Zelin Wan

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

Education

Virginia Tech Falls Church, VA
Doctor of Philosophy in Computer Science and Applications Aug. 2020 - Present

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

Virginia Tech Falls Church, VA
Master of Science in Computer Science and Applications Aug. 2019 - Dec. 2021

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

University of Arizona Tucson, AZ
Bachelor of Science in Computer Science Aug. 2015 - May 2019

- Major: Computer Science
- Minor: Mathematics

Experience

Graduate Research Assistant (GRA) May 2020 – Present
Department of Computer Science, Virginia Tech Falls Church, VA

- Involved with the project funded by U.S. Army Research Office (ARO), entitled "Foureye: Cyber Defensive Deception based on Hypergame Theory for Tactical Networks."
- Involved with the project funded by U.S. Army Research Office (ARO), entitled "Uncertainty-Aware Deep Reinforcement Learning-based Defense for Resilient Cyber-Physical Systems."

Recommendation Algorithm Internship Mar 2023 – Aug 2023
ByteDance, TikTok Recommendation Technology Team 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 May 2022 – Aug 2022
Intelligent Fusion Technology Germantown, MD

- Involved with the project funded by U.S. Air Force Research Laboratory (AFRL), entitled "EXTRA: Explainable and Transparent Machine Learning for Autonomous Decision-Making".
- Involved with the project funded by U.S. Air Force Research Laboratory (AFRL), entitled "ROBOT: Resilience Oriented Blockchain Operational Transactor for Urban Air Mobility Networks".
- Involved with the proposal for the project "Explainable AI for Complex Decision Making for Command and Control in MDO" funded by America's Seed Fund.
- Involved with the proposal for the project "Deep Reinforcement Learning (DRL) Enabled Warfighter Assistant" funded by America's Seed Fund.

Undergraduate Teaching Assistant (UGTA) Jan. 2019 – May 2019
Department of Computer Science, University of Arizona Tucson, AZ

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

Computer Science Mentor Aug. 2019 – Dec. 2019
Department of Computer Science, University of Arizona Tucson, AZ

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

Area of Interest

Machine/Deep learning, Explainable AI, Game Theory, Cybersecurity, Network Science, Cyber-Physical Systems, 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, 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).

[2] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, "Resisting multiple advanced persistent threats via adaptive defensive deception based on hypergame theory," *IEEE Transactions on Network and Service Management*, DOI: 10.1109/TNSM.2023.3240366, 2023 (2022 JCR IF 4.195).

[3] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, "Foureye: Defensive deception against advanced persistent threats via hypergame theory," *IEEE Transactions on Network and Service Management*, DOI: 10.1109/TNSM.2021.3117698, Oct. 2021 (2020 JCR Impact Factor (IF) 3.894).

[4] **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)

[5] 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).

[6] 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).

[7] 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*, vol. 23, pp. 2460 - 2493, DOI: 10.1109/COMST.2021.3102874, 2021 (2021 JCR IF 25.2)

[8] 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*, DOI: 10.1109/TNSM.2021.3091391, 2021 (2020 JCR IF 4.195).

Under Review

[9] **Z. Wan**, J.H. Cho, M. Zhu, A. Anwar, C. Kamhoua, and M. P. Singh, "Optimizing Effectiveness and Defense of Drone Surveillance Missions via Honey Drones," submitted to *IEEE International Conference on Computer Communications* (2022 JCR IF 4.68).

[10] **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* (2022 JCR IF 7.3).

Selected Projects

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

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.
- **My Contribution**: 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.
- **My Contribution**: 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, 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 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

Journal/Conference Papers Reviews

- 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