Kai Zhou

Postdoctoral Research Associate
Department of Computer Science and Engineering
Washington University in St. Louis

Campus Box 1045, 1 Brookings Drive
St. Louis, MO, 63130
503-676-4760
Website
zhoukai@wustl.edu

December 5, 2019

Research Overview

My research focuses on **data security and privacy** in a broad spectrum of application domains, such as *social network analysis*, *machine learning*, and *mobile cloud computing*. Topics that interest me include secure and verifiable computation, adversarial robustness of learning systems, game-theoretical modeling.

Selected research projects:

- *Adversarial social network analysis* [1,9,10,20]
- *Adversarial robustness of graphical models in machine learning* [19]
- *Secure and privacy-preserving computation outsourcing in mobile cloud computing* [2 - 6, 10 - 13]
- *Equilibrium analysis in graphical games* [8]

Positions

- Washington University in St. Louis · · · (Aug. 2018 - present)
  Postdoctoral Research Associate
  Supervisor: Prof. Yevgeniy Vorobeychik
- Vanderbilt University · · · (May 2018 - Aug. 2018)
  Postdoctoral Research Associate
  Supervisor: Prof. Yevgeniy Vorobeychik
- Michigan State University · · · (Aug. 2013 - May 2018)
  Research Assistant
  Advisor: Prof. Jian Ren

Education

- **Ph.D.** in *Electrical Engineering*, Michigan State University, May 2018
  Advisor: Prof. Jian Ren
  Dissertation: "*Trade-Offs Among Data Security, Usability, and Complexity in Mobile Cloud Computing*"
- **B.S.** in *Electronic and Information Engineering*, Shanghai Jiao Tong University, China, June 2013
  Major GPA: $3.89/4.0$ ($90.5/100$, ranking top 5%)

Publications

Journal Articles

[1] **How to Hide One's Relationships from Link prediction Algorithms**
Marcin Waniek, Kai Zhou, Yevgeniy Vorobeychik, Esteban Moro, Tomasz P. Michalak, and Talal Rahwan
Scientific Reports, 9(1), pp. 1-10, 2019.

[2] **P-mod: Secure Privilege-based Multilevel Organizational Data Sharing in Cloud Computing**
Ehab Zaghloul, Kai Zhou, and Jian Ren
IEEE Transactions on Big Data, 2019.

[3] **Passbio: Privacy-preserving User-centric Biometric Authentication**
Kai Zhou and Jian Ren
IEEE Transactions on Information Forensics and Security, 2018.

[4] **CASO: Cost-Aware Secure Outsourcing of General Computational Problems**
Kai Zhou and Jian Ren
IEEE Transactions on Services Computing, 2018.

[5] **Privacy Characterization and Quantification in Data Publishing**
Mohamed H. Afifi Ibrahim, Kai Zhou, and Jian Ren
IEEE Transactions on Knowledge and Data Engineering, 30(9), pp. 1756-1769, 2018.

[6] **ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing**
Kai Zhou, M. H. Afifi, and Jian Ren
IEEE Transactions on Information Forensics and Security, 12(11), pp. 2518-2531, 2017

[7] **CDMA System Design and Capacity Analysis under Disguised Jamming**
Tianlong Song, Kai Zhou, and Tongtong Li
IEEE Transactions on Information Forensics and Security, 11(11), pp. 2487-2498, 2016.

Conference Proceedings

[8] **Computing Equilibria in Binary Networked Public Goods Games**
Sixie Yu*, Kai Zhou*, P. Jeffrey Brantingham, and Yevgeniy Vorobeychik (*equal contribution)
34th AAAI Conference on Artificial Intellegence (AAAI), 2020, to appear.

[9] **Adversarial Robustness of Similarity-Based Link Prediction**
Kai Zhou, Tomasz P. Michalak , and Yevgeniy Vorobeychik
19th IEEE International Conference on Data Mining (ICDM), Nov. 2019.
regular paper, acceptance rate: 95/1064, 9.08%.
Invited for publication in Knowledge and Information Systems as one of best papers in ICDM'19

[10] **Attacking Similarity-Based Link Prediction in Social Networks**
Kai Zhou, Tomasz P. Michalak, Talal Rahwan, Marcin Waniek, and Yevgeniy Vorobeychik
International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2019.

[11] **Security and Privacy Enhancement for Outsourced Biometric Identification**
Kai Zhou and Jian Ren
IEEE Global Communications Conference (GLOBECOM), Dec. 2018.

[12] **Secure Fine-grained Access Control of Mobile User Data through Untrusted Cloud**
Kai Zhou and Jian Ren
25th International Conference on Computer Communication and Networks (ICCCN), Aug. 2016.

[13] **Secure Outsourcing of Scalar Multiplication on Elliptic Curves**
Kai Zhou and Jian Ren
IEEE International Conference on Communications (ICC), May 2016.

[14] **LinSOS: Secure Outsourcing of Linear Computations based on Affine Mapping**
Kai Zhou and Jian Ren
IEEE International Conference on Communications (ICC), May 2016.

[15] **Robust CDMA Receiver Design under Disguised Jamming**
Kai Zhou, Tianlong Song, Jian Ren, and Tongtong Li
IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Mar. 2016.

[16] **Security and efficiency trade-offs for cloud computing and storage**
Jian Li, Kai Zhou, and Jian Ren
IEEE Resilience Week (RWS), Aug. 2015.

[17] **A Theoretical Framework for Mitigating Delay in 3D Wireless Data Center Networks**
Kai Zhou, Xiaohua Tian, and Yu Cheng
IEEE International Conference on Communications (ICC), Jun. 2013.

[18] **Spatial Reuse in Spectrum Sharing: A Matrix Spatial Congestion Games approach**
Kai Zhou, Gaofei Sun, Xinbing Wang, and Zhiyong Feng
IEEE International Conference on Communications in China (ICCC), Aug. 2012.

Papers in submission

[19] **Robust Collective Classification against Structural Attacks**
Kai Zhou and Yevgeniy Vorobeychik
In submission.

[20] **Blocking Adversarial Influence in Social Networks**
Feiran Jia, Kai Zhou, Charles Kamhoua, and Yevgeniy Vorobeychik
In submission.

Professional Activities

- Talks:

  Adversarial Robustness of Similarity-Based Link Prediction
  19th IEEE International Conference on Data Mining (ICDM)
  November 2019, Beijing, China

Robust Collective Classification against Structural Attacks
Annual meeting of Multidisciplinary University Research Initiative (MURI)
July 2019, University of Michigan, MI, USA

Attacking Similarity-Based Link Prediction in Social Networks
AI Cybersecurity Workshop
June 2019, University of Maryland, MD, USA

Adversarial Link Prediction in Social Networks
Annual meeting of Multidisciplinary University Research Initiative (MURI)
July 2018, University of Michigan, MI, USA

Secure Outsourcing of Scalar Multiplication on Elliptic Curves
IEEE International Conference on Communications (ICC)
May 2016, Kuala Lumpur, Malaysia

LinSOS: Secure Outsourcing of Linear Computations based on Affine Mapping
IEEE International Conference on Communications (ICC)
May 2016, Kuala Lumpur, Malaysia

- Reviews:

  IEEE Transactions on Mobile Computing, IEEE Transactions on Cloud Computing, IEEE Transactions on Signal Processing, ACM Transactions on Sensor Networks, ELSEVIER Pervasive and Mobile Computing, Springer Artificial Intelligence Review

  AAAI, AAMAS, Wine, INFOCOM, GlOBECOM, ICC, ICNC, TrustCom

Teaching

- *Mentoring*, Feiran Jia (now master student at Washington University in St. Louis)
- *Guest lecture*, "Adversarial Social Network Analysis" for *CSE 544T Special Topics in Computer Science Theory (Adversarial AI)* at Washington University in St. Louis
- *Homework design*, for *CSE 411A AI and Society* at Washington University in St. Louis

References

Jian Ren
Associate Professor
Electrical and Computer Engineering
Michigan State University
renjian@egr.msu.edu

Yevgeniy Vorobeychik
Associate Professor
Computer Science and Engineering
Washington University in St. Louis
yvorobeychik@wustl.edu

Tongtong Li
Associate Professor
Electrical and Computer Engineering
Michigan State University
tongli@egr.msu.edu