

Zelin Wan

Phone: 520-461-8509 | Email: zelin@vt.edu | GitHub.com/Wan-ZL | Wan-ZL.github.io |
scholar.google.com/citations?user=0Z8N7zYAAAAJ

EDUCATION

Virginia Tech

Doctor of Philosophy in Computer Science

Falls Church, VA
Aug. 2020 - Present

- Tentative Dissertation: Artificial Intelligence-based Cyber Defensive Deception
- Advisor: Dr. Jin-Hee Cho
- GPA: 3.84
- Status: Passed the Qualifying Process, Sep. 2021
- Status: Passed the Preliminary Exam, Nov. 2022
- Status: Passed the Research Defense, Oct. 2024
- Anticipated Final Defense and Graduation: Feb. 2025

Virginia Tech

Master of Science in Computer Science

Falls Church, VA
Aug. 2019 - Dec. 2021

- Advisor: Dr. Jin-Hee Cho
- GPA: 3.88
- Aug. 2020: Pursued a master program with PhD course work

University of Arizona

Bachelor of Science in Computer Science

Tucson, AZ
Aug. 2015 - May 2019

- Major: Computer Science
- Minor: Mathematics

EXPERIENCE

Graduate Teaching Assistant (GTA)

Department of Computer Science, Virginia Tech

Dec 2023 – Present
Falls Church, VA

- **CS 5624: Natural Language Processing (Spring 2025)**
 - Assisted in creating course assignments and slides focusing on statistical NLP, deep learning architectures, and applications in text processing.
 - Conducted weekly recitation sessions, demonstrating the use of NLP libraries (e.g., NLTK, PyTorch) and best practices for model evaluation.
 - Held office hours to address student questions regarding project implementation, algorithmic complexities, and performance optimization.
- **CS 5914: Decision Making Under Uncertainty (Fall 2024)**
 - Supported lectures and in-class discussions on belief theory, reinforcement learning, and deep learning techniques for decision-making.
 - Collaborated with the instructor to develop and refine course materials, including homework assignments and project guidelines.
 - Provided guidance and feedback on student presentations, term papers, and coding projects involving uncertainty modeling and AI-based decision-making.
- **CS 4804: Introduction to Artificial Intelligence (Spring 2024)**
 - Assisted in designing course materials covering fundamental AI topics such as search, game playing, logic, machine learning, and deep learning.
 - Held interactive lab sessions and office hours to clarify course concepts and troubleshoot student projects.
 - Graded homework assignments, coding projects, and exams, providing detailed feedback to reinforce understanding.

Graduate Research Assistant (GRA)

Department of Computer Science, Virginia Tech

May 2020 – Dec 2023

Falls Church, VA

- Designed and implemented a Human-AI teaming system utilizing Evidential Deep Learning algorithms and computer vision techniques to enhance operational performance.
- Designed a game-theory-guided deep learning model to address the cold start problem in neural networks and applied specialized AI algorithms for real-time drone monitoring.
- Engaged academic project funded by the U.S. Army Research Office (ARO): Foureyeye: Cyber Defensive Deception based on Hypergame Theory for Tactical Networks.
- Engaged in multiple AI and cybersecurity projects funded by the U.S. Army Research Office (ARO), exploring sensor data and visual feeds for drone fleet and unmanned ground vehicle (UGV) surveillance missions.
- Published nine peer-reviewed papers to IEEE Journals/Conferences, ACM Conference, and more in the pipeline.

Computer Vision Internship

Bobyard

May 2024 – Aug 2024

San Francisco, CA

- Developed and implemented zero-shot learning techniques for detecting, localizing, and classifying symbols and pipe/irrigation notations on complex construction drawings.
- Designed a novel algorithm based on the Segment Anything Model (SAM) to accurately detect very long and thin lines in construction drawings, enhancing the precision of symbol localization.
- Conducted extensive experiments with various CV models and synthetic data generation pipelines.
- Deployed CV models on cloud infrastructure, optimizing performance and inference speed to improve operational efficiency.

Recommendation Algorithm Internship

ByteDance, TikTok Recommendation Technology Team

Mar 2023 – Aug 2023

Remote

- Involved in developing a dynamic recommendation system that suggests the optimal merchandise for sellers to display during live streams, enhancing viewer engagement and sales potential.
- Integrated Deep Reinforcement Learning (DRL) into the merchandise recommendation system to optimize for long-term user engagement and sales.
- Enhanced DRL performance by implementing a multimodal neural network that generates feature vectors from both photos and merchandise descriptions.

Research Scientist Internship

Intelligent Fusion Technology

May 2022 – Aug 2022

Germantown, MD

- Involved and contributed to the projects funded by U.S. Air Force Research Laboratory (AFRL):
 - Entitled “EXTRA: Explainable and Transparent Machine Learning for Autonomous Decision-Making” (\$1.5M contract).
 - Entitled “ROBOT: Resilience Oriented Blockchain Operational Transactor for Urban Air Mobility Networks”.
- Involved with the proposal for the project funded by America’s Seed Fund.
 - Entitled “Explainable AI for Complex Decision Making for Command and Control in MDO”.
 - Entitled “Deep Reinforcement Learning (DRL) Enabled Warfighter Assistant”.
- Developed deep neural network prototypes that fused structured sensor data and textual system logs to improve maintenance predictions.
- Explored advanced DRL techniques (A2C, target network, double DQN, dueling network, prioritized experience replay) and applied explainable AI (Saliency Map) to highlight decision points.

Undergraduate Teaching Assistant (UGTA)

Department of Computer Science, University of Arizona

Jan. 2019 – May 2019

Tucson, AZ

- UGTA for course CS445: Introduction of Algorithms
- Supported in-class activities, offered office hours, and graded assignments and exams.

- Provided Computer Science majors with the guidance of professional coaches.

AREA OF INTEREST

Machine / Deep Learning in Computer Vision and Reinforcement Learning, Explainable AI, Game Theory, Cybersecurity, Network Science, Uncertainty-Aware Decision Making, Knowledge Representation and Reasoning, Simulation and Modeling.

GRADUATE COURSES TAKEN

Advanced Machine Learning, Deep Learning, Data Analytics, Computer Vision, Game Theoretic Cybersecurity, Network Security, Intro to Urban Computing, Theory of Algorithms, Ethics & Professionalism in CS, Deep Learning, Modeling and Evaluation of Computer Systems, Network Arch and Protocols, Analysis of Discrete Structures, Comparative Programming Languages, Computer Networking, Computer Organization, Web Programming, Data Visualization, Object-Oriented Programming and Design, Systems Programming and Unix, Principles of Operating Systems.

PUBLICATIONS

PUBLISHED AND ACCEPTED

- [1] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, et al., “Optimizing Effectiveness and Defense of Drone Surveillance Missions via Honey Drones”, *ACM Transactions on Internet Technology*, Sep. 2024 (2023 JCR IF 5.3).
- [2] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “Deception in Drone Surveillance Missions: Strategic vs. Learning Approaches,” *Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, DOI: 10.1145/3565287.3616525, 2023 (2021 JCR IF 3.7).
- [3] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “Resisting multiple advanced persistent threats via hypergame-theoretic defensive deception,” *IEEE Transactions on Network and Service Management (TNSM)*, DOI: 10.1109/TNSM.2023.3240366, 2023 (2022 JCR IF 4.195).
- [4] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “Foureyeye: Defensive deception against advanced persistent threats via hypergame theory,” *IEEE Transactions on Network and Service Management (TNSM)*, DOI: 10.1109/TNSM.2021.3117698, Oct. 2021 (2020 JCR Impact Factor (IF) 3.894).
- [5] **Z. Wan**, Y. Mahajan, B. Kang, T. J. Moore, and J.H. Cho, “A survey on centrality metrics and their network resilience analysis,” *IEEE Access*, vol. 9, pp. 104773-104819, DOI: 10.1109/ACCESS.2021.3094196, 2021 (2021 JCR IF 3.75)
- [6] Z. Guo*, **Z. Wan***, X. Zhao*, Q. Zhang*, Qi Zhang, A. Jøsang, L. Kaplan, A. Swami, F. Chen, D. Jeong, and J.H. Cho, “A survey on uncertainty reasoning and quantification in belief theory and its application to deep learning,” *Information Fusion*, DOI: 10.1016/j.inffus.2023.101987., 2023 (2023 JCR IF 18.6).
- [7] A. Anwar, M. Zhu, **Z. Wan**, J.H. Cho, C. Kamhoua, and M. P. Singh, “Honeypot-Based Cyber Deception Against Malicious Reconnaissance via Hypergame Theory,” *IEEE Global Communications Conference*, DOI: 10.1109/GLOBECOM48099.2022.10000813, 2022 (2019 JCR IF 2.836).
- [8] M. Zhu*, A. H. Anwar*, **Z. Wan***, J.H. Cho, C. Kamhoua, and M. P. Singh, “A survey of defensive deception: Approaches using game theory and machine learning,” *IEEE Communications Surveys & Tutorials (CST)*, vol. 23, pp. 2460 - 2493, DOI: 10.1109/COMST.2021.3102874, 2021 (2021 JCR IF 25.2)

- [9] Q. Zhang*, A. Z. Mohammed*, **Z. Wan***, J.H. Cho, and T. J. Moore, “Diversity-by-design for dependable and secure cyber-physical systems: A survey,” *IEEE Transactions on Network and Service Management (TNSM)*, DOI: 10.1109/TNSM.2021.3091391, 2021 (2020 JCR IF 4.195).

UNDER REVIEW

- [10] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “Decision Theory-Guided Deep Reinforcement Learning for Fast Learning”, submitted to *IEEE International Conference on Robotics and Automation (ICRA)*.
- [11] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “Cyber Deception for Mission Surveillance via Hypergame-Theoretic Deep Reinforcement Learning”, submitted to *IEEE Transactions on Dependable and Secure Computing (TDSC)*.
- [12] D. Chen, **Z. Wan**, D.S. Ha and J.H. Cho, “Sustainable Smart Farm Networks: Enhancing Resilience and Efficiency with Decision Theory-Guided Deep Reinforcement Learning”, submitted to *ACM Transactions on Intelligent Systems and Technology (TIST)*.

IN PREPARATION

- [13] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, “A Shared Mental Model Framework for Human-Machine Teaming System”.
- [14] D. Chen, **Z. Wan**, H.J. Yoon, R. He, S.W. Lee, J.H. Cho, “Human-Machine Teaming Systems: A Survey”.

SELECTED PROJECTS

Shared Mental for Human-AI Teaming (Jan. 2024 - Present, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Developed a secure framework that integrates cyber deception with shared mental models to enhance UGV surveillance missions.
- Key Methodologies: Leveraged a Vision Transformer (ViT) pipeline for UGV-based image tokenization and object detection. And integrated Evidential Deep Learning (EDL) for uncertainty quantification, allowing the model to express “I don’t know” when predictions are uncertain.

Decision Theory-Guided Deep Reinforcement Learning for Fast Learning (Feb. 2023 - May 2024, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Mitigate the cold start problem in Deep Reinforcement Learning (DRL) by integrating decision theory to enhance initial performance and robustness.
- Key Methodologies: Developed a DT-guided DRL framework combining decision theory with Proximal Policy Optimization (PPO). Tested on cart pole and maze environments, comparing against traditional DRL, transfer learning, sample efficiency, and imitation learning methods.
- Key Findings: Achieved up to 184% higher initial rewards and 53% more accumulated rewards in large mazes compared to standard DRL. Enabled faster convergence and improved performance in complex environments.
- Source Code: <https://github.com/Wan-ZL/DT-DRL>

Optimizing Effectiveness and Defense of Drone Surveillance Missions via Honey Drones (Jan. 2022 - Mar. 2023, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Develop a honey drone-based surveillance mission system that allows drones to effectively execute an assigned surveillance mission while thwarting DoS attacks by using honey drones.
- Key Methodologies: We consider attack-defense interactions where both parties use DRL-based signal strength selection to achieve their respective goal. We particularly leverage the Asynchronous Advantage actor-Critic (A3C) and introduce fast training using parallel processing with multiple local workers.

- Key Findings: The honey drone-based mission system outperforms non-honey drone counterparts. Through in-depth sensitivity analyses, we demonstrate how DRL-based (attack or defense) decision making improves attack strength and mission performance, respectively.
- Source Code: <https://github.com/Wan-ZL/gym-drones>

Foureye: Defensive Deception Against Advanced Persistent Threats via Hypergame Theory (May 2020 - Mar. 2021, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Design and analyze an attack-defense hypergame with defensive deception techniques under a high mobility network.
- Key Methodologies: We used hypergame theory as a framework to simulate the interactions between attackers and a defender, where the player's decision is made based on belief and utility dynamically estimated under uncertainty.
- Key Findings: Even if defensive deception techniques mainly aim to mislead attacker's perception, they also lead to a positive effect to the system security by increasing the true positive rate of intrusion detection system due to the benefit from attacker's intelligence collected.
- Source Code: <https://github.com/Wan-ZL/ARO-Foureye>

Resisting Multiple Advanced Persistent Threats via Adaptive Defensive Deception Based on Hypergame Theory (Apr. 2021, - Feb. 2023, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Analyze the hypergame with multiple attackers and a single defender under an uncertain environment composed of IoT devices.
- Key Methodologies: We leveraged hypergame theory to properly deal with a multi-agent game with uncertainty and employed the machine learning algorithms defender directly identify the optimal strategy.
- Key Findings: The game-theoretic machine learning-based defense solutions provide higher performance mainly when attackers slowly arrive.
- Source Code: <https://github.com/Wan-ZL/Foureye-2-simulation>

Belief Theories in Deep Learning for Uncertainty Decisions (Dec. 2020, - Jun. 2022, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Bridge the gap between belief/evidence theories and machine learning for improved uncertainty reasoning and decision-making.
- Key Methodologies: Studied uncertainty in belief and deep learning models, evaluating belief theories' potential to enhance deep learning decision-making.
- Key Findings: Identified deep learning's limitations in handling uncertainty and explainability. Showed how belief models (DST, IDM, SL) enhance decision-making and explainable AI.

A Survey on Centrality Metrics and Their Network Resilience Analysis (Nov. 2019 - Jul. 2021, Computer Science, Virginia Tech)

- Role: Lead GRA for PI Dr. Jin-Hee Cho
- Goal: Introduce various existing centrality metrics, including point, group, and graph centrality metrics, and discusses their applicabilities in various networks
- Key Methodologies: We first discussed the multidisciplinary concepts of centrality. We conducted a comprehensive survey on centrality metrics including over 60 metrics of point, group, and graph centrality measures. We implemented over 60 centrality metrics surveyed and conducted extensive performance evaluation to analyze their network resilience in the wide range of attack severity and network dynamics under four different real datasets.
- Key Findings: The meaning of centrality is not only limited to how a node is connected to other nodes, but also implies how actively the node communicates to each other and how it can control or influence other nodes in their centrality or vulnerability.

- Source Code: <https://github.com/Wan-ZL/Centrality-Metric-Survey>

Hackathon 2019 – Hack Arizona (Jan. 2019, University of Arizona)

- Role: Team Leader
- Goal: Designed a voice program for Autistic children.
- Key Methodologies: The program was built based on Amazon Alexa.
- Obtained Prize: Overall Best Hack
- Source Code: <https://github.com/Wan-ZL/Hack-Arizona-2019>

Hackathon 2018 – Hack Arizona (Jan. 2018, University of Arizona)

- Role: Team Member
- Goal: Created an IOS app that connects to the UAccess database and shows classroom location and course detail with AR View.
- Key Methodologies: Devised the web crawler, collected and classified the information of curriculum of our university. Matched the curriculum information with the relevant geographic positions on the e-map for the frontend developers.
- Source Code: <https://github.com/wenkangzh/folo>.

Hackathon 2017 – Hack Arizona (Jan. 2017, University of Arizona)

- Role: Team Member
- Goal: Created an intelligence home assistant based on Amazon Alexa.
- Key Methodologies: Built remote connectivity between the servers and household appliances. Designed and manufactured household appliances models.
- Source Code: <https://github.com/blueandhack/Pandora-Box>

TECHNICAL SKILLS

Python–proficient, Java–proficient, Matlab–proficient, Jupyter Notebook–proficient, PyTorch–proficient, Numpy–proficient, scikit-learn–proficient, C–familiar, HTML–familiar, MIPS–familiar, TensorFlow–familiar, OpenCV–familiar, PyBullet–familiar, OpenAI Gym–familiar, Google MediaPipe–familiar, Anaconda–familiar, Windows–familiar, Linux–familiar.

LANGUAGES

English–Professional, Mandarin Chinese–Native, Spanish–Basic.

LICENSES & CERTIFICATIONS

IBM Certificate for Computer Vision and Image Processing Fundamentals

- Issued Apr 2022
- Credential Link: <https://courses.edx.org/certificates/076de7bac7194cc1ab100afec66a6a4a>

HONORS & AWARDS

- **Graduate Candidacy Status Tuition Reduction** - Aug 2024
- **Graduate Candidacy Status Tuition Reduction** - Aug 2023
- **College of Engineering Graduate Student Publication Fellowship** - Apr 2023
- **Nomination for the Joseph Frank Hunkler Memorial Scholarship** - Jan 2022
- **Overall Best Hack for Hack Arizona (Hackathon 2019)** - Jan 2019

EDITORIAL BOARD

- Editorial Board, Section Editor, Computer Software and Media Applications (CSMA), Nov. 2023 - current
- Program Committee, The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS 2024), 2024

- Information Fusion, 2025
- The Journal of Supercomputing, 2025
- Discover Internet of Things, 2024
- Information Fusion, 2024
- Discover Internet of Things, 2024
- PeerJ Computer Science, 2024
- Discover Internet of Things, 2024
- IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, 2024
- IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, 2024
- IEEE Transactions on Services Computing, Sep, 2024
- IEEE Transactions on Aerospace and Electronic Systems, Jul, 2024
- Social Network Analysis and Mining, Jul, 2024
- IEEE Transactions on Information Forensics and Security, Jun, 2024
- Transactions on Services Computing, Jun, 2024
- Transactions on Services Computing, Jun, 2024
- Social Network Analysis and Mining, Apr, 2024
- Transactions on Services Computing, Mar, 2024
- Transactions on Services Computing, Mar, 2024
- IEEE Transactions on Information Forensics and Security, Feb, 2024
- IEEE Transactions on Aerospace and Electronic Systems, Feb, 2024
- Transactions on Services Computing, Jan, 2024
- Green Energy and Environmental Technology, Jan, 2024
- Transactions on Services Computing, Nov. 2023
- Social Network Analysis and Mining, Nov. 2023
- AI, Computer Science and Robotics Technology, Oct. 2023
- Transactions on Services Computing, Sep. 2023
- IEEE Transactions on Aerospace and Electronic Systems, Sep. 2023
- IEEE Transactions on Aerospace and Electronic Systems, Apr. 2023
- AI, Computer Science and Robotics Technology, Sep. 2023
- Green Energy and Environmental Technology, Sep. 2023
- AI, Computer Science and Robotics Technology, Aug. 2023
- Qeios, Sep. 2023
- AI, Computer Science and Robotics Technology, Jul. 2023
- IEEE Transactions on Network and Service Management, Jun. 2023
- Social Network Analysis and Mining, Jun. 2023
- Journal of Intelligent & Fuzzy Systems, Apr. 2023
- AI, Computer Science and Robotics Technology, Mar. 2023
- AI, Computer Science and Robotics Technology, Feb. 2023
- IEEE Transactions on Information Forensics & Security, 2023
- IEEE Transactions on Aerospace and Electronic Systems, Dec. 2022
- The 7th IEEE European Symposium on Security and Privacy (Euro S&P), Nov. 2022
- IEEE Transactions on Aerospace and Electronic Systems, May 2022
- The 23rd World Conference on Information Security Applications, 2022
- The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022)
- The Computer Journal, Dec. 2021
- IEEE Access, Jul. 2021