(334) 332-3617
amin.ghafouri@vanderbilt.edu

Amin Ghafouri

linkedin.com/in/aminghafouri
github.com/aminghafouri

Education

Graduate **Vanderbilt University** **2013 – 2017**

- Ph.D. in Computer Science, October 2017 (expected). GPA: 4.0
- M.Sc. in Computer Science, May 2015. GPA: 3.9
- Dissertation: Anomaly Detection in Data-Driven Cyber-Physical Systems. Advisor: Dr. Xenofon Koutsoukos.
- Related Courses: Intermediate Software Design; Advanced Algorithms; Advanced Artificial Intelligence; Machine Learning; Distributed Systems; Embedded Systems; Operating Systems; Network Security.

Undergraduate **University of Tehran** **2008 – 2013**

- B.Sc. in Electrical Engineering with specialization in Control Systems, May 2013. GPA: 3.85
- Related Courses: Object-Oriented Programming; Statistical Analysis; Computer Architecture; Linear Algebra.

Technical Skills

- **Languages:** C++, Java, Python, C, Matlab, R, JavaScript, SQL
- **Tools:** [Git, SVN, UNIX Shell, Linux, Valgrind, Maven], [Scikit-learn, TensorFlow, Keras, Numpy, Scipy, Pandas], [MongoDB, SQL Server], [Simulink, LabVIEW, OMNet++]

Work Experience

Research Assistant **Institute for Software Integrated Systems** **2013 - present**

- Designed and implemented methods for anomaly detection in time series data using adversarial machine learning, statistical analysis, game theory, and software engineering.
- Developed algorithms for robust operation of complex physical systems; applied to a traffic application.
- Studied the problem of finding adversarial examples in neural networks used for regression (for the first time).
- Co-developed a robust multi-modal route planner for Nashville with 500 active users.
- Designed a dynamic anomaly detector that is resilient in the presence of data poisoning, and reduces losses by up to 15% compared to existing models; applied to a real-world application.

Research Assistant **Systems and Machines Research Laboratory** **2011- 2013**

- Developed performance evaluation methods for smart grid operators, and applied them to the Greater Tehran Electricity Distribution Company (GTEDC); closely collaborating with domain experts.

Intern **Control and Intelligent Processing Center of Excellence** **2012**

- Developed an object-oriented software to assess the performance of the GTEDC using SVMs.

Selected Software Projects

- Implemented an open-source robust route planner class for OpenTripPlanner platform, 2016-2017. Java
- Developed an algorithm for predicting conversion rates using data from eBay, 2017. Python
- Designed a provably-safe method for control of self-driving cars under cyber-attacks, and simulated it using Vanderbilt University's campus as road network, 2014-2015. C++, Matlab, SUMO
- Implemented Bittorrent, Paxos, and client-server communication protocols, 2014. C++, Omnet++

Selected Honors and Awards

- Ranked in the top 3 of Code Golf competition hosted by Google and Vanderbilt University, 2017.
- Passed the computer science PhD qualifying examination at Vanderbilt University, 2017.
- Ranked in the top 3 of Connect-Five coding tournament at Vanderbilt University, 2015.
- Awarded full scholarship by the Graduate School of Vanderbilt University, 2013-present.
- Nominated for Best Thesis Award, Electrical Engineering Department at University of Tehran, 2013.

- Selected among the students of exceptional talents by the Iran's National Organization for Educational Testing.
- Ranked in the top 0.2% and 0.5% in Iranian National Universities Entrance Exam-Undergraduate and -MBA.

Professional Activities

- Recent Talks: FORCES'17 (UC Berkeley), AISOC'17 (Stanford), FORCES'16 (MIT), GameSec'16 (NYU)
- Member of FORCES (collaborative project between Vanderbilt University, UC Berkeley, MIT, and University of Michigan), attending weekly project meetings and presenting reports at semiannual project meetings.
- Member of Vanderbilt Initiative for Smart-Cities Operations and Research (VISOR)
- Reviewer/Program Committee Member: EMSOFT'17, ICAC'16, SSIC'16, ADHS'15
- Teaching Assistant: Digital Logic Design, Microprocessors, Linear Control Systems, Operations Research
- Mentored three PhD students and two undergraduate students at Vanderbilt University.

Publications

1. **A. Ghafouri**, Y. Vorobeychik, X. Koutsoukos, "Adversarial Machine Learning for Regression." *To be submitted to ICCPS 2017*.
2. **A. Ghafouri**, A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "A Game-Theoretic Approach for Selecting Optimal Thresholds for Anomaly Detection in Dynamical Environments." *Elsevier Journal of Information Sciences (Under Review)*, 2017.
3. **A. Ghafouri**, A. Laszka, X. Koutsoukos, "Application-Aware Anomaly Detection in CPS." *Submitted to the Journal of Sensors*, 2017.
4. **A. Ghafouri**, A. Laszka, A. Dubey, and X. Koutsoukos, "Optimal Detection of Faulty Sensors Used in Route Planning." *Second International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE)*, Pittsburgh, PA, 2017.
5. S. Hasan, **A. Ghafouri**, A. Dubey, G. Karsai, and X. Koutsoukos, "Vulnerability Analysis Based on Cyber-Attack and Defense Models in Power Transmission Systems." *Submitted to ISGT 2018*.
6. S. Hasan, **A. Ghafouri**, A. Dubey, G. Karsai, and X. Koutsoukos, "Heuristics-Based Approach for Identifying Critical $N-k$ Contingencies in Power Systems." *10th International Symposium on Resilient Control Systems*, Wilmington, DE, 2017.
7. **A. Ghafouri**, A. Laszka, A. Dubey, and X. Koutsoukos, "Optimal Detection of Faulty Traffic Sensors." *AAAI 2017 Spring Symposium on AI for Social Good (AISOC)*, Stanford University, March 27-29, 2017.
8. **A. Ghafouri**, W. Abbas, A. Laszka, Y. Vorobeychik, and X. Koutsoukos, "Optimal Thresholds for Anomaly-Based Intrusion Detection in Dynamical Environments." *2016 Conference on Decision and Game Theory for Security (GameSec 2016)*, New York, NY, November 2-4, 2016.
9. **A. Ghafouri**, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Vulnerability of Fixed-Time Control of Signalized Intersections to Cyber-Tampering." *9th International Symposium on Resilient Control Systems*, Chicago, IL, Aug. 16-18, 2016.
10. **A. Ghafouri** and X. Koutsoukos, "Resilient Supervisory Control of Autonomous Intersections in the Presence of Sensor Attacks." 2016.
11. **A. Ghafouri**, A. Fereidunian, H. Lesani, H. Torabi, and P. Kharazmi. "Performance Evaluation for DNO Governance Using Data Envelopment Analysis Method." *2nd Iranian Conference on Smart Grids (ICSG 2012)*, pp. 1-5. IEEE, 2012.