Alesia Chernikova

chernikova.a@husky.neu.edu

1 Oak Grove Avenue, apt.217
Melrose, MA 02176
(857) 413-1191

Research Interests

Adversarial machine learning, applications of machine learning in self-driving cars, Bayesian methods for probabilistic modeling and inference.

Education

Doctor of Philosophy — Fall 2017 - Present
Computer Science
Northeastern University, Boston, MA
GPA: 3.71
Advisor: Dr. Alina Oprea

Bachelor of Science — Fall 2009 - Spring 2014
Applied Mathematics and Computer Science
Belarusian State University, Minsk, Belarus
GPA: 3.8
Advisor: Dr. Vladimir Malugin
Thesis: "Development of risk management algorithms based on derivatives contracts"

Professional Experience

Research Assistant — Fall 2017 - Present
Network and Distributed Systems Security Lab
Northeastern University, Boston, MA
Conducting research on:

- evasion attacks against Deep Neural Networks in cybersecurity and self-driving cars domains;
- detecting malicious behaviour through network data analysis.

Software Engineer — November 2013 - July 2017
IBA IT Park, Minsk, Belarus

- Participated as lead developer in the development and improvement of IBM GSAR web portal.

Research Assistant — January 2012 - December 2013
Belarusian State University, Minsk, Belarus

- Participated in the research project for estimation and evaluation of credit rankings of national enterprises using mathematical, statistical, econometric methods and models based on the data from National Bank of the Republic of Belarus enterprise monitoring systems.

Research Projects

Adversarial Examples for Deep Learning Cyber Security Analytics
Advisor: Dr. Alina Oprea

- Trained machine learning model for classification of aggregated network traffic into malicious and benign.
- Proposed new type of evasion attack against Feed-Forward Neural Nerwork for network traffic classification.

Evasion Attacks against Deep Neural Networks for Self-Driving Cars
Advisors: Dr. Alina Oprea and Dr. Cristina Nita-Rotaru

- Trained Convolutional Neural Networks for autonomous vechicle direction and steering angle prediction.
- Created adversarial examples for Deep Neural Network that predicts self-driving car direction, proposed new type of evasion attack against steering angle prediction.

Publications

Alesia Chernikova, Alina Oprea, Cristina Nita-Rotaru and Baekgyu Kim. **Are Self-Driving Cars Secure? Evasion Attacks against Deep Neural Networks for Steering Angle Prediction.** IEEE Workshop on the Internet of Safe Things 2019.

Alesia Chernikova and Alina Oprea. **Adversarial Examples for Deep-Learning Cyber Security Analytics.** (Under preparation)

Alesia Strechka. **Algorithms for interest-rate swaps hedging**. In the 70th undergraduate, graduate and postgraduate students scientific conference of Belarusian State University (vol. 1, pp. 242 – 245).

Honors & Awards

National Bank of the Republic of Belarus Merit Scholarship (2014-2015)

BSU Excellence Merit Scholarship (2009-2014)

Relevant Skills

Programming: C/C++, Python, Java, C#, SQL

Tools: Tensorflow, Keras, scikit-learn, PyTorch, Git

Frameworks: Spring, Hibernate, JSP, JSF

Databases: Oracle, MySQL, PostgreSQL, DB2

Operating Systems: Windows, Unix.

Languages: English (Advanced), Russian (Native), German(Intermediate)

Relevant Courses

Advanced Machine Learning(Bayesian methods for probabilistic modeling and inference), Machine Learning, Algorithms and Data Structures, Advanced Algorithms, Data Mining(Unsupervised Learning), Distributed Systems, Networks, C/C++ Programming, Data Models and Databases, Mathematical Analysis I – IV, Geometry and Higher Algebra, Matrix Analysis, Functional Analysis, Numeric Analysis, Discrete Mathematics, Theory of Probabilities and Mathematical Statistics I - III, Differential Equations, Methods of Optimization, Multivariate Statistical Analysis, Mathematical Theory of Forecasting, Computer Data Analyses and Modeling