Adversarial Learning for Recommendation

Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra

Polytechnic University of Bari, Italy
{name.surname}@poliba.it

Abstract. Modern recommender systems (RSs) utilize a variety of machine learning (ML) models to provide users with relevant, personalized suggestions about products in a vast catalog. Notwithstanding the great success of ML models to make recommendations, they are often no-robust to adversarial actors, e.g., competitors, that might act to alter recommendations toward a malicious outcome. While the injection of hand-engineered fake profile, i.e., shilling attacks, [2,1] has been the core of investigation between years 2000 and 2015, the last years have been characterized by the rise of Adversarial Machine Learning (AML) techniques, i.e., ML-based approaches for attacking and defending RSs. In this tutorial, we present an overview of more than 75 publications on AML applications in RSs reviewed in our recent survey [3]. In particular, we introduce a twofold categorization of AML uses in RSs: the one based on the study of adversarial attacks, and defenses, against either the model parameters [5], content data [4], or user-item interactions [6]; the other one related to the use of Generative Adversarial Networks (GAN) to propose novel recommender models [7]. All the material is publicly available at github.com/sisinflab/amlrecsys-tutorial.

Keywords: Adversarial Machine Learning · Recommender Systems

References