FAMILY: Foundations and Applications of Machine Intelligence Lab for societY

In this talk, I will present the current problems that we are currently considering at our Lab in Purdue ECE, and the progress we have made towards understanding these problems; hoping to stir participants' interest for future collaborations. The overarching objectives is to study foundations and potential of state of the art machine learning algorithms, with the current focus on deep learning algorithms due to their impressive successes in practice. On the foundations side, we will discuss recent advances on the information bottleneck problem, their impact on understanding the optimization of deep learning algorithms, and introduce our preliminary results that unveil the potential of this theoretical formulation. We will then discuss the adversarial deep learning problem, and present recent work and an envisioned framework for detecting and combatting input-perturbation-based attacks. On the applications side, we will first discuss a hierarchical vision for employing deep learning in collaborative wireless networks. The lowest level of the hierarchy consists of source identification tasks that facilitate identifying transmission origins for a given received signal. Given accurate source identification, analyzing and predicting peer behavior becomes feasible. Finally, spectrum/context understanding tasks like scenario classification and recognizing the behavior of peer networks can take place by building on lower-level capabilities. Our discussion is aided by concrete preliminary results, datasets, and lessons learned from Purdue's participation in the DARPA Spectrum Collaboration Challenge (SC2). I will then present a novel architecture for wireless network intrusion detection. The architecture relies on both supervised (signature-based) and unsupervised (anomaly detecting) machine learning components, along with a rule-based brain that makes decisions and provides lifelong learning updates. Further, features are extracted from the physical and network layers, along with semantics provided by the aforementioned hierarchy. One distinctive property of the proposed architecture is the reliance on a curiosity-driven honeypot that lures attackers without letting them infiltrate the system. Another is the adjustment of physical layer security protocols when an increase in classification confidence is needed. Finally, we will discuss recent work on deep learning for autonomous racing and the Purdue-West Point participation in the Indy Autonomous Challenge.

Short Bio

Aly El Gamal is an Assistant Professor at the Electrical and Computer Engineering Department of Purdue University. He received his Ph.D. degree in Electrical and Computer Engineering and M.S. degree in Mathematics from the University of Illinois at Urbana-Champaign, in 2014 and 2013, respectively. Prior to that, he received the M.S. degree in Electrical Engineering from Nile University and the B.S. degree in Computer Engineering from Cairo University, in 2009 and 2007, respectively. His research interests include information theory and machine learning.

Dr. El Gamal has received a number of awards, including the Purdue Seed for Success Award, the Purdue CNSIP Area Seminal Paper Award, the Purdue Engineering Outstanding Teaching Award, the DARPA Spectrum Collaboration Challenge (SC2) Contract Award and Preliminary Events 1 and 2 Team Awards, and the Huawei Innovation Research Program (HIRP) OPEN Award. He is currently serving as an associate editor in the area of Machine Learning and AI for Wireless at the IEEE Transactions on Wireless Communications, and as a reviewer for the American Mathematical Society (AMS) Mathematical Reviews.