Lucy Cherkasova, ARM Research

The Good, The Bad and The Ugly of AI for IoT and Sensor Networks

April 17, 2019

Dr. Lucy Cherkasova, Principal Research Scientist, ARM Research (IoT Services Group), San Jose, California, USA

- Lucy's research interests include the analysis, design, and performance management of concurrent and distributed systems with the the latest focus on emerging IoT systems and Big Data processing.

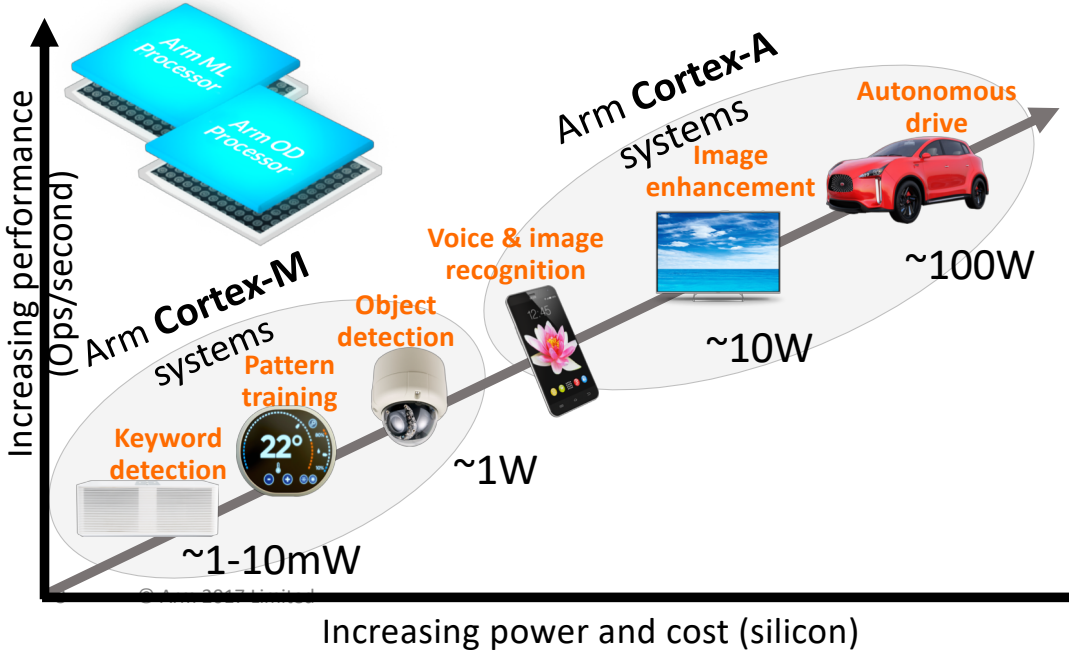
- Before joining Arm, Lucy worked for 20+ years at HP Labs, where she has authored over 100 referred publications and 78 patents.

- Over the years she has mentored and co-advised more than 20 PhD students/interns.

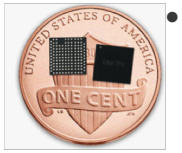
- She is an ACM Distinguished Scientist and recognized by multiple Certificates of Appreciation from the IEEE Computer Society.

AI/the Good

- Today, over 95% of AI-enabled devices are in mobile, smart home and IoT (90% are based in ARM arch)
- Could there be a trillion connected things/sensors? 150 billion embedded processors, 20% growth….
- How do we get useful insights from data and automate these findings?
- Smart environments, personal assistants, self-driving cars – require an efficient ML/AI processing
- *AI applications are pushing compute to the Edge:* design of new hw and programming frameworks
  - Google: Tensor Processing Unit (TPU) for inference (Cloud)



- ***TinyML*** *(ARM)*: deep learning in ultra-low power systems (Arm Helium™ technology)
  - Improves: *ML* (15 times) and *DSP* (5 times)
- ***Edge TPU:*** Google's purpose-built ASIC designed to run AI at the edge



  - ***TensorFlow Light*** *(Google)* for mobile and microcontrollers: 25KB of flash, 30KB of RAM to operate
- ***Federated ML*** *(CMU, Google)*
- ***AutoML:*** selects the best model for the task

arm

AI/the Bad

- **Adversarial Machine Learning & Data Poisoning Attacks**

Suppose that the sign is

Add small adversarial noise…

and the ML in your self-driving car thinks it's

- Black box analysis. Lack of "explainability"...
  - Rich Caruana "Friends Don't Let Friends Deploy Black-Box Models: The Importance of Intelligibility in Machine Learning"
- Ethics, morals, and decision making issues
  - Google announces AI ethics panel (March, 2019) on how to use emerging technologies.
- No security standards… *Mirai Botnets of Things* earned an unfortunate distinction of being on the *Breakthrough Technologies of 2017* according to the MIT Technology Review
  - A flood of cheap webcams, video recorders, and IoT gadgets have little or no security
  - This makes it easier than ever to build huge botnets for DDoS attacks