

Alesia Chernikova

chernikova.a@northeastern.edu

<https://www.linkedin.com/in/alesia-chernikova/>

(781) 350-0139

Research Interests	Adversarial machine learning, deep learning, network science, mathematical modeling, network robustness, cloud security, and threat intelligence.	
Education	<i>Doctor of Philosophy</i>	Fall 2017 - Present
	Computer Science	
	Northeastern University, Boston, MA	
	GPA: 3.9	
	Advisor: Dr. Alina Oprea	
	<i>Bachelor of Science</i>	Fall 2009 - Spring 2014
	Applied Mathematics	
	Belarusian State University, Minsk, Belarus	
	GPA: 3.8	
	Advisor: Dr. Vladimir Malugin	
	Thesis: "Development of risk management algorithms based on derivatives contracts"	
Professional Experience	<i>Research Assistant</i>	Fall 2017 - Present
	NDS2 Lab, Northeastern University, Boston, MA	
	Conducting research on:	
	<ul style="list-style-type: none">• Robustness of deep neural networks in constrained environments and self-driving cars domain.• Detecting malicious behavior through network data analysis.• Modeling the behavior of self-propagating malware in the networks with the help of compartmental models of epidemiology.• Improving network robustness in the face of self-propagating malware by leveraging spectral graph theory.	
	<i>CS4100: Artificial Intelligence Teaching Assistant</i>	Fall 2022, Fall 2023
	Northeastern University, Boston, MA	
	<ul style="list-style-type: none">• Grading exams and homework, holding office hours, assisting Professor in homework and exam preparation, advising students regarding final projects.	
	<i>Applied Scientist Intern</i>	May 2021 - September 2021, May 2020 - August 2020
	Amazon Web Services, Boston, MA	
	<ul style="list-style-type: none">• Conducting research on cloud security as a part of the AWS ESS-Detective team.	
	<i>Software Engineer</i>	November 2013 - July 2017
	IBA IT Park, Minsk, Belarus	
	<ul style="list-style-type: none">• Participated as lead developer in the development and improvement of the IBM GSAR web portal.	
	<i>Research Assistant</i>	January 2012 - December 2013
	Belarusian State University, Minsk, Belarus	
	<ul style="list-style-type: none">• Participated in the research project for the estimation and evaluation of credit rankings of national enterprises using mathematical, statistical, and econometric methods and models based on the data from the National Bank of the Republic of Belarus enterprise monitoring systems.	

Research Projects

Feasible Evasion Attacks on Neural Networks in Constrained Environments

Advisor: Dr. Alina Oprea

- Trained machine learning models for classification of aggregated network traffic into malicious and benign.
- Proposed new type of evasion attack against Feed-Forward Neural Network 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 vehicle direction and steering angle prediction.
- Created adversarial examples for Deep Neural Network that predicts self-driving car direction, proposed a new type of evasion attack against steering angle prediction.

Cyber Network Resilience against Self-Propagating Malware Attacks

Advisors: Dr. Alina Oprea

- Proposed a new compartmental model SIIDR that captures self-propagating malware (SPM) behavior.
- Reconstructed the spreading dynamics of an actual SPM (WannaCry) using real-world traces obtained by running a vulnerable version of Windows in a virtual environment and deriving the model's transition rates from actual attacks.
- Performed an in-depth evaluation of 10 defense techniques while introducing two novel defenses to increase the robustness of the networks in the face of SPM. The evaluation was performed using large real-world communication graphs from enterprises and estimated transition rates.
- Provided recommendations on the effectiveness and cost of defenses to inform network operators on various proactive preventive options against SPM attacks.

Modeling Self-Propagating Malware with Epidemiological Models

Advisors: Dr. Alina Oprea

- Analyzed a SIIDR model that captures self-propagating malware (SPM) behavior and showed that SIIDR outperforms several classical models in terms of capturing WannaCry behavior.
- Derived the basic reproduction number of the SIIDR model and discussed the stability conditions of the disease-free equilibrium points of the system of ordinary differential equations that represents SIIDR under a homogeneous mixing assumption.
- Derived the conditions for stability of the SIIDR disease-free equilibrium points on arbitrary graphs thus relaxing the homogeneous mixing assumption and experimentally confirmed the results by modeling SIIDR propagation on a variety of graphs with different topological characteristics.

Robustness of Graph Neural Networks in Constrained Environments (in progress)

Advisors: Dr. Alina Oprea

Publications

Alesia Chernikova, Nicolò Gozzi, Simona Boboila, Nicola Perra, Tina Eliassi-Rad, and Alina Oprea. **Modeling Self-Propagating Malware with Epidemiological Models**. [Applied Network Science 2023]

Alesia Chernikova, Nicolò Gozzi, Simona Boboila, Priyanka Angadi, John Loughner, Matthew Wilden, Nicola Perra, Tina Eliassi-Rad, and Alina Oprea. **Cyber Network**

Resilience against Self-Propagating Malware Attacks. [European Symposium on Research in Computer Security (ESORICS) 2022]

Alesia Chernikova and Alina Oprea. **Fence: Feasible evasion attacks on neural networks in constrained environments.** [ACM Transactions on Security and Privacy 2022]

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 Vladimir Malugin. **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**

Khoury College of Computer Science Fellowship (2017-2018)
National Bank of the Republic of Belarus Merit Scholarship (2014-2015)
BSU Excellence Merit Scholarship (2009-2014)

**Relevant
Skills**

Programming Languages: Python, Java, Scala, Javascript, C/C++
Frameworks and Libraries: PyTorch, Tensorflow, Keras, Spark

**Relevant
Courses**

Advanced Machine Learning (Bayesian methods for probabilistic modeling and inference), Data Visualization, Machine Learning, Advanced Algorithms, Data Mining (Un-supervised Learning), Distributed Systems, Theory of Probabilities and Mathematical Statistics, Methods of Optimization, Multivariate Statistical Analysis, Mathematical Theory of Forecasting, Discrete Mathematics and Graph Theory, Differential Equations, Matrix Analysis, Real and Complex Analysis.