QISHENG ZHANG

Phone: +1 202-445-6768|Email: a87107678z@gmail.com|LinkedIn: https://www.linkedin.com/in/qs666
Github: https://github.com/DigitalErage|Homepage: https://DigitalErage.github.io

EDUCATION

Virginia Tech, Falls Church, VA, USA *Aug. 2019 - Present*
Ph.D. in Computer Science GPA: 3.8/4.0
Courses: Introduction to Deep Learning, Network Security, Theory of Algorithms, Data Analytics, Advanced Topics in Game Theoretic Cybersecurity, Spatial Data Management

University of Warwick, Coventry, United Kingdom *Oct. 2017 - Jul. 2018*
M.S. in Mathematical Sciences (with Distinction) GPA: 3.8/4.0
Courses: Algebraic Geometry, Representation Theory, Elliptic Curves, Commutative Algebra, Group Theory, Ring Theory

Loughborough University, Loughborough, United Kingdom *Sep. 2016 - Jun. 2017*
Exchange Student in Mathematics GPA: 87/100
Courses: Random Processes and Time Series Analysis, Introduction to Stochastic Processes, Discrete Stochastic Methods in Finance, Continuous Stochastic Methods in Finance

Shandong University, Jinan, China *Sep. 2013 – Jun. 2017*
B.S. in Mathematics and Applied Mathematics GPA: 88/100
Courses: Differential Geometry, Abstract Algebra, Functional Analysis, General Topology, Partial Differential Equations, Mathematical Statistics, Probability Theory

SKILLS

Programming Languages: C / C++, Java, Python, MATLAB, Mathematica, R, SQL, HTML, CSS
Python Libraries: TensorFlow, PyTorch, Keras, Scikit-learn, Networkx, Jupyter, Pandas, SciPy, CARLA, SUMO, python-can
Tools: git, AWS, Linux, Kubernetes

EXPERIENCE

Virginia Tech - *Graduate Research Assistant* *Aug. 2019 - Present*
Research Interests: AI-based cybersecurity, deep reinforcement learning, autonomous driving, robotics, decision-making under uncertainty, multi-agent systems, network science, Natural Language Processing (NLP), Internet of Things (IoT),
Research Projects:
[1] "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
- Developed an **intrusion response system** in **in-vehicle networks (CAN Bus)** for **autonomous driving** tasks with **deep reinforcement learning** and **uncertainty estimation**.
- Developed a **deep reinforcement learning**-based network adaptations for **network resilience** algorithm to generate robust network topologies against epidemic attacks under **multiple system objectives** in **IP networks**.
- Deployed the network environment with **Networkx** and the deep reinforcement learning algorithms with **Tensorflow** and **Pytorch**.

[2] "Energy Centric Wireless Sensor Node System for Smart Farms," funded by the NSF (2021-2025), https://wordpress.cs.vt.edu/nsfsf
- Leveraged **multi-agent deep reinforcement learning** and subjective logic to propose an **uncertainty-aware** energy-adaptive **monitoring system** for a solar sensor-based **smart animal farm**.

[3] "MUDL: Multidimensional Uncertainty-Aware Deep Learning Framework," funded by the NSF (2021-2025)
- Proposed a **deep reinforcement learning** algorithm PPO-UE for **robotic tasks**, a PPO variant equipped with self-adaptive **uncertainty-aware** explorations based on a ratio uncertainty level.
- Proposed a **NLP** and **deep reinforcement learning**-based **intent classification framework** that can **identify the intent of fake news**.

PUBLICATIONS

Journal Papers
[1] **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", accepted to *IEEE Internet of Things Journal*, May. 2023.
[2] **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.
[3] **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.

Conference Papers

[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 Topology Shuffling Using Deep Reinforcement Learning", *The 21st International Conference on Applied Cryptography and Network Security* (ACNS), Jun. 2023.

[2] **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", in *2022 IEEE Global Communications Conference* (GLOBECOM), Rio de Janeiro, Brazil, 2022, pp. 2776-2781.

[3] **Qisheng Zhang**, Jin-Hee Cho, Terrence J. Moore, and Frederica Free Nelson, "DREVAN: Deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks", in *2021 IEEE Conference on Communications and Network Security (CNS)*, Tempe, AZ, USA, 2021, pp. 137-145.

[4] **Qisheng Zhang**, Jin-Hee Cho, and Terrence J. Moore, "Network resilience under epidemic attacks: Deep reinforcement learning network topology adaptations", *IEEE Global Communications Conference*, Madrid, Spain, 2021, pp. 1-7.

[5] Zhen Guo, Qi Zhang, **Qisheng Zhang**, Lance Kaplan, Audun Jøsang, Feng Chen, Dongseong Jeong, and Jin-Hee Cho, "Detecting Intents of Fake News Using Uncertainty-Aware Deep Reinforcement Learning", accepted to *The International Conference on Web Services* (ICWS), Jul. 2023.

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", *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", *1st AAAI Workshop on Uncertainty Reasoning and Quantification in Decision Making*, 2023.

Papers Under Review

[1] 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", submitted to *IEEE Transactions on Sustainable Computing*, Apr. 2023.

[2] Lei Zhang, **Qisheng Zhang**, Zhiqian Chen, Yanshen Sun, Chang-Tien Lu, and Liang Zhao, "Infinitely Deep Graph Transformation Learning", submitted to *the 23rd IEEE International Conference on Data Mining (ICDM 2023)*, Jul. 2023.

Papers In Preparation

[1] **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.

Professional Presentations, Talks, & Briefing

[1] Conference Presentation, "PPO-UE: Proximal Policy Optimization via Uncertainty-Aware Exploration," *AAAI*, 7-14 Feb. 2023, Washington DC, USA (in-person).

[2] 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).

[3] 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).

[4] 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).

[5] 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 – 2023*
IEEE Transactions on Network and Service Management (TNSM) *2020 – 2022*
Computer Journal, Oxford Press *2020 – 2022*

Honors & Awards

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