QISHENG ZHANG

4th year Ph.D. student
Department of Computer Science, Virginia Tech, VA, USA
Email: qishengz19@vt.edu
Phone number: +1 202-445-6768
LinkedIn: https://www.linkedin.com/in/qs666
Github: https://github.com/DigitalErage
Homepage: https://DigitalErage.github.io

EXPERIENCE

Computer Science, Virginia Tech - *Graduate Research Assistant*
Falls Church, VA, USA — Aug. 2019 - present

Research Interests: AI-based cybersecurity, decision-making under uncertainty, deep reinforcement learning, cybersecurity for cyber-physical systems, network science

The supported research projects include:

- "Uncertainty-Aware Deep Reinforcement Learning-based Defense for Resilient Cyber-Physical Systems," funded by the US Army Research Office (2021-2024), https://github.com/DigitalErage
- "Energy Centric Wireless Sensor Node System for Smart Farms," funded by the NSF (2021-2025), https://wordpress.cs.vt.edu/nsfsf/
- "MUDL: Multidimensional Uncertainty-Aware Deep Learning Framework," funded by the NSF (2021-2025)

EDUCATION

Virginia Tech, Falls Church, VA, USA — Aug. 2019 - present

Ph.D. in Computer Science
Advisor: Dr. Jin-Hee Cho

Ph.D. Dissertation Title: "Autonomous Active Cyber Defense for Resilient Cyber-Physical Systems"

Expected Graduation: Spring 2023

GPA: 3.8/4.0

University of Warwick, Coventry, United Kingdom — Oct. 2017 - Jul. 2018

M.S. in Mathematics with Distinction
Advisor: Dr. Diane Maclagan

Master Thesis: "Tropical Ideals and Smooth Hypersurfaces," 2018.

GPA: 3.8/4.0

Loughborough University, Loughborough, United Kingdom — Sep. 2016 - Jun. 2017

Exchange Student in Mathematics
Advisor: Dr. Elisa Postinghel
GPA: 87/100 (∼3.3/4)

Shandong University, Jinan, China — Sep. 2013 – Jun. 2016
B.S. in Mathematics and Applied Mathematics
GPA: 88/100 (∼ 3.3/4)
Bachelor Thesis: "Different Ranks of a Tropical Matrix," 2017.

GRADUATE COURSES TAKEN

- Virginia Tech: Introduction to Deep Learning; Network Security; Theory of Algorithms; Data Analytics; Advanced Topics in Game Theoretic Cybersecurity; Spatial Data Management
- University of Warwick: Algebraic Geometry; Representation Theory; Elliptic Curves; Commutative Algebra; Group Theory; Ring Theory

PUBLICATIONS

Journal Papers

1. **Qisheng Zhang**, Abdullah Zubair Mohammed, Zelin Wan, Jin-Hee Cho, and Terrence J. Moore, "Diversity-By-Design for Dependable and Secure Cyber-Physical Systems: A Survey," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, Mar. 2022 (2022 JCR IF 4.758)

2. **Qisheng Zhang**, Jin-Hee Cho, Terrence J. Moore, and Ing-Ray Chen, "Vulnerability-Aware Resilient Networks: Software Diversity-based Network Adaptation," *IEEE Transactions on Network Service and Management*, vol. 18, no. 3, pp. 3154–3169, Sep. 2021. (2020 JCR IF 4.195)

Conference Papers

1. **Qisheng Zhang**, Yash Mahajan, Ing-Ray Chen, Dong Sam Ha, and Jin-Hee Cho, "An Attack-Resilient and Energy-Adaptive Monitoring System for Smart Farms," *IEEE Global Communications Conference*, 2022.

2. **Qisheng Zhang**, Jin-Hee Cho, Terrence J. Moore, and Frederica Free Nelson, "DREVAN: Deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks," *IEEE Conference on Communications and Network Security*, 2021.

3. **Qisheng Zhang**, Jin-Hee Cho, and Terrence J. Moore, "Network resilience under epidemic attacks: Deep reinforcement learning network topology adaptations," *IEEE Global Communications Conference*, 2021.

Workshop Papers

1. **Qisheng Zhang**, Zhen Guo, Audun Jøsang, Lance Kaplan, Feng Chen, Dong Hyun Jeong, Jin-Hee Cho, "PPO-UE: Proximal Policy Optimization via Uncertainty-Aware Exploration," accepted at *1st AAAI Workshop on Uncertainty Reasoning and Quantification in Decision Making*, 2023.

2. Zhen Guo, Qi Zhang, Xinwei An, **Qisheng Zhang**, Audun Jøsang, Lance Kaplan, Feng Chen, Dong Hyun Jeong, Jin-Hee Cho, "Uncertainty-Aware Reward-based Deep Reinforcement Learning for Intent Analysis of Social Media Information," accepted at *1st AAAI Workshop on Uncertainty Reasoning and Quantification in Decision Making*, 2023.

Papers Under Review

1. Zhen Guo, Qi Zhang, **Qisheng Zhang**, Lance Kaplan, Audun Jøsang, Feng Chen, Dongseong Jeong, and Jin-Hee Cho, "`mudRIA`: Multidimensional Uncertainty-Aware Deep Reinforcement Learning-based Intent Analysis of Fake News Spreaders, submitted to *The Pacific-Asia Conference on Knowledge Discovery and Data Mining* (PAKDD), Dec. 2022.

2. **Qisheng Zhang**, Dian Chen, Y. Mahajan, Ing-Ray Chen, Dong S. Ha, and Jin-Hee Cho, "Attack-Resistant, Energy-Adaptive Monitoring for Smart Farms: Uncertainty-Aware Deep Reinforcement Learning Approach," submitted to *IEEE Internet of Things Journal*, Oct. 2022 (2022 JCR IF 10.238).

3. Zhen Guo*, Zelin Wan*, **Qisheng Zhang***, Xujiang Zhao*, Feng Chen, Jin-Hee Cho, Qi Zhang, Lance Kaplan, Dong Hyun Jeong, and Audun Jøsang, "A Survey on Uncertainty Reasoning and Quantification for Decision Making: Belief Theory Meets Deep Learning," submitted to the *ACM Computing Surveys (CSUR)*, May 15, 2022 (2021 JCR IF 14.324; ranked 3/109 in Computer Science Theory & Methods; * indicates an equal contribution).

Papers In Preperation

1. **Qisheng Zhang**, Jin-Hee Cho, Terrence J. Moore, Dongseong Kim, Hyuk Lim, and Frederica F. Nelson, "EVADE: Efficient Moving Target Defense for Autonomous Network," in preparation for a conference paper submission.

2. **Qisheng Zhang**, Terrence J. Moore, Dongseong Kim, Hyuk Lim, Frederica F. Nelson, and Jin-Hee Cho, "Uncertainty-Aware Intrusion Response System in In-Vehicle Networks," for a conference paper submission.

3. **Qisheng Zhang**, Terrence J. Moore, Frederica F. Nelson, Hyuk Lim, Dongseong Kim, and Jin-Hee Cho, "Deep Reinforcement Learning-based Adaptive Moving Target Defense: Network Topology Shuffling Approach," in preparation for a journal paper submission.

4. Dian Chen, **Qisheng Zhang**, Ing-Ray Chen, Dong S. Ha, and Jin-Hee Cho, "Energy-Aware, Attack-Resilient Monitoring for Smart Farms Using Transfer Learning-based Deep Reinforcement Learning," for a journal paper submission.

Professional Presentations, Talks, & Briefing

1. Demonstration & Technical Talk, "Deep Reinforcement Learning and Its Applications in Computer Science, " NSF-Funded Summer Workshop, *Artificial Intelligence Awareness*, Computer Science Department, University of District Columbia, Aug. 2022 (in-person).

2. Conference Presentation, "An Attack-Resilient and Energy-Adaptive Monitoring System for Smart Farms," *IEEE GLOBECOM*, 4–8 Dec. 2022, Rio de Janeiro, Brazil (in-person).

3. Conference Presentation, "Analysis of Network Resilience Under Epidemic Attacks: Deep Reinforcement Learning-based Network Topology Adaptations," *The 2021 IEEE Global Communications Conference (GLOBECOM 2021)*, Dec. 2021 (virtual).

4. Conference Presentation, "DREVAN: Deep Reinforcement Learning-based Vulnerability-Aware Network Adaptations for Resilient Networks," *The 2021 IEEE Conference on Communications and Network Security (CNS 2021)*, Oct. 2021 (virtual).

Paper Review Services

- IEEE Transactions on Services Computing (TSC), 2022
- IEEE Transactions on Network and Service Management (TNSM), 2020 – 2022
- Computer Journal, Oxford Press, 2020 – 2022

Skills

Languages: Chinese (Mandarin), English
Programming Languages: C / C++, Java, Python, MATLAB
Python Libraries: TensorFlow, PyTorch

Honors & Awards

First-Class Honours, University of Warwick	2018
Academic Scholarships, Loughborough University	2017
Academic Scholarships, Shandong University	2014–2016