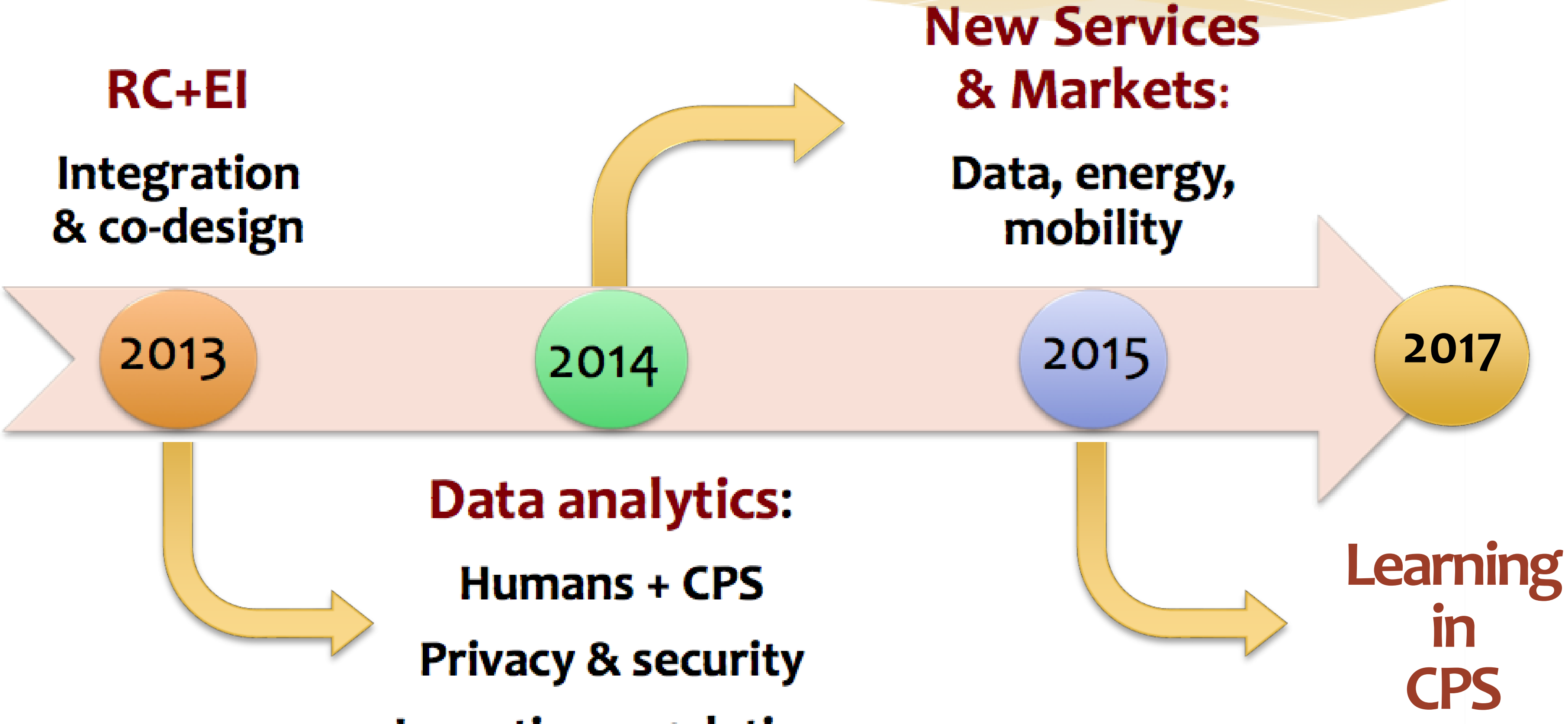
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES
Program Highlights

Larry Rohrbough, UC Berkeley

August 23, 2017

Building Up of the FORCES Agenda



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Recent FORCES Highlights

Research

- Demand Response
  - ML-based inference tools for load forecasting; “counterfactual” estimations; development of incentive schemes
- Electricity Markets Renewable Integration
  - Market-based mechanisms for efficient allocation of power that models consumer heterogeneity and generation costs in electricity markets
- Mechanism Design
  - Dynamic market mechanism for integrating wind energy; more optimal than current forward and real-time mechanisms

Recent FORCES Highlights

Research (cont.)

- Distributed Learning
  - For accelerated/sequential dynamics; applied to transportation, results in improved route choices
- Secure Learning
  - Resilience to adversarial attacks; especially relevant for increasing number of deep learning technologies applied to CPS
- Learning in Traffic Networks
  - Framework to model traffic routing and analysis of changes in information affect traffic equilibrium (congestion, travel time, topologies)
- Learning and Control for Resilience
  - Predictive detection of faulty traffic sensors, alert prioritization modeling in the face of adaptive adversaries, collaborative filtering algorithms to mitigate data poisoning attacks on recommendation systems

Recent FORCES Highlights

Research (cont.)

- Security Assessment & Resource Allocation
  - Security risks and approaches for DER distribution network attacker/defender scenarios (set points/control logic <--> load control/demand shedding) & power grid network control functionality via vulnerability assessment of commercial Energy Management System
- Secure State Estimation
  - New schemes for nonlinear (CPS) systems security; application to autonomous systems in which networked CPS can be attacked via the network
- Resilience in Transportation Systems
  - Data-driven models for air traffic networks and incident-aware control strategies for improved ground transportation [Amin to discuss related research focused on WDNs]

Recent FORCES Highlights

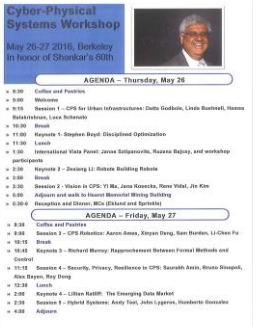
Research (cont.)

- Robust Monitoring, Diagnosis, and Networked Control
  - Game theoretic approach to optimize thresholds of anomaly-based IDS, including the use of time-varying (adaptive) thresholds
- Threat Assessment and Diagnostics
  - Cyber attacks on traffic management system sensor data, modeling incentives in networks with interdependent security
- System-Security Co-Design
  - System-level design and synthesis tools, message authentication for time-triggered architectures and resource-bound systems, synergistic security for WDNs via redundancy, diversity, and hardening, resilient operation and execution of mobile CPS via self-reconfiguration

Recent FORCES Highlights

Outreach

- Workshop on the Future of Cyber-Physical Systems (May 26-27, 2016), UC Berkeley
  - Theme of the workshop was “looking forward,” or exploring the new directions for CPS in the era of big data analytics and machine learning and a focus on CPS in societal scale infrastructures
  - https://www.eventbrite.com/e/workshop-on-the-future-of-cyber-physical-systems-registration-24850665008



Cyber-Physical Systems Workshop

May 26-27 2016, Berkeley
In honor of Shankar's 60th

AGENDA – Thursday, May 26

- 8:30 Coffee and Pastries
- 9:00 Welcome
- 9:15 Session 1 – CPS for Urban Infrastructures: Datta Godbole, Linda Bushnell, Hamsa Balakrishnan, Luca Schenato
- 10:30 Break
- 11:00 Keynote 1- Stephen Boyd: Disciplined Optimization
- 11:30 Lunch
- 1:30 International Vista Panel: Janos Sztipanovits, Ruzena Bajcsy, and workshop participants
- 2:30 Keynote 2 – Zexiang Li: Robots Building Robots
- 3:00 Break
- 3:30 Session 2 - Vision in CPS: Yi Ma, Jana Kosecka, Rene Vidal, Jin Kim
- 5:00 Adjourn and walk to Hearst Memorial Mining Building
- 5:30-9 Reception and Dinner, MCs (Eklund and Sprinkle)

AGENDA – Friday, May 27

- 8:30 Coffee and Pastries
- 9:00 Session 3 – CPS Robotics: Aaron Ames, Xinyan Deng, Sam Burden, Li-Chen Fu
- 10:15 Break
- 10:45 Keynote 3 – Richard Murray: Rapprochement Between Formal Methods and Control
- 11:15 Session 4 – Security, Privacy, Resilience in CPS: Saurabh Amin, Bruno Sinopoli, Alex Bayen, Roy Dong
- 12:30 Lunch
- 2:00 Keynote 4 – Lillian Ratliff: The Emerging Data Market
- 2:30 Session 5 – Hybrid Systems: Andy Teel, John Lygeros, Humberto Gonzalez
- 4:00 Adjourn

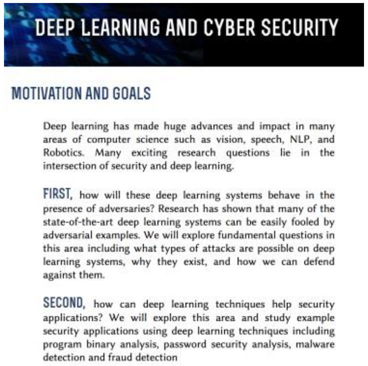
- Workshop on Information, Decisions, and Networks (July 28-29, 2016), Ann Arbor, MI
  - Highlights of FORCES-themed contributions in information theory, mechanism design, energy markets, and cyber-physical security, among other areas
  - http://www.ece.umich.edu/events/demosteneketzis/

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY OF MICHIGAN

Recent FORCES Highlights

Outreach (cont.)

- Deep Learning Security Workshop (Feb. 19, 2017), Singapore
  - Organized in conjunction with 2nd Singapore Cyber Security R&D Conference (SG-CRC 2017)
  - Presented FORCES research on adversarial deep learning, including talks, tutorials, and instructional lab sessions



DEEP LEARNING AND CYBER SECURITY

MOTIVATION AND GOALS

Deep learning has made huge advances and impact in many areas of computer science such as vision, speech, NLP, and Robotics. Many exciting research questions lie in the intersection of security and deep learning.

FIRST, how will these deep learning systems behave in the presence of adversaries? Research has shown that many of the state-of-the-art deep learning systems can be easily fooled by adversarial examples. We will explore fundamental questions in this area including what types of attacks are possible on deep learning systems, why they exist, and how we can defend against them.

SECOND, how can deep learning techniques help security applications? We will explore this area and study example security applications using deep learning techniques including program binary analysis, password security analysis, malware detection and fraud detection

- CPS Week 2017 (April 18-21, 2017), Pittsburgh, PA
  - Amin (HSCC), Balakrishnan (HSCC, ICCPS), Tomlin (HSCC Steering), Koutsoukous (ICCPS Steering)
  - Karsai (talk) at 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG 2017)
  - Laszka (talk) at 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWATER 2017)
  - Ratliff (PC) and Ghafouri (talk) at 2nd International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE 2017)
  - Abbas (talk) at 2nd International Workshop on Social Sensing (SocialSens 2017)

Recent FORCES Highlights
Outreach (cont.)

- Smart Urban Infrastructures Workshop (May 11-12, 2017), MIT
  - Keynote talks and panel discussions from academia, industry, and government
  - Topics included: smart grid and energy services, smart cities/communities, security and privacy in smart services, transportation services and platforms, autonomous transportation, and communications and IoT in smart cities
  - https://lidssmart2017.mit.edu/

Smart Urban Infrastructures Workshop
presented by the Laboratory for Information and Decision Systems at MIT
May 11 + 12, 2017 | MIT

- Games of Asymmetric Information in Networked Environments – Invited Session at ACC 2017 (May 25, 2017), Seattle, WA
  - Focus on recent work using games with asymmetric information applied to areas such as networked control systems, communication networks, and transportation systems
  - https://css.paperplaza.net/conferences/scripts/rtf/2017ACC_ContentListWeb_3.html#thc10

Recent FORCES Highlights

Outreach (cont.)

- Resilience Week 2017
  (Sept. 18-20, 2017), Wilmington, DE
  - Amin and Schwartz on Technical Program Committee of International Symposium on Resilient Control Systems

- CPS-Virtual Organization (VO)
  - Built out program space (migrating public website to VO) for project info, videos, meeting presentations, publications
  - FORCES Newsletters featured on VO homepage: more views and new subscribers as a result

- IEEE Power & Energy Society Task Force on Methods for Analysis and Quantification of Power System Resilience
  - Co-sponsored with IEEE PES Computing and Analytical Methods (CAMS) subcommittee
  - Hiskens task force member addressing how to define resilience and relevant metrics

Recent FORCES Highlights

Education

- Berkeley EE 290-O / IEOR 290: Societal-Scale Cyber-Physical Systems: Machine Learning and the Internet of Things (S. Sastry, R. Dong)
  - New graduate course on theoretical tools for analysis of data and human agents in CPS, including optimization, game theory, differential privacy, behavioral methods, statistical estimation, information theory, and utility function learning; a focus on resilience, security, privacy, and data markets
- Berkeley EE 16A/B: Designing Information Devices and Systems I/II
  - Updated undergraduate (freshmen) course covering CPS: circuits, systems, and controls
- Michigan EECS 558: Stochastic Control (D. Teneketzis)
  - New graduate course; term projects include topics on Energy Markets, Cyber Security, and Dynamic Games with Asymmetric Information

Recent FORCES Highlights

Education (cont.)

- Michigan EECS 463: Power System Design and Operation (I. Hiskens)
  - Special topics course with a CPS (power systems) focus and FORCES themes (resilient control)
- MIT Security Games on Infrastructure Networks
  - Educational module offered to MIT Freshmen that simulates failures scenarios of transportation and energy networks and the effects of various strategies (all via an online tool at http://resilserv.mit.edu/game/)
- Vanderbilt Master of Engineering (MEng) in CPS
  - Teaches foundations of CPS, engineering principals and application areas + management and leadership + capstone project
  - https://engineering.vanderbilt.edu/academics/m_eng/CPS/index.php
- Berkeley Girls in Engineering 2017
  - One-week camp (4 sessions offered) for middle school girls to introduce STEM and CPS via short talks, hands-on activities, and team projects
- Vanderbilt CPS Summer Camp 2017
  - One-week camp for high school rising Juniors and Seniors to learn about CPS and CPS-related disciplines via tutorials and hands-on experiences

Recent FORCES Highlights

Knowledge Transfer and Partnerships

- Demand Response with OhmConnect (Bay Area demand-response firm)
- UAS Traffic Management with NASA Ames
- Large-scale simulation runs of learning models on NERSC/LBNL supercomputers
- Air Traffic Management – EWR and LGA data via airlines/authorities
- FORCES IAB Member Companies UTRC (aircraft engine performance) and EPRI (distribution network resilience)

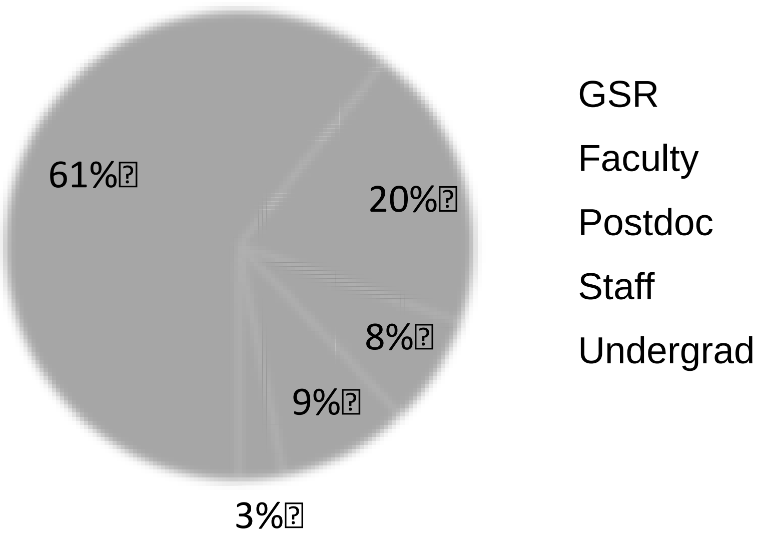
- PCARI – Expanded collaboration on resilient societal-scale CPS (buildings, water, cyber security) and electricity grids
- SMART Future Urban Mobility – Extend FORCES research to traffic transportation systems in Singapore

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The FORCES Team

- Total Participants = 66
  - Graduate Students = 40
  - Faculty = 13
  - Post Docs = 5
  - Staff = 6
  - Undergrad = 2
- Demographics
  - Female = 27%
  - URM = 2%
  - U.S. Persons = 61%

FORCES Personnel (all institutions)



The FORCES Team (cont.)

- New to FORCES this year…
  - Hamzah Abdelaziz, Vanderbilt
  - Kene Akametalu, Berkeley
  - Palak Bhushan, Berkeley
  - Hao Yu (Derek) Chang, MIT
  - Margaret Chapman, Berkeley
  - Dustin Derryberry, Vanderbilt*
  - Elizabeth Diehl, Vanderbilt*
  - Saqib Hasan, Vanderbilt
  - Sylvia Herbert, Berkeley
  - Qie Hu, Berkeley
  - Julien Jacquemot, Berkeley
  - Jonas Kersulis, Michigan
  - Forrest Laine, Berkeley
  - Jiani Li, Vanderbilt
  - Patrick McFarlane, MIT
  - Emily Meigs, MIT
  - Md Salamn Nazir, Michigan
  - Vicenc Royo, Berkeley
  - Tyler Westenbroek, Berkeley
  - Cathy Wu, Berkeley

* Undergraduate Students

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES Work Products

(2016 – 2017)

119 Total Publications (incl. **79** conference/workshop, **33** journal)

Prominent Conferences…

- Control: American Controls Conference (ACC), IEEE Conference on Decision Control (CDC), IEEE Mediterranean Conference on Control and Automation
- Security: ACM Conference on Computer and Communications Security (CCS), ASIACCS, Network and Distributed System Security (NDSS) Symposium, ACM GameSec, ACM HotSoS
- CPS: ACM International Conference on Embedded Systems for Energy-Efficient Building Environments, ICCPS
- Other: Allerton, AAAI Conference on AI, Knowledge Discovery and Data Mining (KDD), Conference on Learning Theory (COLT)

Prominent Journals…

- Automatica
- IEEE Communications Letters
- IEEE Transactions on Automatic Control
- IEEE Transactions on Control of Network Systems
- IEEE Transactions on Control Systems Technology
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Intelligent Transportation Systems
- IEEE Transactions on Network Control Systems
- IEEE Transactions on Network Science and Engineering
- IEEE Transactions on Power Systems
- International Journal of Information Security
- International Journal of Electrical Power and Energy Systems
- Journal of Systems and Software
- Mathematics of Operations Research
- Sensors, Special Issue on Real-Time and Cyber-Physical Systems
- The Energy Journal
- Transportation Science

All Hands Meeting Format

- Research Sessions
  - Medium dives into work & results of FORCES teams
- Keynote Talks
  - Deeper dives into current/emerging themes of FORCES
- Young Researcher Talks
  - Short but interesting introductions to research by grad students and postdocs
  - 15 talks over three sessions (all partner institutions represented)
- Education & Outreach
- Caucus Time & Outbrief from NSF

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS