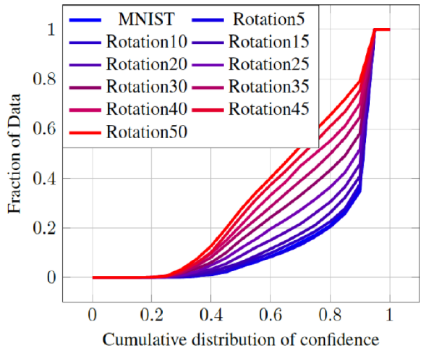
Image with a banana patch generated using adversarial patch method

Masking its top 0.2% of attribution

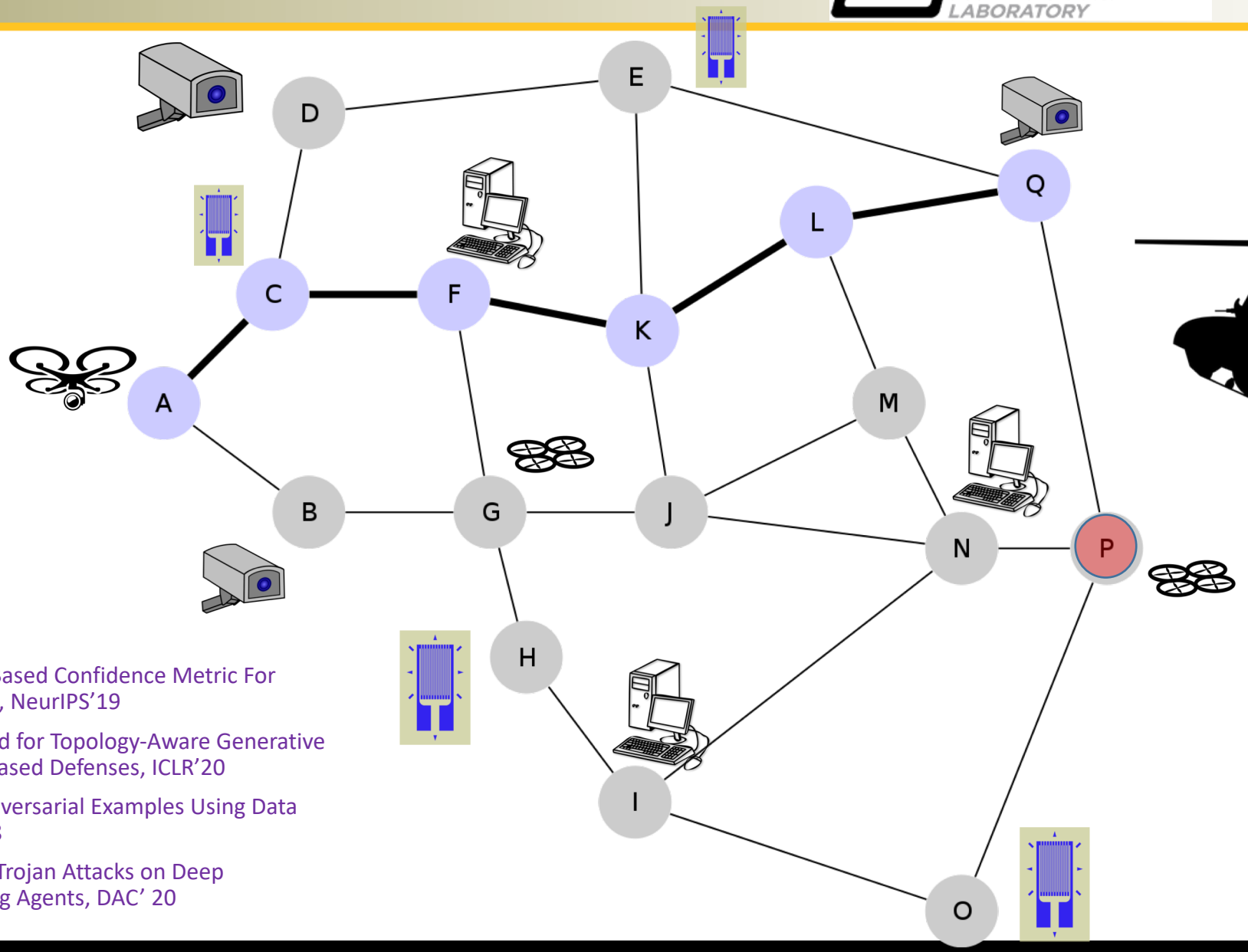
Masking its top 0.4% of attribution







Task 2.3: Fast and Adaptive Learning



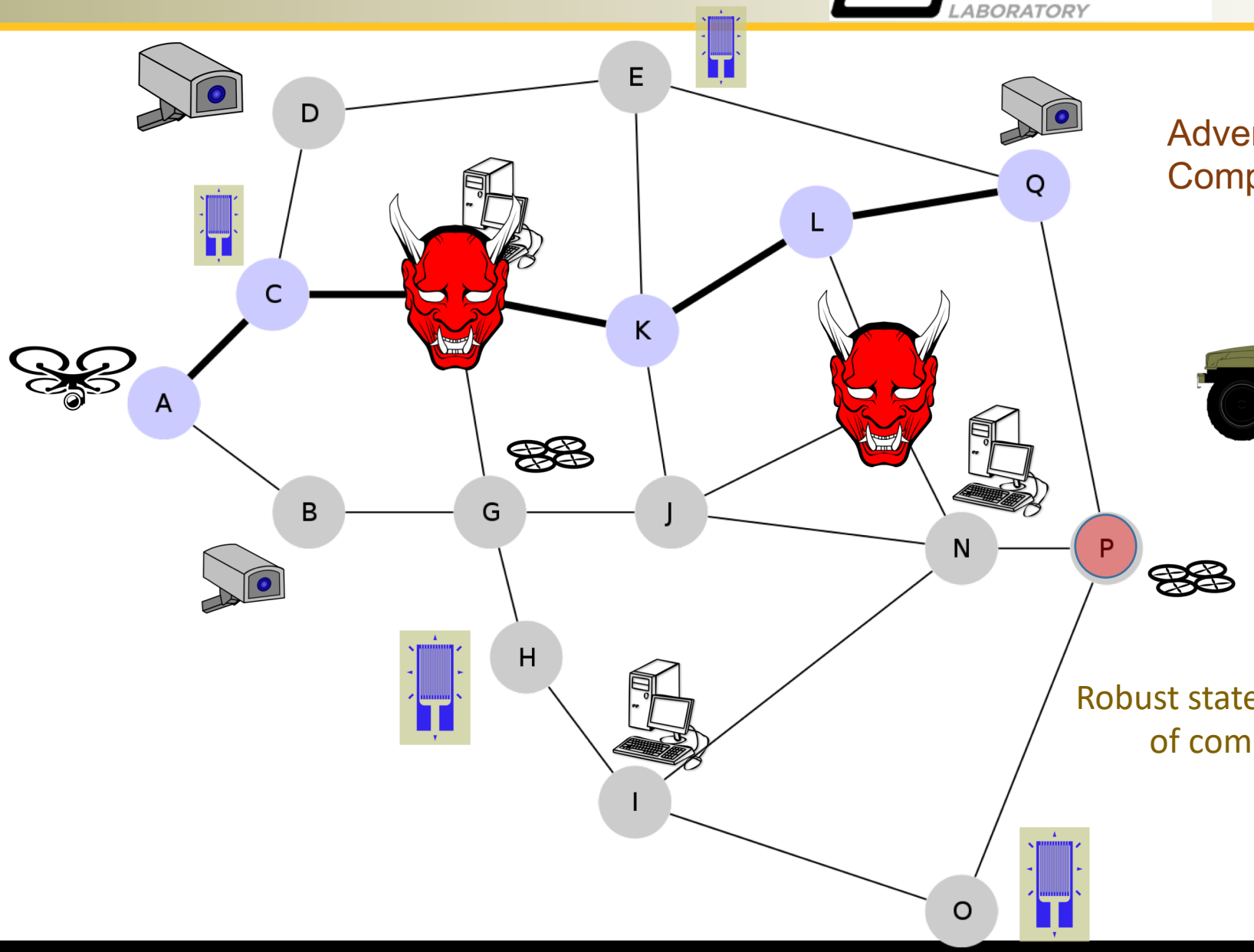
Adversarial Attack

Digital Physical

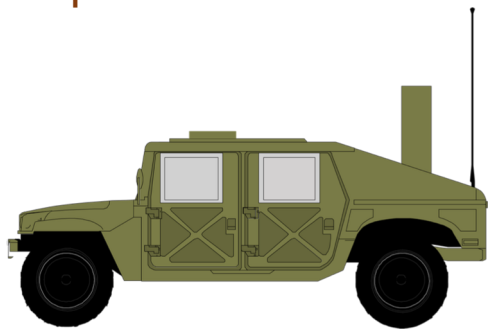
Key Publications:

- Jha et. al. Attribution-Based Confidence Metric For Deep Neural Networks, NeurIPS'19
- Jang et. al. On the Need for Topology-Aware Generative Models for Manifold-Based Defenses, ICLR'20
- Jha et. al. Detecting Adversarial Examples Using Data Manifolds, MILCOM'18
- Kiourti et. al. TrojDRL: Trojan Attacks on Deep Reinforcement Learning Agents, DAC' 20

Task 2.3: Fast and Adaptive Learning



Adversarial Attack and Compromised Nodes



Robust state estimation in presence of compromised IoBT nodes.

Task 2.3: Fast and Adaptive Learning

- Model the dynamics of sensed quantities as a linear dynamical system: $x(k+1)=Ax(k)$,
  with measurement equation: $y(k)=Cx(k)+e(k)$,
  subject to the adversarially injected signal e.

- We assume the adversary can attack at most s sensors (at most s entries of e are non-zero)

- **Objective**: estimate the state x despite the presence of the injected signal e.

Given a sequence of measurements $y(0), y(1), \ldots, y(k)$ we need to compute a subset of (malicious) sensors so that the data provided by the non-malicious sensors obeys the linear dynamics.

If there are p sensors and at most s are under attack, we need to search over all possible "p choose s" subsets of sensors.

Task 2.3: Fast and Adaptive Learning

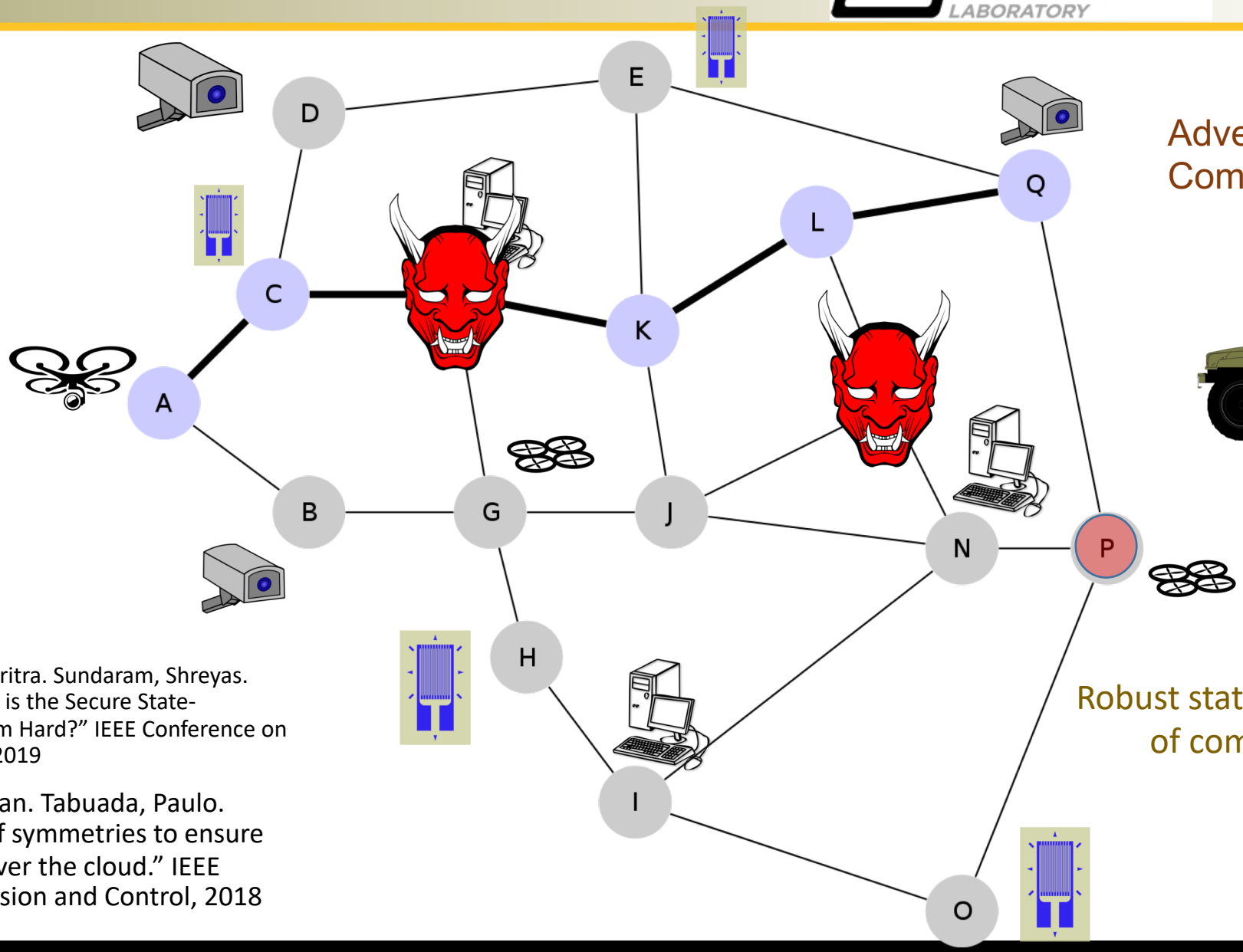
Given a sequence of measurements $y(0), y(1), \ldots, y(k)$ we need to compute a subset of (malicious) sensors so that the data provided by the non-malicious sensors obeys the linear dynamics:

$$x(t+1)=Ax(t),\ y(t)=Cx(t)$$

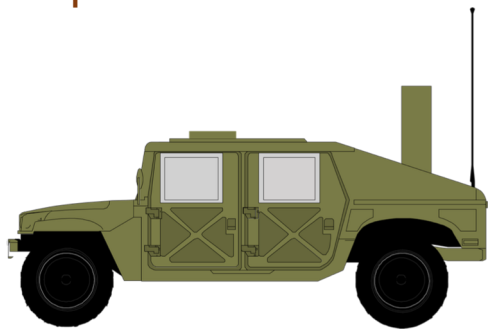
If there are p sensors and at most s are under attack, we need to search over all possible "p choose s" subsets of sensors.

- We showed this problem is, in general, NP-Hard.
- We identified a large class of problems that can be solved in polynomial time: the eigenvalues of the matrix A have geometric multiplicity 1.
- Investigated a more challenging version of this problem where sensor data is routed through a network with attacked nodes and links. Identified necessary and sufficient conditions to solve this problem, relating (A,C) to the number of sensors and network nodes/links under attack.

Task 2.3: Fast and Adaptive Learning



Adversarial Attack and Compromised Nodes

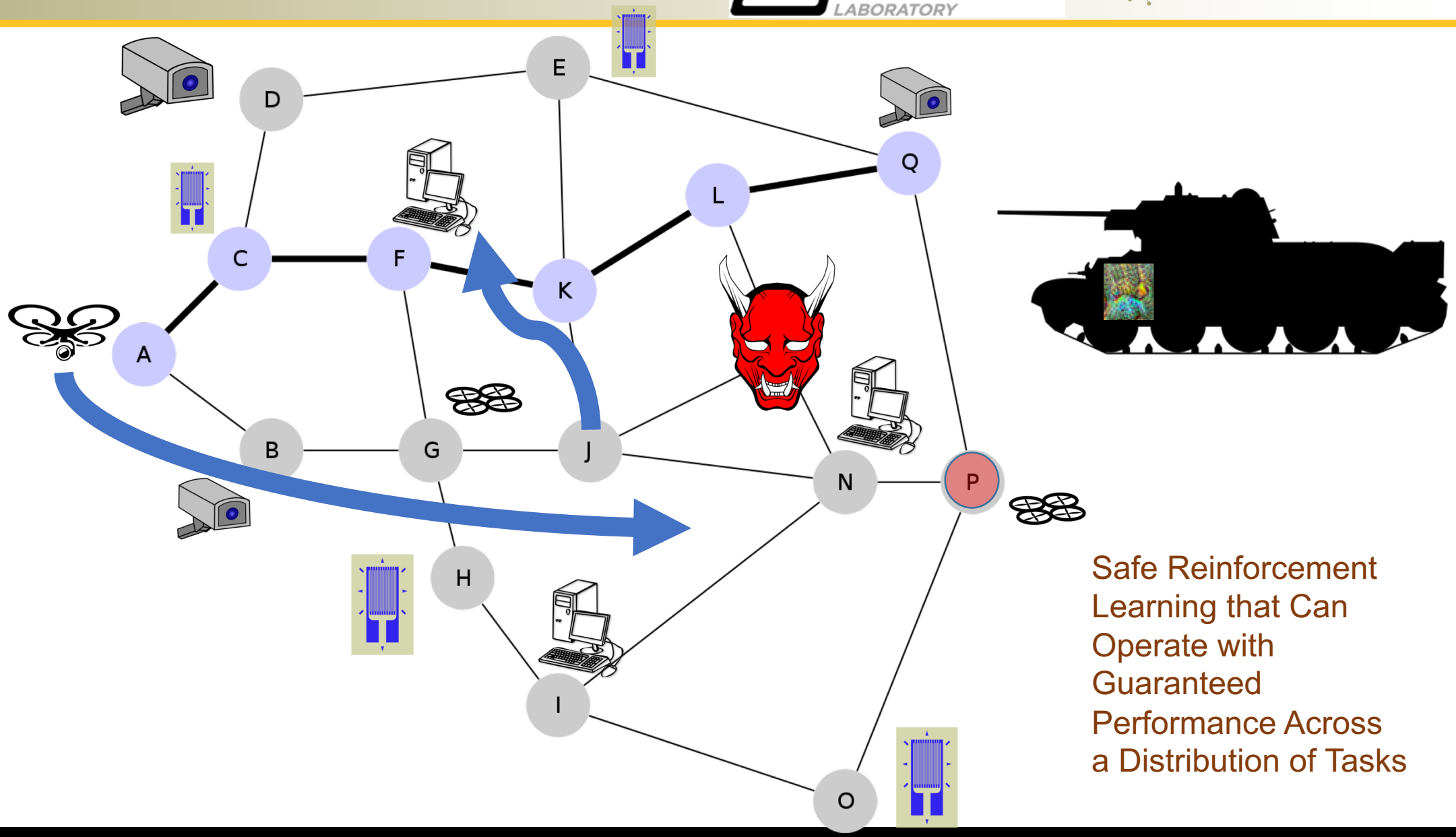


Key Publications:

- Mao, Yanwen. Mitra, Aritra. Sundaram, Shreyas. Tabuada, Paulo "When is the Secure State-Reconstruction Problem Hard?" IEEE Conference on Decision and Control, 2019
- Sultangazin, Alimzhan. Tabuada, Paulo. "Towards the use of symmetries to ensure privacy in control over the cloud." IEEE Conference on Decision and Control, 2018

Robust state estimation in presence of compromised IoBT nodes.

Task 2.3: Fast and Adaptive Learning



Safe Reinforcement Learning that Can Operate with Guaranteed Performance Across a Distribution of Tasks

Task 2.3: Fast and Adaptive Learning

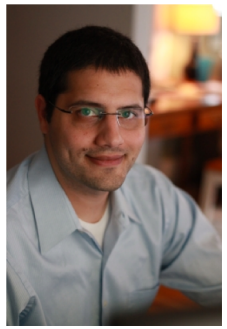
- Reinforcement Learning (RL) Algorithms that Can Operate with Guaranteed Performance Across a Distribution of Tasks.
  - E.g. Resource Allocation for Tracking multiple vehicles.

- The user defines a minimum safe measure of performance for the RL task and specifies the probability with which the algorithm must achieve this measure of performance.

- **Train on a distribution of tasks, and returns**:
  - a solution that is guaranteed to be safe across all tasks from the same distribution with the specified probability, or
  - if a safe solution cannot be found with the specified probability, the algorithm returns “NO SOLUTION FOUND”.

- **Robust to new distribution (bounded from training)**: By modifying the types of bounds we use, we can guarantee performance even when the target task does not come from the training distribution (assuming other assumptions are met, and that sufficient data exists).

Task 2.3: Fast and Adaptive Learning

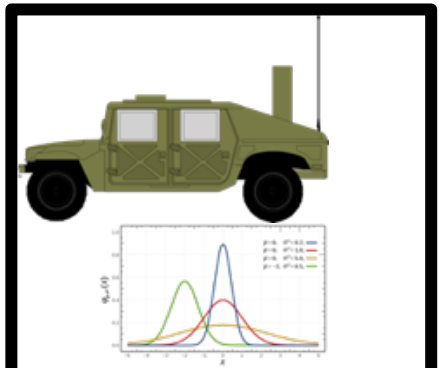


Safe Reinforcement Learning that Can Operate with Guaranteed Performance Across a Distribution of Tasks

Key Publications:

- Giguere, Stephen. Jha, Susmit. Thomas, Phil . Safe and Robust Machine Learning. ICML 2020 **Under Submission**

Military Impact

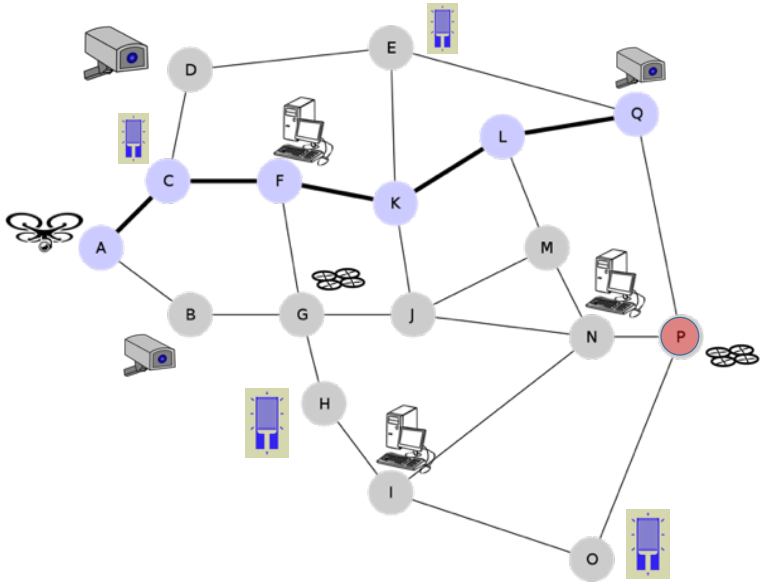


Model-based change detection

Adversarial Attack

Safe Reinforcement Learning that Can Operate with Guaranteed Performance Across a Distribution of Tasks

Robust state estimation in presence of compromised IoBT nodes.



Enable Assured Adaptive IoBT network in a contested and congested environment for Network C3I.
Enable Rapid Change Detection in U.S. Army C3I Systems and Networks
Enable Adversarial Attack Detection for AI/ML in U.S. Army Network C3I Sytem and Network
Enable Command by intent through autonomic reflex capability.

Academic Impact

- **Publications:**
  - **30 peer-reviewed publications** including prestigious venues such as AAAI, NeurIPS, ICLR, ICRA, ACC, HSCC, DAC and MILCOM : 27 Conference/Symposium papers + 3 Journal papers
  - Each thrust has multiple PIs working collaboratively
- Services, Awards and Books

Veeravalli, UIUC

- Book: P. Moulin and V.V. Veeravalli. Statistical Inference for Engineers and Data Scientists. Cambridge University Press, 2019.
- Book: V.V. Veeravalli and A. ElGamal. Interference Management inWireless Networks: Fundamental Bounds and the Role of Cooperation. Cambridge University Press, 2018
- Technical Program Committee Co-Chair, IEEE International Symposium on Information Theory, Paris, France, 2019.
- Area Editor for IEEE Open Journal of Signal Processing, 2019 - present

Tabuada, UCLA

- Guest editor for the special issue of Acta Informatica on Synthesis, 2020.
- Steering committee member for CPS-IoTWeek
- Chair of steering committee for the International Conference on Hybrid Systems: Computation and Control
- General co-chair for the 10th ACM/IEEE International Conference on Cyber-Physical Systems, 2019
- Program committee co-chair for the 9th ACM/IEEE International Conference on Cyber-Physical Systems, 2019.
- Chair of the IEEE Transactions on Control of Network Systems Outstanding Paper Award Committee.
- Vice-chair of the IFAC technical committee on networked systems.
- Visits/rotations to/from or with ARL and duration:
  3 day visit to ARL in Adelphi, September 2019.

Jha, SRI

- 10 year Most-influential Paper Award at 42nd International Conference on Software Engineering (ICSE)
- Program co-chair for 12th NASA Symposium on Formal Methods
- Best Demo Award at HSCC 2019 for Neural Network Verification Tool Sherlock
- Visits/rotations: Visit from Brian Jalain, ARL for one week at SRI, Menlo Park in February