Zizhan Zheng

CONTACT INFORMATION

Assistant Professor
Department of Computer Science
Tulane University

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

RESEARCH INTERESTS

- Reinforcement Learning
- Distributed AI (multi-agent learning, cooperative AI, game theory, etc.)
- Security and AI
- Networks

EDUCATION

PhD in Computer Sc. and Engg., The Ohio State University — June 2010

– Dissertation: "Sparse Deployment of Large Scale Wireless Networks for Mobile Targets"
– Committee: Prasun Sinha (chair), Ness B. Shroff, Yusu Wang

MS in Computer Science, Peking University, Peking, China — July 2005

BE in Polymer Sc. and Engg., Sichuan University, Chengdu, China — July 2002

– 1st rank in class (among 108 students)

PROFESSIONAL EXPERIENCE

Assistant Professor, Tulane University — July 2016 - present

Associate Specialist, University of California at Davis — Sept. 2014 - June 2016

– Supervisor: Prasant Mohapatra

Postdoctoral Researcher, The Ohio State University — Sept. 2010 - Aug. 2014

– Supervisor: Ness B. Shroff

TEACHING EXPERIENCE

Assistant Professor, Tulane University — July 2016 - present

– *CMPS/MATH 2170 Discrete Mathematics* (Fall 2016, Fall 2017, Fall 2018)
– *CMPS 4010 Capstone Project I* (Fall 2019)
– *CMPS 4660/6660 Reinforcement Learning* (Fall 2020)
– *CMPS 4750/6750 Computer Networks* (Spring 2017, Spring 2018, Spring 2020)
– *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

PROFESSIONAL ACTIVITIES

Research Grants

- **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), 08/15/2018-07/31/2021, Sole PI.
- **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, 10/01/2018-09/30/2021, Collaborative PI: Parth Pathak (GMU).
- **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.

Organizing Committee Member

1. Travel Grant Co-Chair of The 2022 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. IEEE International Conference on Computer Communications (INFOCOM), 2017-2022
2. International Conference on Learning Representations (ICLR), 2022
3. Conference on Neural Information Processing Systems (NeurIPS), 2021
4. International Joint Conference on Artificial Intelligence (IJCAI), 2020-2021
5. AAAI Conference on Artificial Intelligence (AAAI), 2021
6. International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt), 2021
7. International Conference for Military Communications (MILCOM), 2016-2019, 2021
8. IEEE Wireless Communications and Networking Conference (WCNC), 2020
9. Conference on Decision and Game Theory for Security (GameSec), 2018
10. 13th IEEE International Conference on Sensing, Communication and Networking (SECON), 2016
11. International Conference on Distributed Computing and Networking (ICDCN), 2013, 2016
12. 10th International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (ALGOSENSORS), 2014
13. IEEE International Conference on Mobile Ad-hoc and Sensor Networks (MSN), 2012-2013
14. 7th International ICST Conference on Broadband Communications, Networks, and Systems (BROADNETS), 2010

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

Reviewer for Conferences

1. IEEE International Conference on Computer Communications (INFOCOM), 2011-2015
2. IEEE International Conference on Sensing, Communication and Networking (SECON), 2011, 2012
3. IEEE International Conference on Distributed Computing Systems (ICDCS), 2011, 2014
4. IEEE Conference on Decision and Control (CDC), 2014, 2018
5. IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), 2009-2012
6. IEEE/ACM International Symposium on Quality of Service (IWQoS), 2011

HONERS AND AWARDS

- 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

PUBLICATIONS

Conference/Workshop papers

1. 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**).
2. 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**).
3. 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%)
4. 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%)
5. 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%)
6. Henger Li and Zizhan Zheng, "Optimal Timing of Moving Target Defense: A Stackelberg Game Model," *International Conference for Military Communications (MILCOM)*, Nov. 2019.
7. 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%)
8. 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.

9. 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%)
10. 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.
11. 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.
12. 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.
13. 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%)
14. 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.
15. 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 $< 17\%$)
16. 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%)
17. 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%)
18. 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 $< 25\%$)
19. Xiaotao Feng, Zizhan Zheng, Derya Cansever, Ananthram Swami, and Prasant Mohapatra, "Stealthy Attacks with Insider Information: A Game Theoretic Model with Asymmetric Feedback," *International Conference for Military Communications (MILCOM)*, Nov. 2016.
20. Hao Fu, Hongxing Li, Zizhan Zheng, Pengfei Hu, and Prasant Mohapatra, "Trust Exploitation and Attention Competition: A Game Theoretic Model," *International Conference for Military Communications (MILCOM)*, Nov. 2016.
21. Hao Fu, Zizhan Zheng, Aveek Kumar Das, Parth H. Pathak, and Prasant Mohapatra, "FlowIntent: Detecting Privacy Leakage from User Intention to Network Traffic Mapping," *IEEE International Conference on Sensing, Communication and Networking (SECON)*, June 2016.
22. 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%)
23. 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%)
24. 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.

25. 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.
26. 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%)
27. 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.
28. 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%)
29. 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%)
30. 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.
31. 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.
32. 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.
33. 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%)
34. 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.
35. 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%)
36. 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%)
37. 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%)
38. 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%)
39. 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.
40. 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.

41. 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. Hao Fu, Pengfei Hu, Zizhan Zheng, Aveek K. Das, Parth H. Pathak, Tianbo Gu, Sencun Zhu, Prasant Mohapatra, "Towards Automatic Detection of NonfunctionalSensitive Transmissions in Mobile Applications," *IEEE Transactions on Mobile Computing (TMC)*, 2020.
2. 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)*, 2020.
3. 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)*, 4(4), pp. 886-898, 2017. (*corresponding author)
4. 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)*, 23(3):768-781, 2015.
5. Zizhan Zheng and Ness B. Shroff, "Submodular Utility Maximization for Deadline Constrained Data Collection in Sensor Networks," *IEEE Transactions on Automatic Control (TAC)*, 59(9):2400-2412, 2014.
6. 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)*, 22(4):1245-1256, 2014.
7. 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)*, 58(6):1416-1429, 2013.
8. Zizhan Zheng, Prasun Sinha, and Santosh Kumar, "Sparse WiFi Deployment for Vehicular Internet Access with Bounded Interconnection Gap," *IEEE/ACM Transactions on Networking (TON)*, 20(3):956-969, 2012.
9. 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)*, 19(4):947-960, 2011.
10. 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.

SUPERVISION

Postdoctoral Researchers

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

PhD Students

1. Henger Li, Spring 2018 - present

2. Tianyi Xu, Fall 2019 - present
3. Xiaolin Sun, Fall 2020 - present

Dissertation Committees

1. Ellis Fenske, Tulane University, Fall 2017 - Spring 2018
2. Andrea Martin, Tulane University, Fall 2018 - Spring 2019
3. Cody Licorish, Tulane University, Spring 2019 - present

Undergraduate Students

1. Emma LeBouef, Fall 2020 - present, supervising research on AI and security (Tulane Research & Innovation Award (TRIA)).
2. Rebekah Doochin, Kyle Strougo, David Ziman, Fall 2020 - Spring 2021, supervising CS coordinate major research on contact tracing.
3. Grayson Buchholz and Joseph Pravder, Fall 2020 - Spring 2021, supervising CS coordinate major research on IoT security.
4. Harrison Pratt and Tom Roginsky, Fall 2019 - Spring 2020, supervised CS coordinate major research on moving target defense.
5. Hanyu Lu, Fall 2019 - Spring 2020, supervised CS coordinate major research on federated machine learning.
6. Sarah Xing, Zachary Seymour, and Zekun Wu, Fall 2019 - Spring 2020, supervised CS coordinate major research on news aggregator.
7. Aleksa Todorovic, Alexandra Westlake, Vincent Sgarzi, Fall 2019 - Spring 2020, supervised CS coordinate major research on economic forecasting.
8. Zekun Wu, Summer 2019, supervised research on adversarial machine learning (supported by a CELT Summer Research Award for Faculty Mentored Undergraduate Research).
9. Matthew Fein and Noah Hendlish, Fall 2018 - Spring 2019, supervised CS coordinate major research on bot detection in social media.
10. Reid Bachman, Fall 2018 - Spring 2019, supervised CS coordinate major research on experimental study of moving target defense.
11. Theodore Steffens, Fall 2017 - Spring 2018, supervised CS coordinate major research on identifying vulnerabilities in smart home devices.
12. James McLennan, Fall 2017 - Spring 2018, supervised CS coordinate major research on understanding the impact of news shocks on the price of cryptocurrencies.
13. Daniel Barrach, Fall 2016 - Spring 2017, supervised CS coordinate major research on interdependent security games.
14. Daniel Verb, Fall 2016 - Spring 2017, supervised CS coordinate major research on cost analysis of drone delivery.