Zizhan Zheng

Contact Information

Associate Professor
Department of Computer Science
Tulane University

Voice: (614) 312-3013
E-mail: zzheng3@tulane.edu
WWW: `https://cs.tulane.edu/~zzheng3`

Research Interests

- AI Security and Safety
- Reinforcement Learning
- Generative AI
- Networks

Education

PhD in Computer Sc. and Engg., The Ohio State University	June 2010
MS in Computer Science, Peking University, Peking, China	July 2005
BE in Polymer Sc. and Engg., Sichuan University, Chengdu, China	July 2002

Professional Experience

Associate Professor, Tulane University	July 2023 - present
Assistant Professor, Tulane University	July 2016 - June 2023
Associate Specialist, University of California at Davis	Sept. 2014 - June 2016
Postdoctoral Researcher, The Ohio State University	Sept. 2010 - Aug. 2014

Teaching Experience

Tulane University July 2016 - present

- *CMPS 1500 Intro to Computer Science I* (Spring 2024)
- *CMPS/MATH 2170 Discrete Mathematics* (Fall 2016-2018, Fall 2021, Spring 2024)
- *CMPS 4010 Capstone Project I* (Fall 2022)
- *CMPS 4740/6740 Reinforcement Learning* (Fall 2020, Spring 2022)
- *CMPS 4750/6750 Computer Networks* (Spring 2017-2018, Spring 2020)
- *CMPS 6750 Computer Networks (Online)* (Fall 2023)
- *CMPS 4760/6760 Distributed Systems* (Spring 2019, Spring 2021)
- *CMPS 7010 Research Seminar* (Fall 2019)

Teaching Assistant, The Ohio State University	Sept. 2006 - Dec. 2007
Teaching Assistant, Peking University	Feb. 2004 - July 2004

Honors and Awards

- NSF CAREER Award, 2022
- IEEE INFOCOM Distinguished TPC Member, 2019, 2021
- ACM SenSys Student Travel Award, 2008
- University Fellowship, The Ohio State University, 2005
- May 4th Scholarship, Peking University, 2003
- Outstanding Student Award (first class), Sichuan University, 2000, 2001
- Rohm and Haas Scholarship, Sichuan University, 1999

Grants

1. **Co-PI**, *Tulane Institute for Integrated Data and Health Sciences (TIIDHS)*, **Tulane University**, Total funding: $600,000, Zheng's share: $45,000, 12/01/2022-11/30/2025, PI: Hong-Wen Deng, Co-PIs: Hui Shen, Yu-Ping Wang, Donald P. Gaver, Xiaowen Liu, Zhengming Ding, Amanda Anderson, Tanika Kelly, Katherine Mills.
2. **PI**, *CAREER: Learning to Secure Cooperative Multi-Agent Learning Systems: Advanced Attacks and Robust Defenses*, **National Science Foundation**, Total funding: $494,192, 06/01/2022-05/31/2027, Sole PI.
3. **Senior Personnel**, *IUCRC Planning Grant: Tulane: Center for Applied Artificial Intelligence (CAAI)*, **National Science Foundation**, Total funding: $19,990, 03/01/22-02/28/23, PI: Aron Culotta.
4. **PI**, *SaTC: CORE: Small: Towards Robust Moving Target Defense: A Game Theoretic and Learning Approach*, **National Science Foundation**, Total funding: $260,105 (including an REU Supplement), 08/15/2018-07/31/2022, Sole PI.
5. **PI**, *NeTS: Small: Collaborative Research: Reliable 60 GHz WLANs through Coordination: Measurement, Modeling and Optimization*, **National Science Foundation**, Total funding: $499,028, Zheng's share: $235,912, 10/01/2018-09/30/2022, Collaborative PI: Parth Pathak (GMU).
6. **PI**, *RCS: Towards Optimal Timing in Cyber Defense: A Game Theoretic and Learning Approach*, **Louisiana Board of Regents**, Total funding: $97,566, 06/01/2017-06/30/2019, Sole PI.

Publications

(Note: * indicates my student)

Preprints

1. Haifeng Xia, Taotao Jing, Chen Chen, Zizhan Zheng, and Zhengming Ding, "Similar-Silo Classification Model Ensemble for Personalized Federated Learning," 2022.
2. Haifeng Xia, Taotao Jing, Zizhan Zheng, and Zhengming Ding, "Privacy-Protected "Win-Win" Multi-Domain Collaborative Learning," 2022.

Conference/Workshop papers

1. Xiaolin Sun* and Zizhan Zheng, "Belief-Enriched Pessimistic Q-Learning against Adversarial State Perturbations," *International Conference on Learning Representations (**ICLR**)*, May 2024.
2. Xiaolin Sun* and Zizhan Zheng, "Robust Q-Learning against State Perturbations: a Belief-Enriched Pessimistic Approach," *The NeurIPS Workshop on Multi-Agent Security: Security as Key to AI Safety (MASEC)*, Dec. 2023.
3. Yunian Pan, Tao Li, Henger Li*, Tianyi Xu*, Quanyan Zhu, and Zizhan Zheng, "A First Order Meta Stackelberg Method for Robust Federated Learning," *The ICML Workshop on New Frontiers in Adversarial Machine Learning (AdvML-Frontiers)*, July 2023.
4. Xiaolin Sun*, Jacob Masur, Ben Abramowitz, Nicholas Mattei, and Zizhan Zheng, "Pandering in a (Flexible) Representative Democracy," *Conference on Uncertainty in Artificial Intelligence (**UAI**)*, May 2023.
5. Ding Zhang, Panneer Selvam Santhalingam, Parth Pathak, and Zizhan Zheng, "CoBF: Coordinated Beamforming in Dense mmWave Networks," *ACM International Conference on Measurement and Modeling of Computer Systems (**SIGMETRICS**)*, June 2023. (Acceptance Rate = 10%)
6. Henger Li*, Chen Wu, Senchun Zhu, and Zizhan Zheng, "Learning to Backdoor Federated Learning," *ICLR 2023 Workshop on Backdoor Attacks and Defenses in Machine Learning (BANDS)*, May 2023.
7. Xiaolin Sun*, Jacob Masur, Ben Abramowitz, Nicholas Mattei, and Zizhan Zheng, "Does Delegating Votes Protect Against Pandering Candidates? (Extended Abstract)," *International Conference on Autonomous Agents and Multi-Agent Systems (**AAMAS**)*, May 2023.

8. Tianyi Xu*, Ding Zhang, and Zizhan Zheng, "Online Learning for Adaptive Probing and Scheduling in Dense WLANs," *IEEE International Conference on Computer Communications (**INFOCOM**)*, May 2023. (Acceptance Rate = 19.2%)

9. Henger Li*, Xiaolin Sun*, and Zizhan Zheng (*Co-primary authors), "Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework," *Conference on Neural Information Processing Systems (**NeurIPS**)*, Dec. 2022. (Acceptance Rate = 25.6%)

10. Henger Li* and Zizhan Zheng, "Robust Moving Target Defense against Unknown Attacks: A Meta-Reinforcement Learning Approach," *Conference on Decision and Game Theory for Security (GameSec)*, Oct. 2022.

11. Zhongdong Liu, Bin Li, Zizhan Zheng, Y. Thomas Hou, and Bo Ji, "Towards Optimal Tradeoff Between Data Freshness and Update Cost in Information-update Systems," *International Conference on Computer Communications and Networks (ICCCN)*, July 2022.

12. Ding Zhang, Panneer Selvam, Parth H. Pathak, and Zizhan Zheng, "Networked Beamforming in Dense mmWave WLANs," *International Workshop on Mobile Computing Systems and Applications (HotMobile)*, Mar. 2022.

13. Tianyi Xu*, Ding Zhang, Parth H. Pathak and Zizhan Zheng, "Joint AP Probing and Scheduling: A Contextual Bandit Approach," *Military Communications Conference (MILCOM)*, Nov. 2021.

14. Wen Shen*, Henger Li*, and Zizhan Zheng, "Coordinated Attacks Against Federated Learning: A Multi-Agent Reinforcement Learning Approach," *ICLR 2021 Workshop on Security and Safety in Machine Learning Systems (SecML)*, May 2021 (selected for **travel award**).

15. Wen Shen*, Henger Li*, and Zizhan Zheng, "Learning to Attack Distributionally Robust Federated Learning," *NeurIPS-20 Workshop on Scalability, Privacy, and Security in Federated Learning (NeurIPS-SpicyFL)*, Dec. 2020 (selected for **oral presentation**).

16. Gamal Sallam, Zizhan Zheng, Jie Wu, and Bo Ji, "Robust Sequence Submodular Maximization," *Conference on Neural Information Processing Systems (**NeurIPS**)*, Dec. 2020. (Acceptance Rate = 20.1%)

17. Dan Peng, Zizhan Zheng, Linhao Luo, and Xiaofeng Zhang, "Structure Matters: Towards Generating Transferable Adversarial Images," *European Conference on Artificial Intelligence (**ECAI**)*, June 2020. (Acceptance Rate = 26.8%)

18. Henger Li*, Wen Shen*, and Zizhan Zheng, "Spatial-Temporal Moving Target Defense: A Markov Stackelberg Game Model," *International Conference on Autonomous Agents and Multi-Agent Systems (**AAMAS**)*, May 2020 (long paper). (Acceptance Rate = 23%)

19. Henger Li* and Zizhan Zheng, "Optimal Timing of Moving Target Defense: A Stackelberg Game Model," *Military Communications Conference (MILCOM)*, Nov. 2019.

20. Gamal Sallam, Zizhan Zheng, and Bo Ji, "Placement and Allocation of Virtual Network Functions: Multi-dimensional Case," *IEEE International Conference on Network Protocols (**ICNP**)*, Oct. 2019 (long paper). (Acceptance Rate = 14.2%)

21. Ding Zhang, Panneer Selvam Santhalingam, Parth Pathak, and Zizhan Zheng, "Characterizing Interference Mitigation Techniques in Dense 60 GHz mmWave WLANs," *International Conference on Computer Communications and Networks (ICCCN)*, July 2019.

22. Hao Fu, Zizhan Zheng, Sencun Zhu, Pransant Mohapatra, "Keeping Context In Mind: Automating Mobile App Access Control with User Interface Inspection," *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2019. (Acceptance Rate = 19.7%)

23. Dan Peng, Zizhan Zheng, and Xiaofeng Zhang, "Structure-Preserving Transformation: Generating Diverse and Transferable Adversarial Examples," *AAAI-19 Workshop on Artificial Intelligence for Cyber Security (AICS)*, Jan. 2019.

24. Ming Zhang, Zizhan Zheng, and Ness B. Shroff, "An Online Algorithm for Power-proportional Data Centers with Switching Cost," *IEEE Conference on Decision and Control (CDC)*, Dec. 2018.

25. Fang Liu, Zizhan Zheng, and Ness B. Shroff, "Analysis of Thompson Sampling for Graphical Bandits Without the Graphs," *Conference on Uncertainty in Artificial Intelligence (**UAI**)*, Aug. 2018.

26. Sungjin Im, Maryam Shadloo, and Zizhan Zheng (alphabetical order), "Online Partial Throughput Maximization for Multidimensional Coflow," *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2018. (Acceptance Rate = 19.2%)

27. Xiaotao Feng, Zizhan Zheng, Prasant Mohapatra, and Derya Cansever, "A Stackelberg Game and Markov Modeling of Moving Target Defense," *Conference on Decision and Game Theory for Security (GameSec)*, Oct. 2017.

28. Zhenzhi Qian, Fei Wu, Zizhan Zheng, Kannan Srinivasan and Ness B. Shroff, "Concurrent Channel Probing and Data Transmission in Full-duplex MIMO Systems," *ACM International Symposium on Mobile Ad Hoc Networking and Computing (**MobiHoc**)*, July 2017. (Acceptance Rate $<$ 17%)

29. Hao Fu, Zizhan Zheng, Somdutta Bose, Matt Bishop, and Prasant Mohapatra, "LeakSemantic: Identifying Abnormal Sensitive Network Transmissions in Mobile Applications," *IEEE International Conference on Computer Communications (**INFOCOM**)*, May 2017. (Acceptance Rate = 20.93%)

30. Xiaotao Feng, Zizhan Zheng, Derya Cansever, Ananthram Swami, and Prasant Mohapatra, "A Signaling Game Model for Moving Target Defense," *IEEE International Conference on Computer Communications (**INFOCOM**)*, May 2017. (Acceptance Rate = 20.93%)

31. Zizhan Zheng, Ness B. Shroff, and Prasant Mohapatra, " When to Reset Your Keys: Optimal Timing of Security Updates via Learning," *The Thirty-First AAAI Conference on Artificial Intelligence (**AAAI**)*, Feb. 2017. (Acceptance Rate $<$ 25%)

32. Xiaotao Feng, Zizhan Zheng, Derya Cansever, Ananthram Swami, and Prasant Mohapatra, "Stealthy Attacks with Insider Information: A Game Theoretic Model with Asymmetric Feedback," *Military Communications Conference (MILCOM)*, Nov. 2016.

33. Hao Fu, Hongxing Li, Zizhan Zheng, Pengfei Hu, and Prasant Mohapatra, "Trust Exploitation and Attention Competition: A Game Theoretic Model," *Military Communications Conference (MILCOM)*, Nov. 2016.

34. Hao Fu, Zizhan Zheng, Aveek Kumar Das, Parth H. Pathak, and Prasant Mohapatra, "Flow-Intent: Detecting Privacy Leakage from User Intention to Network Traffic Mapping," *IEEE International Conference on Sensing, Communication and Networking (SECON)*, June 2016.

35. Zizhan Zheng and Ness B. Shroff, "Online Multi-Resource Allocation for Deadline-Sensitive Jobs with Partial Values in Cloud," *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2016. (Acceptance Rate = 18.25%)

36. Eilwoo Baik, Amit Pande, Zizhan Zheng, and Prasant Mohapatra, "VSync: Cloud Based Video Streaming Service for Mobile Devices," *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2016. (Acceptance Rate = 18.25%)

37. Ming Zhang, Zizhan Zheng, and Ness B. Shroff, "A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources," *Conference on Decision and Game Theory for Security (GameSec)*, Nov. 2015.

38. Xiaotao Feng, Zizhan Zheng, Pengfei Hu, Derya Cansever, and Prasant Mohapatra, "Stealthy Attacks Meets Insider Threats: A Three-Player Game Model," *International Conference for Military Communications (MILCOM)*, Oct. 2015.

39. Yin Sun, Zizhan Zheng, Can Emre Koksal, Kyu-Han Kim, and Ness B. Shroff, "Provably Delay Efficient Data Retrieving in Storage Clouds," *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2015. (Acceptance Rate = 19%)

40. Ming Zhang, Zizhan Zheng, and Ness B. Shroff, “Stealthy Attacks and Observable Defenses: A Game Theoretic Model Under Strict Resource Constraints,” *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Dec. 2014.

41. Zizhan Zheng and Ness B. Shroff, “Online Welfare Maximization for Electric Vehicle Charging with Electricity Cost,” *International Conference on Future Energy Systems (**ACM e-Energy**)*, June 2014. (Acceptance Rate = 20%)

42. Shuang Li, Zizhan Zheng, Eylem Ekici, and Ness B. Shroff, “Maximizing Social Welfare in Operator-based Cognitive Radio Networks under Spectrum Uncertainty and Sensing Inaccuracy,” *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2013. (Acceptance Rate = 17%)

43. Yara Abdallah, Zizhan Zheng, Ness B. Shroff, and Hesham El Gamal, “On the Efficiency-vs-Security Tradeoff in the Smart Grid,” *IEEE Conference on Decision and Control (CDC)*, Dec. 2012.

44. Shuang Li, Zizhan Zheng, Eylem Ekici, and Ness B. Shroff, “Maximizing System Throughput Using Cooperative Sensing in Multi-Channel Cognitive Radio Networks,” *IEEE Conference on Decision and Control (CDC)*, Dec. 2012.

45. Zizhan Zheng and Ness B. Shroff, “Maximizing a Submodular Utility for Deadline Constrained Data Collection in Sensor Networks,” *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2012.

46. Shuang Li, Zizhan Zheng, Eylem Ekici, and Ness B. Shroff, “Maximizing System Throughput by Cooperative Sensing in Cognitive Radio Networks,” *IEEE International Conference on Computer Communications (**INFOCOM**)*, Mar. 2012. (Acceptance Rate = 18%)

47. Ying Zhang, Gang Huang, Xuanzhe Liu, Zizhan Zheng, and Hong Mei, “Towards Automatic Tuning of Adaptive Computations in Autonomic Middleware,” *International Workshop on Adaptive and Reflective Middleware (ARM)*, Nov. 2010.

48. Zizhan Zheng, Zhixue Lu, Prasun Sinha, and Santosh Kumar, “Maximizing the Contact Opportunity for Vehicular Internet Access,” *IEEE International Conference on Computer Communications (**INFOCOM**)*, Mar. 2010. (Acceptance Rate = 17.5%)

49. Paul N. Balister, Zizhan Zheng, Santosh Kumar, and Prasun Sinha, “Trap Coverage: Allowing Coverage Holes of Bounded Diameter in Wireless Sensor Networks,” *IEEE International Conference on Computer Communications (**INFOCOM**)*, Apr. 2009. (Acceptance Rate = 19.7%)

50. Zizhan Zheng, Prasun Sinha, and Santosh Kumar, “Alpha Coverage: Bounding the Interconnection Gap for Vehicular Internet Access,” *IEEE International Conference on Computer Communications (**INFOCOM**)*, mini-conference, Apr. 2009. (Acceptance Rate = 26.7%)

51. Kai-Wei Fan, Zizhan Zheng, and Prasun Sinha, “Steady and Fair Rate Allocation for Rechargeable Sensors in Perpetual Sensor Networks,” *ACM Conference on Embedded Networked Sensor Systems (**SenSys**)*, Nov. 2008. (Acceptance Rate = 16%)

52. Zizhan Zheng, Kai-Wei Fan, Prasun Sinha, and Yusu Wang, “Distributed Roadmap Aided Routing in Sensor Networks,” *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, short paper, Sep. 2008.

53. Zizhan Zheng and Prasun Sinha, “XBC: XOR-based Buffer Coding for Reliable Transmissions over Wireless Networks,” *International Conference on Broadband Communications, Networks, and Systems (IEEE BROADNETS)*, Sep. 2007.

54. Gang Huang, Tiancheng Liu, Hong Mei, Zizhan Zheng, Zhao Liu, and Gang Fan, “Towards Autonomic Computing Middleware via Reflection,” *International Computer Software and Applications Conference (COMPSAC)*, Sep. 2004.

Journal articles

1. Zhongdong Liu, Bin Li, Zizhan Zheng, Y. Thomas Hou, and Bo Ji, "Towards Optimal Tradeoff Between Data Freshness and Update Cost in Information-update Systems," *IEEE Internet of Things Journal (IoTJ)* (**Impact Factor: 9.471**), 2023.
2. Gamal Sallam, Zizhan Zheng, and Bo Ji, "Placement and Allocation of Virtual Network Functions: Multi-dimensional Case," *IEEE Transactions on Mobile Computing (TMC)* (**Impact Factor: 5.112**), 2022.
3. Hao Fu, Pengfei Hu, Zizhan Zheng, Aveek K. Das, Parth H. Pathak, Tianbo Gu, Sencun Zhu, and Prasant Mohapatra, "Towards Automatic Detection of NonfunctionalSensitive Transmissions in Mobile Applications," *IEEE Transactions on Mobile Computing (TMC)* (**Impact Factor: 5.112**), 20(10):3066-3080, 2020.
4. Ming Zhang, Zizhan Zheng, and Ness B. Shroff, "Defending Against Stealthy Attacks on Multiple Nodes with Limited Resources: A Game-Theoretic Analysis," *IEEE Transactions on Control of Network Systems (TCNS)* (**Impact Factor: 4.802**), 7(4):1665-1677, 2020.
5. Yara Abdallah, Zizhan Zheng*, Ness B. Shroff, and Hesham El Gamal, "The Impact of Stealthy Attacks on Smart Grid Performance: Tradeoffs and Implications," *IEEE Transactions on Control of Network Systems (TCNS)* (**Impact Factor: 4.802**), 4(4):886-898, 2017. (*corresponding author)
6. Zizhan Zheng, Zhixue Lu, Prasun Sinha, and Santosh Kumar, "Ensuring Predictable Contact Opportunity for Scalable Vehicular Internet Access On the Go," *IEEE/ACM Transactions on Networking (TON)* (**Impact Factor: 1.986**), 23(3):768-781, 2015.
7. Zizhan Zheng and Ness B. Shroff, "Submodular Utility Maximization for Deadline Constrained Data Collection in Sensor Networks," *IEEE Transactions on Automatic Control (TAC)* (**Impact Factor: 5.792**), 59(9):2400-2412, 2014.
8. Shuang Li, Zizhan Zheng, Eylem Ekici, and Ness B. Shroff, "Maximizing System Throughput by Cooperative Sensing in Cognitive Radio Networks," *IEEE/ACM Transactions on Networking (TON)* (**Impact Factor: 1.986**), 22(4):1245-1256, 2014.
9. Srikanth Hariharan, Zizhan Zheng, and Ness B. Shroff, "Maximizing Information in Unreliable Sensor Networks under Deadline and Energy Constraints," *IEEE Transactions on Automatic Control (TAC)* (**Impact Factor: 5.792**), 58(6):1416-1429, 2013.
10. Zizhan Zheng, Prasun Sinha, and Santosh Kumar, "Sparse WiFi Deployment for Vehicular Internet Access with Bounded Interconnection Gap," *IEEE/ACM Transactions on Networking (TON)* (**Impact Factor: 1.986**), 20(3):956-969, 2012.
11. Ren-Shiou Liu, Kai-Wei Fan, Zizhan Zheng, and Prasun Sinha, "Perpetual and Fair Data Collection for Environmental Energy Harvesting Sensor Networks," *IEEE/ACM Transactions on Networking (TON)* (**Impact Factor: 1.986**), 19(4):947-960, 2011.
12. Zizhan Zheng and Prasun Sinha, "Buffer Coding for Reliable Transmissions over Wireless Networks," *Elsevier Computer Communications (COMCOM)*, 32(1):111-123, 2009.

Posters and demos

1. Benjamin Sperisen, Stefano Barbieri, K. Brent Venable1, and Zizhan Zheng*, "Policy Design under Collusion," *ACM Conference on Economics and Computation (EC)*, poster, June 2018. (*presenter)
2. Somnath Mitra, Zizhan Zheng, Santanu Guha, Animikh Ghosh, Prabal Dutta, Bhagavathy Krishna, Kurt Plarre, Santosh Kumar, and Prasun Sinha, "Demo Abstract: An Affordable, Long-Lasting, and Autonomous Theft Detection and Tracking System," *ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Nov. 2009.

External Professional Activities

NSF Panelist

1. Division of Computer and Network Systems (CNS) review panelist, 2021, 2023

Organizing Committee Member

1. Travel Grant Co-Chair of The 23rd ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc), 2022
2. Registration Co-Chair of The 27th ACM Annual International Conference On Mobile Computing And Networking (MobiCom), 2021
3. Workshop Co-Chair of The Third ACM/IEEE Workshop on Security and Privacy in Edge Computing (EdgeSP), 2020

Technical Program Committee Member

1. AAAI Conference on Artificial Intelligence (AAAI), 2021-2024
2. International Joint Conference on Artificial Intelligence (IJCAI), 2020-2024
3. IEEE International Conference on Computer Communications (INFOCOM), 2017-2024
4. ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc), 2022-2024
5. International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt), 2021-2023
6. International Conference for Military Communications (MILCOM), 2016-2019, 2021
7. IEEE Wireless Communications and Networking Conference (WCNC), 2020
8. Conference on Decision and Game Theory for Security (GameSec), 2018
9. 13th IEEE International Conference on Sensing, Communication and Networking (SECON), 2016
10. International Conference on Distributed Computing and Networking (ICDCN), 2013, 2016
11. 10th International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (ALGOSENSORS), 2014
12. IEEE International Conference on Mobile Ad-hoc and Sensor Networks (MSN), 2012-2013
13. 7th International ICST Conference on Broadband Communications, Networks, and Systems (BROADNETS), 2010

Reviewer for Conferences

1. International Conference on Learning Representations (ICLR), 2022-2024
2. International Conference on Machine Learning (ICML), 2022, 2024
3. Conference on Neural Information Processing Systems (NeurIPS), 2021-2023
4. IEEE International Conference on Computer Communications (INFOCOM), 2011-2024
5. IEEE Conference on Decision and Control (CDC), 2014, 2018
6. IEEE International Conference on Distributed Computing Systems (ICDCS), 2011, 2014
7. IEEE International Conference on Sensing, Communication and Networking (SECON), 2011-2012
8. IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), 2009-2012
9. IEEE/ACM International Symposium on Quality of Service (IWQoS), 2011

Reviewer for Journals

1. IEEE Transactions on Information Forensics & Security (T-IFS)
2. IEEE Transactions on Parallel and Distributed Systems (TPDS)
3. IEEE/ACM Transactions on Networking (TON)
4. IEEE Journal on Selected Areas in Communications (JSAC)
5. IEEE Transactions on Automatic Control (TAC)
6. IEEE Transactions on Communications (TC)
7. IEEE Transactions on Cloud Computing (TCC)
8. IEEE Transactions on Control of Network Systems (TCNS)
9. IEEE Transactions on Dependable and Secure Computing (TDSC)
10. IEEE Transactions on Mobile Computing (TMC)
11. IEEE Transactions on Services Computing (TSC)
12. IEEE Transactions on Wireless Communications (TWC)
13. ACM Transactions on Sensor Networks (TOSN)
14. Elsevier Automatica
15. Elsevier Computer Communications
16. Elsevier Computer Networks

Internal Professional Services

1. Chair, PoP Search Committee, CS, Tulane, 2023-2024
2. Member, NTC Honor Board, Tulane, 2023 - present
3. Member, Graduate Studies Committee, CS, Tulane, 2022-present
4. Member, Undergraduate Studies Committee, CS, Tulane, 2017-2022
5. Member, Faculty Search Committee, CS, Tulane, 2017-present
6. Member, Nominating Committee, SSE, Tulane, 2021-2022
7. Member, Senate IT Committee, Tulane, 2020-2023
8. PhD Committee Chair: Henger Li, Tianyi Xu, Xiaolin Sun
9. PhD Committee Member: Ellis Fenske (2018), Haifeng Xia (2023), Cody Licorish, Andrea Martin, Akshay Mehra

Supervision

Postdoctoral Researchers

1. Wen Shen (PhD from UC Irvine), Fall 2019 - Summer 2021

PhD Students

1. Zixuan Liu, Fall 2023 - present
2. Xiaolin Sun, Fall 2020 - present
3. Tianyi Xu, Fall 2019 - present
4. Henger Li, Spring 2018 - present

Undergraduate Students

1. Caitlin Chen, Jason Min, and Max Curl, Fall 2023 - present, supervising CS coordinate major research on reinforcement learning and neuromorphic computing.
2. Jason Li and Rehan Mullan, Fall 2023 - present, supervising CS coordinate major research on reinforcement learning for Micromouse competitions.

3. Jake Johnston and Kelsey Peltz, Fall 2022 - Spring 2023, supervised CS coordinate major research on reinforcement learning for card games (selected for **audience favorite award**).
4. Caroline Casella and Lily Yee, Fall 2022 - Spring 2023, supervised CS coordinate major research on deep learning for multi-omics data.
5. Ajit Alapati, Christopher Callahan, Edward Moy, Eli Mendels, and Samuel Traylor, Fall 2021 - Spring 2022, supervised CS coordinate major research on robust and secure power grid (selected for **professionals' award**).
6. Dung Ngo, Fall 2021, supervised research on moving target defense (supported by an NSF REU grant).
7. Emma LeBouef, Fall 2020 - Spring 2021, supervised research on AI and security (Tulane Research & Innovation Award (TRIA) – supported by an NSF REU grant).
8. Rebekah Doochin, Kyle Strougo, and David Ziman, Fall 2020 - Spring 2021, supervised CS coordinate major research on contact tracing.
9. Grayson Buchholz and Joseph Pravder, Fall 2020 - Spring 2021, supervised CS coordinate major research on IoT security.
10. Sarper Tutuncuoglu, Fall 2020, supervised independent study on moving target defense.
11. Harrison Pratt and Tom Roginsky, Fall 2019 - Spring 2020, supervised CS coordinate major research on moving target defense (supported by an NSF REU grant).
12. Hanyu Lu, Fall 2019 - Spring 2020, supervised CS coordinate major research on federated machine learning.
13. Sarah Xing, Zachary Seymour, and Zekun Wu, Fall 2019 - Spring 2020, supervised CS coordinate major research on news aggregator.
14. Aleksa Todorovic, Alexandra Westlake, Vincent Sgarzi, Fall 2019 - Spring 2020, supervised CS coordinate major research on economic forecasting.
15. Zekun Wu, Summer 2019, supervised research on adversarial machine learning (supported by a CELT Summer Research Award for Faculty Mentored Undergraduate Research).
16. Matthew Fein and Noah Hendlish, Fall 2018 - Spring 2019, supervised CS coordinate major research on bot detection in social media.
17. Reid Bachman, Fall 2018 - Spring 2019, supervised CS coordinate major research on experimental study of moving target defense.
18. Theodore Steffens, Fall 2017 - Spring 2018, supervised CS coordinate major research on identifying vulnerabilities in smart home devices.
19. James McLennan, Fall 2017 - Spring 2018, supervised CS coordinate major research on understanding the impact of news shocks on the price of cryptocurrencies.
20. Daniel Barrach, Fall 2016 - Spring 2017, supervised CS coordinate major research on interdependent security games.
21. Daniel Verb, Fall 2016 - Spring 2017, supervised CS coordinate major research on cost analysis of drone delivery.

K-12 Students

1. Srija Tamidela (Patrick F. Taylor Science and Technology Academy in Jefferson Parish, Louisiana), Summer 2023, supervised summer research on reinforcement learning and its application in autonomous racing.
2. Jerry Chen (Haynes Academy in Metairie, Louisiana), Summer 2021, supervised summer research on the robustness of Q-learning.