Curriculum Vitae

Felice Antonio Merra

July 12, 2020

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 approaches for recommender systems.

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*. **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 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.

I am focusing 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 Research Institutes

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

- Escuela Politécnica Superior, Universidad Autónoma de Madrid (dr. Alejandro Bellogín), Madrid, Spain
- Knowledge Media institute - The Open University (prof. Enrico Motta, dr. A. Antonini), Milton Keynes, United Kingdom

4 International Internship

- **Machine Learning Scientist Intern - Amazon.com**. I will start a 3-months internship in Summer 2020 in Amazon.com as a Machine Learning Scientist Intern in the *Amazon Search* research team.

5 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 [**?**].
- 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 [**?**] 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.

6 Teaching Activities

- **Data Structure and Algorithm in Java.** I started my teaching activity in the academic year 2019/20 as Course Assistant for the bachelor degree course: *Data Structure and Algorithm in Java*.

7 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.

8 Publications

[1] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial learning for recommendation: Applications for security and generative tasks - concept to code. In *The 14th ACM Conference on Recommender Systems*. ACM Digital Library, 2020.

[2] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Felice Antonio Merra, Giuseppe Acciani, and Eugenio Di Sciascio. Knowledge-enhanced shilling attacks for recommendation. In *The 28th Italian Symposium on Advanced Database Systems (SEBD 2020), Villasimius (CA), Italy, June 21-24, 2020*. CEUR Workshop Proceedings, 2020. to Appear in SEBD2020.

[3] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. Sasha: Semantic-aware shilling attacks on recommender systems exploiting knowledge graphs. In *The Semantic Web - 17th International Conference, ESWC 2020, Heraklion, Crete, Greece, May 31-June 4, 2020, Proceedings*, pages 307–323, 2020.

[4] Yashar Deldjoo, Tommaso Di Noia, Felice Antonio Merra, and Eugenio Di Sciascio. How dataset characteristics affect the robustness of collaborative recommendation models. In *Proc. of ACM SIGIR 2020 - 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*. ACM Press, 2020. to appear.

[5] 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.

[6] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial machine learning in recommender systems (aml-recsys). In *WSDM '20: The Thirteenth ACM International Conference on Web Search and Data Mining, Houston, TX, USA, February 3-7, 2020*, pages 869–872, 2020.

[7] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial machine learning in recommender systems: State of the art and challenges. *CoRR*, abs/2005.10322, 2020.

[8] Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. Taamr: Targeted adversarial attack against multimedia recommender systems. In *The 3rd International Workshop on Dependable and Secure Machine Learning – DSML 2020 Co-located with the 50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2020)*, 2020. IEEE, IEEE Digital Library, 2020.

Bari, July 12, 2020

Felice Antonio Merra