# Cognitive Cyber-Physical Systems: Vision and Ideas for Exploring a New Frontier

## 7th Indian Control Conference

Pramod P. Khargonekar

Department of Electrical Engineering and Computer Science
University of California, Irvine

21 December 2021

# Outline

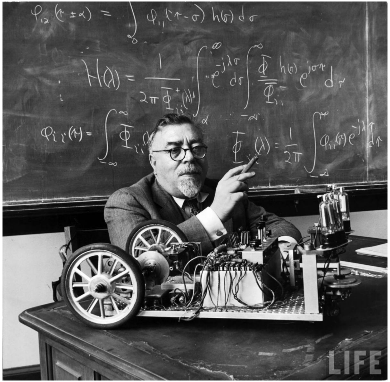
1. Context and Vision
2. Cognitive Cyber-Physical Systems
3. Technical Directions
4. Our Recent Work
5. Concluding Remarks

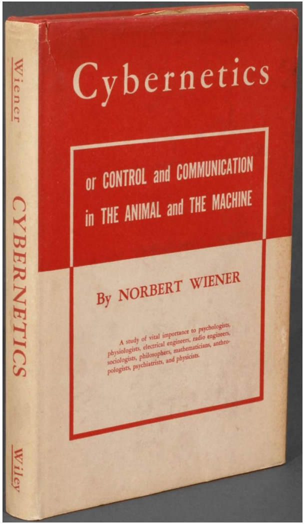
This presentation contains numerous hyperlinks (in blue) as pointers for further study and exploration.

# Dedicated to the Memory of Dr. Kishan Baheti

Thanks to the National Science Foundation for support through
Grant No. ECCS-1839429

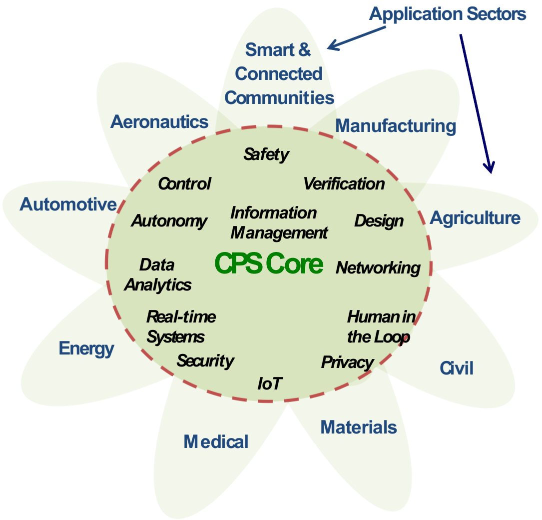
# Wiener, Cybernetics, and Macy Conferences






How would the pioneers of cybernetics and AI envision the future of CPS?

# Cyber-Physical Systems




## Application Domains

### Transportation

- Faster and safer vehicles (airplanes, cars, etc)
- Improved use of airspace and roadways
- Energy efficiency
- Manned and un-manned

### Energy and Industrial Automation

- Homes and offices that are more energy efficient and cheaper to operate
- Distributed micro-generation for the grid

### Healthcare and Biomedical

- Increased use of effective in-home care
- More capable devices for diagnosis
- New internal and external prosthetics

### Critical Infrastructure

- More reliable power grid
- Highways that allow denser traffic with increased safety

Source: NSF

# CPS Properties

- Pervasive computation, sensing, and control
- Networked at multiple scales
- Dynamically reorganizing/reconfiguring
- High degrees of automation
- Dependable operation with potential requirements for high assurance of reliability, safety, security and usability
- With or without human interaction/supervision
- Conventional and unconventional substrates/platforms
- Range from the very small to the large to the very large

Source: NSF

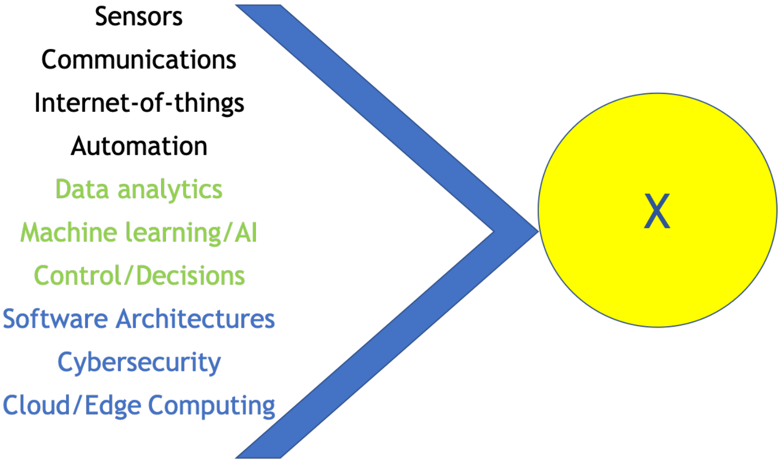
# Aspirational and Emerging Applications

- Smart-X
  1. Smart manufacturing
  2. Smart grid
  3. Smart transportation
  4. Smart cities
  5. Smart health
- Autonomous systems
  1. Unmanned air vehicles
  2. Self-driving cars
  3. Autonomous robots

Human individual and group behavior and their interactions
with technological systems are central in many of these applications:

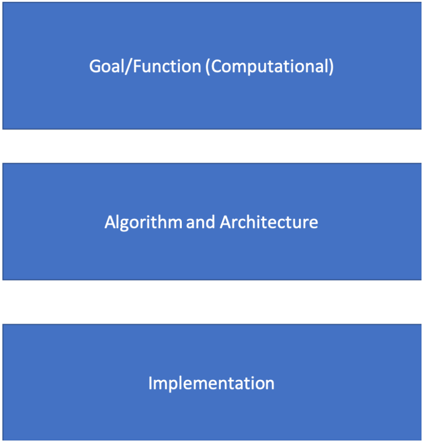
*Smart Cyber-Physical-Human Systems* (CPHS)

# Smart-X: Conceptual View



# Cognitive Cyber-Physical Systems

# Marr's 3 Levels of Analysis and Cognitive Science




Marr's 3 Levels of Analysis and Cognitive Science, Peebles and Cooper (2015)

# Cognition - Definitions and Characteristics

- "All processes by which the sensory input is transformed, reduced, elaborated, stored, recovered, and used." — Neisser, Cognitive Psychology, 1967.
- Important role of evolutionary processes in cognition: genomes, brains, minds, cultures, . . .
- Salient cognitive functions:
  1. Perception
  2. Attention
  3. Memory
  4. Reasoning
  5. Problem solving
  6. Knowledge representation

Cognitive Psychology, Neisser (1967)
Mind as Machine: A History of Cognitive Science, Boden (2006)

# Cognitive CPS - Key Principles

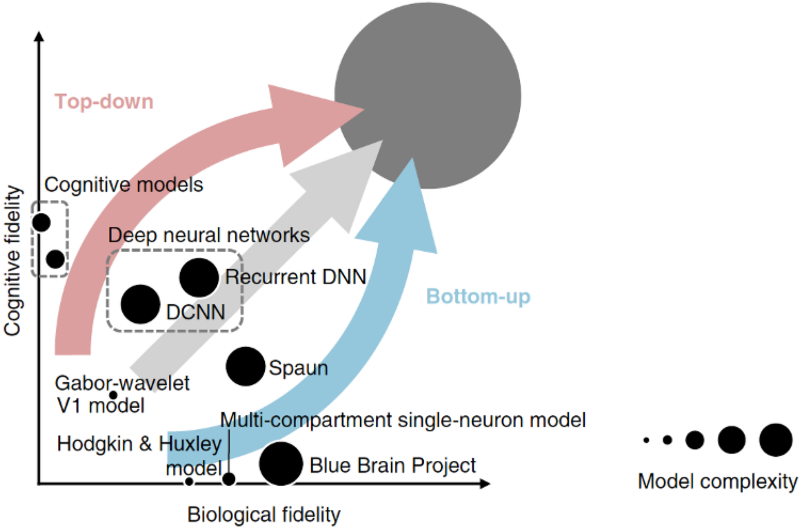
- Working Definition: CPS that have *cognitive functions and capabilities*.
- CPS can be explicitly designed and/or can learn (or evolve) to possess cognitive functions.
- Need for specific cognitive functions and capabilities will depend on the problem.
- Cognitive CPS's may learn from each other, from humans, and also form collaborative networks.
- Cognitive CPS may be better able to augment humans and lead to human flourishing.

**Hypothesis: Cognitive CPS concept offers the most expansive and ambitious program for integrating ML/AI with CPHS for realizing Smart-X Systems.**

# Computational Intelligence: Pattern Recognition or Model Building

- Two fundamentally different perspectives on learning from data:
  - Statistical pattern recognition from data for prediction and control.
  - Use prior knowledge and data to build causal models to understand, predict and control.
- It is possible to combine these two approaches.
- Causality a critical issue in learning from data.

# Cognitive Fidelity, Biological Fidelity, and Model Complexity




Cognitive Computational Neuroscience, Kriegeskorte and Douglas (2018)

# Symbolic vs. Neural Connectionist Approaches

- Historical and ongoing debate on the nature of human cognition and the structure of the brain.
- Key topic in cognitive science: neuroscience, ML/AI, psychology, linguistics.
- Three major components:
  - Computational logic systems
  - Connectionist neural network models
  - Models and tools for uncertainty
- Pragmatic approach: combine connectionist, logic and probabilistic approaches to achieve desired system goals and objectives.

Neural-Symbolic Learning and Reasoning: A Survey and Interpretation, Besold et al. (2017)

# Cognitive Models

- Production systems (Newell and Simon):
  1. If-then rules, logic, symbols
  2. Goals and subgoals, conflict resolution mechanisms
  3. Example: ACT-R, SOAR
- Reinforcement learning based models
  1. Actions, states, rewards
  2. Perception and motor modules
  3. Value and policy based approaches
  4. Three modes: Model-free, model-based, and episodic
  5. Brain combines all three of these modes but it is not known how this is done.
- Bayesian probabilistic models

# Free Energy Principle

- Overarching unifying principle for brain function due to K. Friston.
- Brain seeks to minimize surprise.
- Bayesian brain hypothesis: brain has an internal model that allows for computation of state estimate from sensory observations using Bayes rule.
- Agent chooses action policy to maximize "information gain" (KL divergence or relative entropy).
- Free energy principle: minimize expected free energy under future observations and future states.
- Connections to statistical mechanics, predictive coding, risk sensitive control, ...

The Free-Energy Principle: A Unified Brain Theory?, Friston (2010)

# Perception in ML

- Deep learning is revolutionizing perception.
- Compositionality is built-in.
- Examples of very impressive progress in:
  - Computer vision
  - Speech recognition and processing
  - Language translation
- Architectures:
  - Convolutional neural networks
  - Long Short Term Memory (LSTM) recurrent neural networks
  - Transformers

# Perception in CPS

- CPS with multiple, distributed sources of sensed information.
- Immediately possible to leverage DL advances.
- Prior knowledge plays a very large role in cognitive theories of perception.
- Neural network techniques could be combined with relational prior knowledge for improved context awareness in sensor rich CPS.
- Potential tools and techniques for relational priors:
    1. Neural networks with symbolic front ends.
    2. Inductive biases, deep learning, and graph networks.
    3. Explicitly relational neural networks.

# Computational Models of Attention

- Vision (human, robot, driving) has been a major focus for modeling of attention.
- Feature integration theory, guided search model, CODE theory of visual attention, signal detection theory, . . .
- Computational models:
  1. Itti's model: color, intensity, orientation
  2. Bayesian models of attention
  3. Decision theoretic models
  4. Information theoretic models
  5. Graphical models
  6. Spectrum analysis models

# Attention in ML

- Attention is the key to focusing on the most relevant information from multiple distributed sources of information.
- Examples:
  - Recurrent Models of Visual Attention, Mnih et al. (2014).
  - Effective Approaches to Attention-based Neural Machine Translation, Luong et al. (2015).
  - Show, Attend and Tell: Neural Image Caption Generation with Visual Attention, Xu et al. (2015).
  - Attention is all you need, Vaswani et al (2017).
  - Self-attention Generative Adversarial Networks (GANs), Zhang et al (2019).

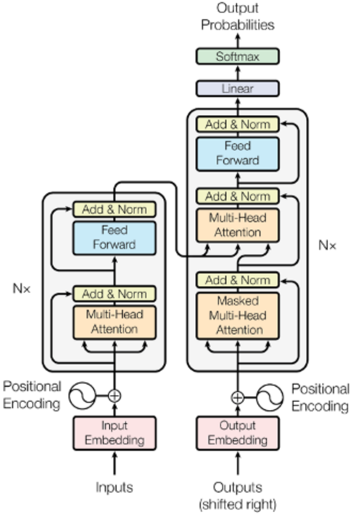



Figure 1: The Transformer - model architecture.

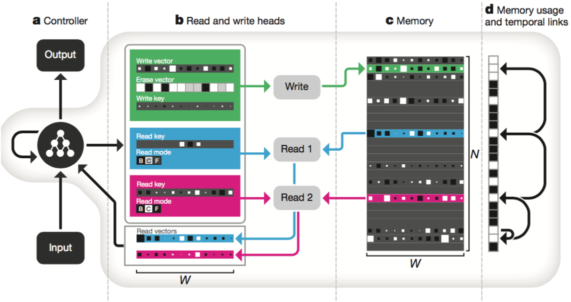
# Role of Attention in CPS

- Two levels of attention:
  - First level - selection and focus on a particular task.
  - Second level - top-down search for relevant information.
- Attention for detecting changing conditions and contexts.
- Attention for fault detection and/or resilience.
- Attention models that are hierarchical and programmable will be required for CPS.
- Examples of programmable attention:
  1. Attention is all you need (Transformer).
  2. Non-local neural networks for image recognition.

# Memory

- Memory is central to learning and intelligent behavior.
- Multiple memory mechanisms in human cognition:
  - short-term
  - long-term
  - episodic (content-addressable)
  - semantic
- LSTM - excellent example of use of memory in machine learning.
- Experience replay - a key innovation in Deep RL breakthroughs.
- Differentiable neural computer by Graves et al. (2016).
- Sparse distributed representations. Examples: hierarchical temporal memory, sparsey.

# Differentiable Neural Computer




Hybrid computing using a neural network with dynamic external memory, Graves et al. (2016)

# Memory, Attention, and Composition Cell Architecture

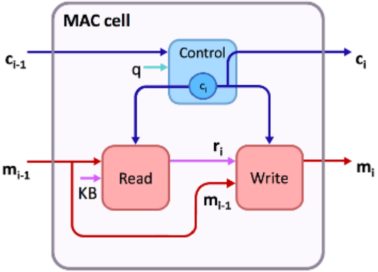



**Figure 3: The MAC cell architecture.** The MAC recurrent cell consists of a control unit, read unit, and write unit, that operate over dual ***control*** and ***memory*** hidden states. The **control unit** successively attends to different parts of the task description (question), updating the control state to represent at each timestep the reasoning operation the cell intends to perform. The **read unit** extracts information out of a knowledge base (here, image), guided by the control state. The **write unit** integrates the retrieved information into the memory state, yielding the new intermediate result that follows from applying the current reasoning operation.

Compositional Attention Networks for machine Reasoning, Hudson and Manning (2018)

# Example of Memory in CPS: Episodic Control

- Episodic control - re-enact successful episodes from memory storage.
- Episodic control has potential relevance to "small data" learning and control.
- Example: Model-free episodic control, Blundell et al. (2016).
- Model-free episodic control – recorded experiences are used as value function estimators.
- Neural episodic control – combining deep learning model and lookup tables of action values.
- Hierarchical episodic control – episodes as options.

# Selected Methodological Challenges

There are numerous major technical challenges:

- Approaches for combining model-based and model-free techniques.
- Approaches to combine hierarchical and distributed architectures and algorithms.
- Reducing the need for large amounts of data: few-shot learning, one-shot learning.
- Bringing meta learning paradigm into cognitive CPS: "learning to learn".

# Combining Model-based and Model-free Approaches

- Model free ML based approaches for sensing, perception, memory and model-based for planning, safety and closing the loop.
- Model predictive control and reinforcement learning – compute action sequence based on the model via MPC (model based), update the model via reinforcement learning and supervised learning.
- Guided policy search – robust local policies are derived from local linear models; these local policies used to efficiently guide a global policy.

# Hierarchical Control

- Hierarchical structures appropriate and necessary for control and management of Smart-X.
- Optimal behavioral hierarchy, Solway et al. (2014).
- Hierarchical control as a natural framework for compositional learning in Smart-X.
- Hierarchical control and learning at multiple scales in time and space. Examples:
  - Options framework in RL/MDP.
  - Feudal RL and hierarchies.
  - MAXQ framework and value function decomposition.

# Our Recent Work

- External memory architectures and algorithms for adaptive control.
- Preadaptation in adaptive control.
- Online learning and optimization:
  - Regret guarantees for online learning for control.
  - Online disturbance gain minimization.
- Reinforcement learning for matching markets with applications to smart grids.
- Online meta learning.
- Smart-X applications:
  - Anomaly detection in smart grids and manufacturing
  - Graph network techniques for decision making in autonomous vehicles.
- Empathetic AI using Generative Adversarial Imitation Learning.

# Cognition: Memory and Preadaptation

- External memory architectures and algorithms for adaptive control
  - External memory augmented to neural network.
  - Short term memory with quick update feature.
  - Performance: significant improvement in adaptation.
  - Theoretical guarantees for signal estimation problem.
  - Attention models in neural adaptive control.
- Preadaptation in adaptive control
  - Preadaptive function block to initialize adaptation algorithm.
  - Online learning algorithm for preadaptation function.
  - Peak reduction upto 50%.

# Online Learning and Optimization

- Regret guarantees for online learning for control.
  - First sub-linear dynamic regret guarantee with limited preview.
- Online disturbance gain minimization.
  - Extension of $\mathcal{H}_\infty$ problem to the online learning setting.
  - Novel characterization and guarantees for disturbance gain with limited preview of future costs and disturbances.
- Adaptive gradient online control.
- Online matching algorithms with applications to smart grids
  - Customers with dynamic willingness to pay.
  - Key idea: online matching by criticality (rate of decrease of willingness to pay) of currently active customers.
  - Novel competitive ratio guarantees in terms of uncertainty in the market.
- Online algorithms for network robustness.

# RL for Matching Markets with Applications to Smart Grids

- Online matching heuristics could be sub-optimal.
- Reinforcement learning can learn optimal online policies.
- Challenges:
  - Large action space of matching markets.
  - Learning to match is a constraint learning problem.
  - Reinforcement learning can converge to sub-optimal solutions.
- Our work: a scalable reinforcement learning algorithm for the matching problem in smart grids.
- We are working on extending this work to large power networks.

# Data-Driven Methods for Smart-X

- Anomaly detection in smart grids and manufacturing.
  - Architectures based on Sparse Representations (Hierarchical Temporal Memory).
  - Demonstrably learns very efficiently, just in one-pass.
  - Key observation: performance better or comparable to LSTMs trained with multiple passes.
- Graph learning techniques in AV decision making:
  - Problem studied: prediction of vehicle collision.
  - Architecture: perception $\rightarrow$ relation graphs $\rightarrow$ graph processing $\rightarrow$ LSTM $\rightarrow$ spatio-temporal embedding $\rightarrow$ prediction.
  - Improved accuracy compared to CNN architecture. Improved efficiency of learning. Implementable on AV hardware.
  - Ongoing work: fast and safe planning using SOS programming.
- Cognitive manufacturing and graph learning

# Meta Learning Paradigm

- Meta learning as a paradigm for dealing with new environments by "learning to learn efficiently and effectively".
- Meta learning idea has been explored in ML since the mid 80's.
- Meta learning in nature and humans
- Two possible approaches
  - First approach: learn the common structures across the tasks to induce a strong prior or "inductive bias" — Bayesian inference
  - Second approach: two-level optimization framework:
    - Inner optimization optimizes the task at hand.
    - Outer optimization optimizes the parameters of the inner optimization.
- Our work: meta-learning algorithm for a control setting.

# Problem Setting: Online Meta Learning

- $N$ episodes of length $T$.
- The environment draws an arbitrary $\theta = [A, B] \in \Theta$ in each episode.
- System dynamics within each episode:

$$x_{t+1} = Ax_t + Bu_t,\ y_t = x_t + \epsilon_t,\ \epsilon_t \text{ is noise.}$$

- Cost function at $t$: $c_t(x_t, u_t)$. Cost function for the future may not be known.
- Information at $t$:
  - $(c_k)_{k\in[t:t+M-1]}$ (limited preview $M$ of future cost).
  - $(y_k)_{k\leq t}, (u_k)_{k\leq t-1}$

# Dynamic Regret

- Dynamic Regret in Episode $i$

$$R_T^i = \left[\mathcal{C}^i(\mathcal{H}) - \mathcal{C}^{i,*}\right], \text{ where } \mathcal{C}^i(\mathcal{H}) = \sum_{j=1}^{T} [c_j(x_j^i, u_j^i)],$$

$\mathcal{C}^{i,*}$ optimal cost with complete information.

- Average regret across $N$ episodes:

$$\overline{R} = \frac{1}{N} \sum_{i=1}^{N} R_T^i$$

# Architecture: Two-Level Learning

subscript $t$: time index within an episode

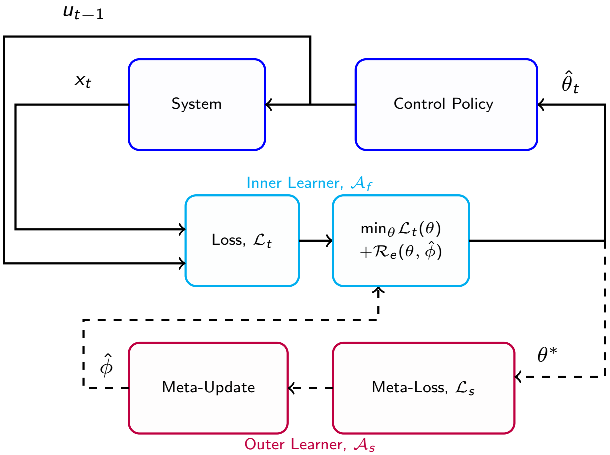



Figure: Online Meta-learning Control Architecture

# Inner Learner $\mathcal{A}_s$

- Loss $\mathcal{L}_t$:

$$\mathcal{L}_t(\hat{\theta}) = \sum_{j=1}^{t} \ell_{\hat{\theta},j},\ \ \ell_{\hat{\theta},j} = \left\| y_{j+1} - \hat{\theta}[y_j^\top, u_j^\top]^\top \right\|_2^2 .$$

- Least-squares estimate:

$$\hat{\theta}_t = \arg\min_{\hat{\theta}} \mathcal{L}_t(\hat{\theta}) + \mathcal{R}_e(\hat{\theta}, \hat{\phi}),$$
$$\mathcal{R}_e(\hat{\theta}, \hat{\phi}) = \lambda \left\| \hat{\theta} - \hat{\phi} \right\|_F^2 \text{(Biased Regularizer)}$$

- $\hat{\phi}$ is the bias given by the outer-learner.

# Outer Learner $\mathcal{A}_f$

- Task is indexed by $i$.
- $\hat{\theta}^{*,i}$ = best inner learner estimate in episode $i$.
- Loss per episode:

$$\ell_i^o(\hat{\phi}) = \left\|\hat{\theta}^{*,i} - \hat{\phi}\right\|_F$$

- Outer learner update:

$$\psi_{i+1} = \hat{\phi}_i - \eta_i \nabla \ell_i^o(\hat{\phi}_i),$$

$$\hat{\phi}_{i+1} = \mathrm{Proj}_{\Theta}(\psi_{i+1}), \ \eta_i = \frac{1}{\sqrt{i}}$$

# Control Policy: $RHC(t, \hat{\theta}_t, \hat{x}_t)$

- Input: Preview $M$, $(c_k)_{k\in[t:t+M-1]}$, Output: $\hat{u}_t$
- $RHC(t, \hat{\theta}_t, \hat{x}_t)$: (Optimizes the cost-to-go for the estimated dynamics.)
  1. $(a_k)^*_{k\in[0:M-1]} = \arg\min_{(a_k)_{k\in[0:M-1]}} \sum_{k=0}^{M-1} c_{k+t}(s_k, a_k)$

     s.t. $s_{k+1} = \hat{A}s_k + \hat{B}a_k,\ \hat{\theta}_t = [\hat{A}, \hat{B}],\ a_k \in \mathcal{U},\ s_0 = \hat{x}$
  2. $\hat{u}_t = a_0^*$ (Current input equals the first value in the optimal sequence.)

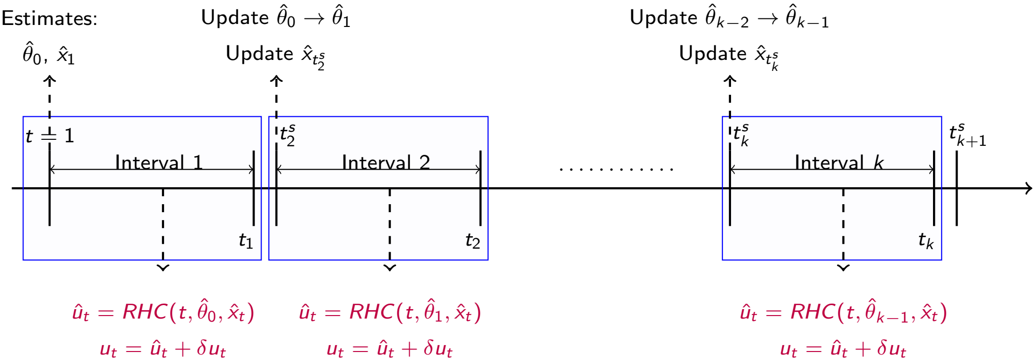
# Balancing Exploration and Exploitation

- Perturbation $\delta u_t$ is applied so that

$$\sum_{j=1}^{t_k} \begin{bmatrix} x_j \\ u_j \end{bmatrix} \left[ x_j^\top, u_j^\top \right] = O(\sqrt{t_k}) \text{ (persistent excitation)}$$

(The specific rate of growth balances exploration and exploitation!)

# Progression within an Episode




Interval Length $=$ Preview Length

# Main Result

- Under suitable technical conditions, for $\delta$ arbitrarily small, with probability greater than $1 - \mathcal{O}(\delta)$

$$\overline{R} = \left(a^{\star} + \mathcal{O}\left(\frac{1}{\sqrt{N}}\right)\right)\tilde{\mathcal{O}}\left(T^{3/4}\right), \; a^{\star} \text{ is a constant.}$$

# Contributions

- Dynamic regret guarantee with limited preview.
- Novel approach to balance exploration and exploitation in online RHC.
- First regret guarantee for online learning RHC.
- First online guarantee for meta-learning in a control setting.

# Publications for More Details I


1. D. Muthirayan and P. P. Khargonekar, "Working Memory Augmentation for Improved Learning in Neural Adaptive Control," IEEE Conference on Decision and Control, pp. 6785-6792, 2019.
2. D. Muthirayan, and P. P. Khargonekar, "Memory Augmented Neural Network Adaptive Controllers: Performance and Stability", arXiv preprint arXiv:1905.02832, 2019.
3. D. Muthirayan, S. Nivison and P. P. Khargonekar, "Improved Attention Models for Memory Augmented Neural Network Adaptive Controllers," arXiv preprint arXiv:1910.01189, 2019, Proceedings of American Control Conference, pp. 639-646, 2020.
4. D. Muthirayan, and P.P. Khargonekar, "Cognitive Preadaptation for Resilient Adaptive Control", In AIAA Scitech 2021 Forum (p. 0786), 2021.
5. D. Muthirayan, J. Yuan, D. Kalathil, and P.P. Khargonekar, "Online Learning for Receding Horizon Control with Provable Regret Guarantees", arXiv preprint arXiv:2111.15041, 2021.
6. D. Muthirayan, D. Kalathil, and P.P. Khargonekar, "Online Robust Control of Linear Dynamical Systems with Prediction", arXiv preprint arXiv:2111.15063, 2021.
7. D. Muthirayan, and P. P. Khargonekar, "Meta-Learning Guarantees for Online Receding Horizon Learning Control," arXiv preprint arXiv:2010.11327, 2021.

# Publications for More Details II


8. D. Muthirayan, J. Yuan, P. P. Khargonekar, "Adaptive Gradient Online Control", arXiv preprint arXiv:2103.08753, 2021.
9. D. Muthirayan, and P.P. Khargonekar, "Online Algorithms for Network Robustness under Connectivity Constraints", arXiv preprint arXiv:2106.04037, 2021.
10. D. Muthirayan, M. Parvania, P. P. Khargonekar, "Online Algorithms for Dynamic Matching Markets in Power Distribution Systems," IEEE Control Systems Letters, pp. 995-1000, 2020.
11. M. Majidi*, D. Muthirayan*, M. Parvania, P. P. Khargonekar, "Dynamic Matching Markets in Power Grid: Concepts and Solution using Deep Reinforcement Learning", arXiv preprint arXiv:2104.05654, 2021.
12. A. Barua, D. Muthirayan, P. P. Khargonekar, M. A. Al. Faruque, "Hierarchical Temporal Memory based One-pass Learning for Real-Time Anomaly Detection and Simultaneous Data Prediction in Smart Grids", IEEE Transactions on Dependable and Secure Computing, 2020
13. A. V. Malawade, N. D. Costa, D. Muthirayan, P. P. Khargonekar, M. A. Al. Faruque, "Neuroscience-inspired algorithms for the predictive maintenance of manufacturing systems", IEEE Transactions on Industrial Informatics, 2021, early access.

# Publications for More Details III


14. S. Y. Yu, A. V. Malawade, D. Muthirayan, P. P. Khargonekar, M. A. Al. Faruque, "Scene-graph augmented data-driven risk assessment of autonomous vehicle decisions", IEEE Transactions on Intelligent Transportation Systems, 2021, early access.
15. A.V. Malawade, S.Y. Yu, B. Hsu, D. Muthirayan, P.P. Khargonekar, and M.A.A. Faruque, "Spatio-Temporal Scene-Graph Embedding for Autonomous Vehicle Collision Prediction", arXiv preprint arXiv:2111.06123, 2021.
16. M.A. Al Faruque, D. Muthirayan, S.Y. Yu, and P.P. Khargonekar, "Cognitive Digital Twin for Manufacturing Systems", In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 440-445), IEEE, 2021, February.
17. T. Mortlock, D. Muthirayan, S.Y. Yu, P.P. Khargonekar, and M.A. Al Faruque, "Graph Learning for Cognitive Digital Twins in Manufacturing System", IEEE Transactions on Emerging Topics in Computing, 2021.
18. P. Muthukumar, K. Muthukumar, D. Muthirayan, and P.P. Khargonekar, "Generative Adversarial Imitation Learning for Empathy-based AI", arXiv preprint arXiv:2105.13328, 2021.

# Concluding Remarks

- Cognitive CPS as a vision for the next frontier in CPS
- Cognitive CPS can provide a framework for integrating ML/AI into CPS
- Architectures and algorithms inspired from computational neuro- and cognitive science have great potential for cognitive CPS
- Cognitive CPS can enable smart-X systems for societal benefits

Thank you!

email: pramod.khargonekar@uci.edu
website: https://faculty.sites.uci.edu/khargonekar/