Curriculum Vitae

Felice Antonio Merra

October 25, 2019

Personal Data

Current Affiliation
Department of Electrical and Information Engineering (DEI)
Polytechnic University of Bari
via E.Orabona, 4 - 70125 Bari (Italy)

mobile: +39 340 421 3 560
e-mail: felice.merra@poliba.it
Institutional Web Site: http://sisinflab.poliba.it/merra/
Personal Web Site: https://merrafelice.github.io/

Social Accounts:
Twitter: @merrafelice
LinkedIn: Felice Antonio Merra
GitHub: merrafelice

Current Position

Since November 1, 2018 PhD Student at Polytechnic University of Bari Bari.

Brief Description of Scientific Activities

My research activities mainly focus on Artificial Intelligence. My investigation is devoted to novel approaches and application of Machine Learning algorithms, and in particular to Adversarial Machine Learning in Recommender System domains. I am currently working on Security of Recommender Systems and the use of Adversarial Machine Learning to improve the robustness of recommendation algorithms, to identify new possible adversarial attacks and to propose novel adversarial-based for recommender systesm.

1 Education

Master's Degree in Computer Science Engineering. October 2018. Thesis title: *Privacy As A Service: automatic anoymization of microdataset for urban analytic.* In this work, a novel initial to data-quality preservation in Open Data has been proposed. **Final Score**: Full marks with honors.

Bachelor's Degree in Computer Science and Automation Engineering. July 2016. Thesis title: *Information Flow Processing: Complex Event Processing in Healthcare Systems.* Full marks with honors. **Final Score**: Full marks with honors.

2 Research Interests

My research activity starts in 2018 soon after my graduation at Polytechnic University of Bari with the Information Systems Laboratory (SisInfLab) group (`http://sisinflab.poliba.it/`). Currently, I am a first-year PhD Student under the supervision of Professor Tommaso Di Noia, technical manager of the laboratory.

2.1 Description of PhD Dissertation

Nowadays, recommender systems are part of our everyday life and one of the most impactful applications of Machine Learning (ML) in the real world. They mainly estimate users' utility on a catalogue of items, news, health training programs and then recommend those a user might be interested in. This has a serious influence not only on the business of many services and product providers but also on users' actual life. Unfortunately, we are well aware that ML systems are vulnerable to adversaries able to invalid the predicted output of a recommendation model. For instance, the top music-services provider Spotify has been recently hacked by adversaries in recommending tracks of non-existent bands. Driven by theoretical and industrial use cases, Adversarial Machine Learning then emerged as a sub-field of machine learning devoted to the study of the vulnerabilities of ML models.

In my first year of Ph.D., I focused on the robustness of recommendation models. Robustness refers here to the consistency of the produced recommendations concerning the expected ones. Low robustness implies that the recommendation system can be maliciously altered with huge risks for the customers, the business of companies, and all the actors of a multi-stakeholder scenario.

I plan to explore different attacks, with a deep focus on the exposure of ML recommender systems to sophisticated ML-based attacks. Indeed, the core of my research is the study and evaluation of ML-based adversarial attacks to recommender systems and the study of the effectiveness and limitations of attackers in different scenarios. The assessment of the analyzed algorithms under adversarial settings is the foundation from which I will address these security shortcomings. To this end, the overarching questions to my research are: "How robust are ML models concerning adversarial attacks?"; "How is it possible to protect recommender systems against malicious adversaries?".

3 Collaboration with national and international research institutes

Within my research activities, I have worked and currently work, with the following international research institute:

- Knowledge Media institute - The Open University (prof. Enrico Motta, dr. A. Antonini), Milton Keynes, United Kingdom

4 International Activities

- WSDM2020, The 13th ACM International Conference on Web Search and Data Mining, WSDM 2020, Houston, USA, February 3-7, 2020, **Presenter** and corresponding author of the tutorial [2].
- SMFC2019, International Workshop on Smart Mobility in Future Cities: The Apulia Industry Summit in conjunction with IEEE International Conference on Systems, Man, and Cybernetics October 6, 2019, Bari, Italy. Poster presentation of *Adversarial Attacks on Mobility Recommender Systems in Smart Cities*.
- RecSys2019, The 13th ACM Recommender Systems Conference, September 16-20, 2019 Copenhagen, Denmark. **Presenter** of Paper [1] at The 1st Workshop on the Impact of Recommender Systems.
- RecSys2019 Summer School, The ACM Summer School on Recommender Systems, September 9-13, 2019 Goteborg, Sweden.
- ESSIR 2019, The 12th European Summer School in Information Retrieval, July 15-19, 2019 Milan, Italy.

5 Tools Experience

Within my research activities, I currently work with different frameworks for the implementation and evaluations of research activities. Particularly, I have strong experience in *Python* programming, with a daily use of $TensorFlow$. I have also worked on projects with other program languages such as $C++$, $C\#$, *Java* and *JavaScript*. I consider my coding skills really important for my research path and career.

6 Publications

[1] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Assessing the impact of a user-item collaborative attack on class of users. In *Proceedings of the 1st Workshop on the Impact of Recommender Systems co-located with 13th ACM Conference on Recommender Systems, ImpactRS@RecSys 2019), Copenhagen, Denmark, September 19, 2019.*, 2019.

[2] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial machine learning in recommender systems. *ACM International Conference on Web Search and Data Mining, WSDM 2020, Houston, USA, February 3-7, 2020*, 2020.

Bari, October 25, 2019

Felice Antonio Merra