Curriculum Vitae for Professor Wanlei Zhou

January 25, 2024

Personal Details

Name:	Wanlei ZHOU
Position:	Vice Rector (Academic Affairs), Professor and Dean of Faculty of Data Science
Organisation:	City University of Macau, Taipa, Macau SAR.
E-mail:	wlzhou@cityu.mo; wanlei.zhou@gmail.com
Phones:	+853-85902788 (O); +853-62171999 (Macao M); +61-418315866 (Aus M)
Citizenship:	Australian

Academic Qualifications

2002:	DSc. (Higher Doctorate), Deakin University, Melbourne, Australia.
1991:	PhD (Comp. Sci.), The Australian National University, Canberra, Australia (Thesis Title: Network services for distributed computing; Supervisor: Dr Brian Molinari).
1984:	MEng (Comp. Sci. & Eng.), Harbin Institute of Technology, Harbin, China.
1982:	BEng (Comp. Sci. & Eng.), Harbin Institute of Technology, Harbin, China.

Employment Summary

- **November 2020 – : Vice Rector (Academic Affairs) and Dean of Faculty of Data Science, City University of Macau, Taipa, Macau SAR, China.**
- **June 2018 – November 2020: Professor and Head of School, School of Computer Science, University of Technology Sydney, Building 11, 81 Broadway, Ultimo, NSW 2007, Australia.**
- **January 1994 – May 2018: Deakin University, Australia, from Lecturer to Senior Lecturer, to Associate Professor, to Professor, to Head of School, and Associate Dean.**
  - January 2016 – May 2018: **Alfred Deakin Professor** (3/10/2013), **Chair of Information Technology** (2002 – 31/5/2018), **Associate Dean (International Research Engagement)** of Faculty of Science, Engineering and Built Environment (1/1/2016 – 31/52018), Research Director of Strategic Research Centre in Cyber Security (1/8/2017 – 31/5/2018), Deakin University, Melbourne Campus, Burwood, VIC 3125, Australia.
  - January 2015 - December 2015: Visiting Professor, Department of Computing, The Hong Kong Polytechnic University (Jan-Jun 2015); Visiting Professor, School of Computing, National University of Singapore (Jul- Dec 2015); on sabbatical leave from Deakin University.
  - January 2009 – January 2015: **Professor of Information Technology and Head**, School of Information Technology, Deakin University, Melbourne Campus, Burwood, VIC 3125, Australia.
  - May 2006 – December 2008: **Professor of Information Technology and Associate Dean (International)**, Faculty of Science and Technology, Deakin University, Melbourne Campus, Burwood, VIC 3125, Australia.
  - January 2002 – April 2006: **Professor of Information Technology and Head**, School of Information Technology, Deakin University, Melbourne Campus, Burwood, VIC 3125, Australia.
  - January 1999 – December 2001: Associate Professor and Deputy Head, School of Computing and Mathematics, Deakin University, Melbourne Campus, Burwood, VIC 3125, Australia.
  - January 1994 – December 1998: Lecturer then Senior Lecturer, School of Computing and Mathematics, Deakin University, Geelong Campus, Geelong, VIC 3217, Australia. (June-December 1998: Visiting Researcher in Department of Computer Science, City University of Hong Kong).
- January 1992 - January 1994: Lecturer, Department of Information Systems and Computer Science, National University of Singapore, Kent Ridge, Singapore.

- January 1991 - January 1992: Lecturer, Department of Computer Technology, Monash University, Caulfield Campus, Melbourne, VIC 3145, Australia.
- November 1987 - December 1990: PhD study in The Australia National University, Canberra, Australia
- March 1989 - August 1989: System Programmer, Domain Distributed Service, Apollo Computer Inc. (merged with Hewlett-Packard in June 1989), Chelmsford, MA, USA.
- February 1987 - November 1987: Visiting Scholar, Department of Computer Science, University of New South Wales, Sydney, NSW 2033, Australia.
- August 1984 - February 1987: Lecturer, Department of Computer Science, University of Electronic Science and Technology of China, Chengdu, China.

Professional Services

- Associate Editor: IEEE Transactions on Information Forensics and Security (2013-2016)
- Editor-in-Chief: International Journal of Computers and Applications (published by Taylor&Francis, 2015-2017)
- Member of the ARC College of Experts, 2017-2020.
- Senior Member, IEEE

Research Interests

- Security and privacy,
- distributed and parallel processing systems,
- data analytics and machine learning, and
- e-learning

Major Research Grants in Recent Years (since 2012)

1. 2023-2025: **Wanlei Zhou** at al., "Privacy-Preserved Cross-border Data Collaborative Management for Credit Investigation", FDCT-NSFC Joint Scientific Research Fund, Grant No. 0051/2022/AFJ. MOP$1.6 million.
2. 2019-2022: Tianqing Zhu, Bo Liu, **Wanlei Zhou** and Mengmeng Yang, ARC Linkage Project LP180101150: "Privacy preservation for personalised smart device". Total: $470,000 (ARC $320,000; Industry: $150,000).
3. 2019-2021: **Wanlei Zhou**, Tianqing Zhu and Phillip Yu, Australian Research Council (ARC) Discovery Project, DP190100981: “Enhancing privacy preserving in dynamic cyberspace,” Total: $314,000.
4. 2018-2020: **Wanlei Zhou** and Shui Yu, ARC Discovery Project DP180102828: "Enhancing information credibility using mathematical prediction," Total: $372,725.
5. 2017-2020: **Wanlei Zhou**, Tianqing Zhu, Gang Li and Paul Kidd, ARC Linkage Project LP170100123: "A provable privacy-preserving data sharing system for the cloud environment". Total: $540,000 (ARC $300,000; Industry: $240,000).
6. 2017-2020: Yong Xiang; **Wanlei Zhou**; Gleb Beliakov; Longxiang Gao, ARC Linkage Project LP170100458, “Novel audio watermarking techniques for tracing multimedia piracy”. Total: $400,000 (ARC $310,000.00; Industry $90,000).
7. 2017-2020: Yang Xiang; Jun Zhang; **Wanlei Zhou**; Sheng Wen; Shigang Liu, ARC Linkage Project LP170100924, “Developing an effective defence to cyber-reputation manipulation attacks”. Total: $639,000 (ARC: $450,000.00; Industry: $189,000).
8. 2014-2016, **Wanlei Zhou** and Yang Xiang, ARC Discovery Project DP140103649, "Modelling and defence against malware propagation," Total ARC: A$330,000.
9. 2012-2015, Yang Xiang, **Wanlei Zhou**, Vijay Varadharajan, and Jonathan Oliver, ARC Linkage Project LP120200266, "Developing an active defence system to identify malicious domains and websites," Total: $330,000 (ARC: $240,000. Industry: $90,000).
10. 2010-2012: **Wanlei Zhou** and Yang Xiang, Australian Research Council Linkage Grant, LP100100208, "An active approach to detect and defend against peer-to-peer botnets," Total: $192,160 (ARC: $159,160. Industry: $33,000).
11. 2010-2012: **Wanlei Zhou** and Robin Doss, ARC Linkage Grant, LP100100816, "Secure and Efficient Communication in Vehicle-based Radio Frequency Identification Systems," Total: $192,160 (ARC:

$159,160. Industry: $33,000).

12. 2010-2012: Yang Xiang, **Wanlei Zhou**, and Yong Xiang, ARC Discovery Grant, DP1095498, "Tracing real Internet attackers through information correlation," Total: ARC: A$220,000.

Keynote Speeches and Tutorials in International Conferences (since 2012)

1. Wanlei Zhou, Keynote Address: “Adversarial Attacks and Defenses in Deep Learning: from a Perspective of Cybersecurity”, The 11th Intelligent Search in Cyberspace & Forum of Future Data. Beijing, China, July 6-8, 2023.
2. 周万雷, “从语言模型到ChatGPT - 对人工智能模型的理解和应用, 金银湾未来科技沙龙（第十四期）——网信办专场”, 珠海，2023年6月29日.
3. 周万雷, “澳门城市大学的数字化变革”, 2023甬港澳教育合作论坛暨数字教育高峰论坛, 香港, 2023年6月27日
4. 周万雷, “建设大数据与智能技术支撑下的新型都会大学”, 首届大湾区数智化赋能大教育高峰论坛, 深圳, 2023 年5 月27 日
5. Wanlei Zhou, Keynote Address: “Balancing Privacy, Fairness, and Accuracy in Machine Learning Models: A Case Study from Cybersecurity Perspective”, The 2002 International Symposium on Data Security and Privacy Protection, Xi'An, China, December 10, 2022.
6. Wanlei Zhou, Keynote Address: “Mitigate the Impact of Advanced Persistent Threats”, The 5th International Conference on Big Earth Data (BED2022), Wuhan, China, November 12-13, 2022.
7. Wanlei Zhou, Keynote Address: “Using Game Theoretic Approach to Defend against Advanced Persistent Threats”, The 15th China Computer Networks and Information Security Conference & 2022 International Network Security Seminar, Zhengjiang, China, October 25-27, 2022.
8. Wanlei Zhou, Keynote Address: “Dealing with malicious agents in intelligent multi-agent applications”, The First International Conference on Ubiquitous Security (UbiSec 2021), Guangzhou, China, December 28 - 31, 2021.
9. Wanlei Zhou, Keynote Address: “Countermeasures to Defend against Advanced Persistent Threats”, The 8th International Conference on Data Science: Advancement of Data Science and Blockchain, Nanjing, China, November 19-21, 2021.
10. Wanlei Zhou, Keynote Address: “Threats and Defenses in Data Security Games”, The 7th International Conference on Data Science (ICDCS 2020), Chengdu, China. Dec. 26-27, 2020.
11. Wanlei Zhou, Keynote Address: “Threats and Defenses in Cyber Security: Using Game theory to Deceive Cyber Adversaries”, University Alliance of the Silk Road (UASR) Events 2020 - Security for Cyber Space Workshop, Xi'An, China, November 25, 2020.
12. Wanlei Zhou, Keynote Address: “AI Security and Privacy: Case Studies in Dealing with Malicious Agents”, International Conference on Security and Privacy in Digital Economy (SPDE 2020), Quzhou, Zhejiang, China. Oct. 30 – Nov. 1, 2020.
13. Wanlei Zhou, Keynote Address: "AI Security: A Case in dealing with malicious agents", The 19th International Conference on Architectures and Algorithms for Parallel Processing (ICA3PP 2019), 9-11 December 2019, Melbourne, Australia.
14. Wanlei Zhou, Keynote Address: “Privacy in Wireless Internet of Things", The 11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019), 11-13 December 2019, Sydney, Australia.
15. Wanlei Zhou, Keynote Address: "Enhancing privacy-preserving through differential privacy", The 10th International Symposium on Information and Communication Technology (SoICT 2019), 4-6/12/2019, Hanoi, Vietnam.
16. Wanlei Zhou, Keynote Address: "AI Security: Impact and Applications", The 5th International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2019), Guangzhou, China, November 12-15, 2019.
17. Wanlei Zhou, Keynote Address: " Trust, Security and Privacy in Low-Cost RFID Systems", The 13th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2019), 3-5 July 2019, Sydney, Australia.
18. Wanlei Zhou, Keynote Address: "Enhancing Location Privacy in the Digital Age: Selected Application Cases", 2019 International Conference on Data Science (ICDS) 2019, May 18-19, 2019, Ningbo, China.
19. Wanlei Zhou, Keynote Address: "Location Privacy and its Applications", International Symposium on

Parallel, Architectures, Algorithms and Programming (PAAP'18). December 26-18, 2018, Taipei.

20. Wanlei Zhou, Keynote Address: "Location Privacy-preserving in Crowdsensing System", 2018 IEEE Smart World Congress, October 8-12, 2018, Guangzhou, China.
21. Wanlei Zhou, Keynote Address: "Preserving privacy in the digital age: Differential privacy and its applications", International Conference on Machine Learning and Data Engineering (iCMLDE2018), 03-07 December 2018, Sydney, Australia.
22. Wanlei Zhou, Keynote Address: "Privacy-preserving in Location-Based Services", The 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2018), during 11 - 13 December 2018, Melbourne, Australia.
23. Wanlei Zhou, Keynote Address: "Trust, Security and Privacy in Mobile RFID Systems", Inscrypt 2018: The 14th International Conference on Information Security and Cryptology, 14th December 2018 - 16th December 2018, Fuzhou, China.
24. Wanlei Zhou, Keynote Address: "Enhancing Privacy in Location-Based Services", The 16th IEEE International Conference On Trust, Security and Privacy In Computing And Communications (IEEE TrustCom-17), Sydney, Australia, August 1 - 4, 2017.
25. Wanlei Zhou and Tianqing Zhu, Tutorial: "Preserving privacy in the digital age: Differential privacy and its applications", The 12th International Conference on Green, Pervasive and Cloud Computing, May 11-14, 2017, Amalfi Coast, Italy.
26. Wanlei Zhou, Keynote Address: "Recommendations based on Offline Data Processing: Techniques, Features, and Challenges", The 16th IEEE International Conference on Computer and Information Technology (IEEE CIT 2016), Fiji, 7-10 December 2016.
27. Wanlei Zhou, Keynote Address: "Security and Privacy in Passive Mobile RFID Systems", 21st Australasian Conference on Information Security and Privacy, Melbourne, Australia, 4-6 July 2016.
28. Wanlei Zhou, Keynote Address: "Identifying Propagation Sources in Social Networks", International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2015), held in Hangzhou, China, 16-18 November, 2015
29. Wanlei Zhou and Tianqing Zhu, Tutorial: "Differential Privacy Techniques for Correlated Dataset", The 15th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2015), in Zhangjiajie, China, November 18-20, 2015
30. Wanlei Zhou, Keynote Address: "Identifying Propagation Sources and Modeling Propagation Dynamics in Networks", The 15th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2015), in Zhangjiajie, China, November 18-20, 2015
31. Gang Li, Tianqing Zhu and Wanlei Zhou, Tutorial: "Differential Privacy and Its Applications", The 19th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2015), in Ho Chi Minh City, Viet Nam, May 19-22, 2015.
32. Wanlei Zhou, Keynote Address: "Modelling the Propagation of Worms and Rumours in Networks", The 2014 International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-14), 24-26 September, 2014. Beijing, China.
33. Wanlei Zhou, Keynote Address: "Recommendation Techniques: Recent Progress and Challenges", ICA3PP 2014/U-Science 2014, August 24-27, 2014. Dalian, China.
34. Wanlei Zhou, Keynote Address: "Dealing with Malware Propagation: Modelling and Defence Strategies", The 6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications (ACSA-14), April 23-25, 2014, Jeju, Korea.
35. Wanlei Zhou, Keynote Address: "Authentication, Privacy and Ownership Transfer in Mobile RFID Systems", The 2013 World Ubiquitous Science Congress (U-Science2013): 2013 IEEE International Conference on PICom / ScalCom / DASC / EmbeddedCom, December 21st - 22nd, 2013, Chengdu, Sichuan, China.
36. Wanlei Zhou, Keynote Address: "Recommendation Techniques based on Off-line Data Processing", The 2013 Conference of Hunan Computer Society, held in Zhangjiajie, Hunan, China during November 14-15, 2013.
37. Wanlei Zhou, Keynote Address: "Recommendation Techniques based on Off-line Data Processing", The 9th International Conference on Semantics, Knowledge and Grids, held in Beijing, China during Oct 3, 2013 - Oct 4, 2013.
38. Wanlei Zhou, Keynote Address: "Authentication, Privacy and Ownership Transfer in Mobile RFID Systems", The 7th International Conference on Network and System Security, Madrid, Spain, 3-4 June, 2013.
39. Wanlei Zhou, Keynote Address: "Dealing with Worm Propagation: Modelling and Defence Strategies",

The Thirteenth International Conference on Parallel and Distributed Computing, Applications and Technologies, Dec 14, 2012 - Dec 16, 2012, Beijing, China.

40. Wanlei Zhou, Keynote Address: "Traceback of Distributed Denial-of-Service (DDoS) Attacks", The 6th International Conference on Network and System Security, November 21-23, 2012, Wu Yi Shan, Fujian, China.
41. Wanlei Zhou, Keynote Address: "Trust Management and Privacy Preservation in Wireless and Sensor Networks", The 9th IEEE International Conference on Ubiquitous Intelligence and Computing, Sep 4-7, 2012, Fukuoka, Japan
42. Wanlei Zhou, Keynote Address: "Detection of and Defense Against Distributed Denial-of-Service (DDoS) Attacks", The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-12), Liverpool, UK, June 25-27, 2012.
43. Wanlei Zhou, Keynote Address: "The Microcosmic Model of Worm Propagation", The First International Workshop on Network Forensics, Security and Privacy (NFSP 2012), Macau, June 18-21, 2012.

Journal Publications (since 2012)

I have published more than 400 papers in international journals and international conference proceedings (including book chapters). As shown below, according to Google Scholar (accessed on 25/01/2023), I have over 14,000 citations and an H-Index of 64. Here I only list my recent **journal publications from 2012**. Detailed publication lists can be found from Google Scholar or dblp computer science bibliography listing.

- **2024 accepted/published articles**

1. Heng Xu, Tianqing Zhu, Lefeng Zhang, Wanlei Zhou, Philip S. Yu, "Machine Unlearning: A Survey". **ACM Computing Surveys**, 56(1): 9:1-9:36 (2024)
2. Huiqiang Chen, Tianqing Zhu, Tao Zhang, Wanlei Zhou, Philip S. Yu, "Privacy and Fairness in Federated Learning: On the Perspective of Tradeoff". **ACM Computing Surveys**, 56(2): 39:1-39:37 (2024)
3. Hui Sun, Tianqing Zhu, Wenhan Chang, Wanlei Zhou, "A two-stage model extraction attack on GANs with a small collected dataset," **Computers & Security**, Volume 137, 2024, 103634, https://doi.org/10.1016/j.cose.2023.103634.
4. Chi Liu, Huajie Chen, Tianqing Zhu, Jun Zhang, Wanlei Zhou, "Making DeepFakes more spurious: evading deep face forgery detection via trace removal attack", accepted by **IEEE Transactions on Dependable and Secure Computing,** early access: https://ieeexplore.ieee.org/document/10035845
5. Minghao Wang, Tianqing Zhu, Xuhan Zuo, Dayong Ye, Shui Yu, Wanlei Zhou, "Public and Private Blockchain Infusion: A Novel Approach to Federated Learning," accepted by **IEEE Internet of Things Journal**, doi: 10.1109/JIOT.2024.3360129. https://ieeexplore.ieee.org/document/10416917
6. Guangsheng Zhang, Bo Liu, Tianqing Zhu, Ming Ding, Wanlei Zhou, "PPFed: A Privacy-Preserving and Personalized Federated Learning Framework," accepted by **IEEE Internet of Things Journal,** doi: 10.1109/JIOT.2024.3360153. https://ieeexplore.ieee.org/document/10416913
7. Dayong Ye, Tianqing Zhu, Kun Gao, Wanlei Zhou, "Defending against Label-only Attacks via Meta-Reinforcement Learning," accepted by **IEEE Transactions on Information Forensics and Security**, doi: 10.1109/TIFS.2024.3357292. https://ieeexplore.ieee.org/document/10411933
8. Minghao Wang, Tianqing Zhu, Xuhan Zuo, Dayong Ye, Shui Yu, Wanlei Zhou, "Blockchain-Based Gradient Inversion and Poisoning Defense for Federated Learning," accepted by **IEEE Internet of Things Journal**, doi: 10.1109/JIOT.2023.3347899. https://ieeexplore.ieee.org/document/10375767
9. Congcong Zhu, Dayong Ye, Tianqing Zhu, Wanlei Zhou, "Location-Based Real-Time Updated Advising Method for Traffic Signal Control," accepted by **IEEE Internet of Things Journal**, doi: 10.1109/JIOT.2023.3342480. https://ieeexplore.ieee.org/document/10356649
10. Minghao Wang; Tianqing Zhu; Xuhan Zuo; Dayong Ye; Shui Yu; Wanlei Zhou, "Blockchain Empowered Multi-Agent Systems: Advancing IoT Security and Transaction Efficiency," accepted by **IEEE Internet of Things Journal**, doi: 10.1109/JIOT.2023.3329961. https://ieeexplore.ieee.org/document/10316248
11. Guangsheng Zhang, Bo Liu, Huan Tian, Tianqing Zhu, Ming Ding, Wanlei Zhou, "How Does a Deep Learning Model Architecture Impact Its Privacy? A Comprehensive Study of Privacy Attacks on CNNs and Transformers," Accepted by **The 33rd USENIX Security Symposium (USENIX Security '24)**, to be held in August 14–16, 2024, PHILADELPHIA, PA, USA.

- **2023**

1. Chi Liu, Tianqing Zhu, Jun Zhang, Wanlei Zhou, "Privacy Intelligence: A Survey on Image Privacy in Online Social Networks", **ACM Computing Surveys**, Vol 55, Issue 8, August 2023, pp 161:1-161:35, https://doi.org/10.1145/3547299
2. Shuai Zhou, Chi Liu, Dayong Ye, Tianqing Zhu, Wanlei Zhou, Philip S. Yu, "Adversarial Attacks and Defenses in Deep Learning: from a Perspective of Cybersecurity", **ACM Computing Surveys,** Vol 55, Issue 8, August 2023, 163:1-163:39, https://doi.org/10.1145/3547330
3. Tao Zhang, Tianqing Zhu, Mengde Han, Jing Li, Wanlei Zhou and Philip Yu, "Fairness in Graph-based Semi-supervised Learning". **Knowledge and Information Systems,** 65(2): 543-570 (February 2023).
4. Tianqing Zhu, Dayong Ye, Shuan Zhou, Bo Liu and Wanlei Zhou, "Label-only Model Inversion Attacks: Attack with the Least Information," **IEEE Transactions on Information Forensics and Security**, 18: 991-1005 (2023).
5. Lefeng Zhang, Tianqing Zhu, Farookh Khadeer Hussain, Dayong Ye, Wanlei Zhou, "A Game-Theoretic Method for Defending Against Advanced Persistent Threats in Cyber Systems", I**EEE Transactions on Information Forensics and Security**, 18: 1349-1364 (2023).
6. Tianqing Zhu, Dayong Ye, Zishuo Cheng, Wanlei Zhou, Philip S. Yu, "Learning Games for Defending Advanced Persistent Threats in Cyber Systems", **IEEE Transactions on Systems, Man, and Cybernetics: Systems.** Vol. 53, No. 4, pp. 2410-2422. April 2023.
7. Xuemeng Zhai, Zhiwei Tang, Zhiwei Liu, Wanlei Zhou, Hangyu Hu, Gaolei Fei, Guangmin Hu, "Sparse representation for heterogeneous information networks". **Neurocomputing** 525: 111-122 (2023).
8. Xiangyu Hu, Tianqing Zhu, Xuemeng Zhai, Wanlei Zhou, Wei Zhao, "Privacy Data Propagation and Preservation in Social Media: a Real-world Case Study", **IEEE Transactions on Knowledge and Data Engineering**, 35(4): 4137-4150 (2023).
9. Lefeng Zhang, Tianqing Zhu, Ping Xiong, Wanlei Zhou, Philip S. Yu, "A Robust Game-Theoretical Federated Learning Framework With Joint Differential Privacy". **IEEE Transactions on Knowledge and Data Engineering,** 35(4): 3333-3346 (2023).
10. Hui Sun, Tianqing Zhu, Zhiqiu Zhang, Dawei Jin, Ping Xiong, Wanlei Zhou, "Adversarial Attacks Against Deep Generative Models on Data: A Survey". I**EEE Transactions on Knowledge and Data Engineering**, 35(4): 3367-3388 (2023).
11. Huan Tian, Bo Liu, Tianqing Zhu, Wanlei Zhou, Philip S. Yu,"CIFair: Constructing continuous domains of invariant features for image fair classifications", **Knowledge-Based Systems**, Vol. 268, 23 May 2023, 110417. https://doi.org/10.1016/j.knosys.2023.110417
12. Xiangyu Hu, Tianqing Zhu, Xuemeng Zhai, Hengming Wang, Wanlei Zhou, and Wei Zhao, "Privacy Data Diffusion Modeling and Preserving in Online Social Network", **IEEE Transactions on Knowledge and Data Engineering,** Vol. 35, No. 6, pp.6224 - 6237 (June 2023).
13. Minghao Wang, Tianqing Zhu, Xuhan Zuo, Mengmeng Yang, Shui Yu, Wanlei Zhou, "Differentially private crowdsourcing with the public and private blockchain", **IEEE Internet of Things Journal**, Vol. 10, No. 10, pp. 8918-8930 (May 2023).
14. Yunjiao Lei, Dayong Ye, Sheng Shen, Yulei Sui, Tianqing Zhu, Wanlei Zhou, "New challenges in reinforcement learning: a survey of security and privacy". **Artificial Intelligence Review**, 56(7): 7195-7236 (2023).
15. Congcong Zhu, Zishuo Cheng, Dayong Ye, Farookh Khadeer Hussain, Tianqing Zhu, Wanlei Zhou, "Time-driven and Privacy-preserving Navigation Model for Vehicle-to-vehicle Communication Systems," **IEEE Transactions on Vehicular Technology**, Vol. 72, No. 7, pp.8459-8470. JULY 2023.
16. Tao Zhang, Dayong Ye, Tianqing Zhu, Tingting Liao and Wanlei Zhou, "Evolution of cooperation in malicious social networks with differential privacy mechanisms". **Neural Computing and Applications,** Vol. 35, pp. 12979–12994 (2023).
17. Tao Zhang, Tianqing Zhu, Jing Li, Wanlei Zhou, Philip S. Yu, "Revisiting model fairness via adversarial examples", **Knowledge-Based Systems**, Volume 277, 2023.
18. Lefeng Zhang, Tianqing Zhu, Haibin Zhang, Ping Xiong and Wanlei Zhou, "FedRecovery: Differentially Private Machine Unlearning for Federated Learning Frameworks," **IEEE Transactions on Information Forensics and Security**, vol. 18, pp. 4732-4746, 2023.
19. Tao Zhang, Tianqing Zhu, Kun Gao, Wanlei Zhou, Philip S. Yu, "Balancing Learning Model Privacy,

Fairness, and Accuracy With Early Stopping Criteria", I**EEE Transactions on Neural Networks and Learning Systems**, 34(9): 5557-5569 (2023).

20. Dayong Ye, Tianqing Zhu, Congcong Zhu, Wanlei Zhou, Philip S. Yu, "Model-Based Self-Advising for Multi-Agent Learning", **IEEE Transactions on Neural Networks and Learning Systems,** 34(10): 7934-7945 (2023).
21. Lefeng Zhang, Tianqing Zhu, Ping Xiong, Wanlei Zhou, and Philip S. Yu, "A Game-Theoretic Federated Learning Framework for Data Quality Improvement", **IEEE Transactions on Knowledge and Data Engineering**, Vol. 35, No. 11, pp.10952 - 10969 (June 2023)
22. Guangsheng Zhang, Bo Liu, Tianqing Zhu, Ming Ding, Wanlei Zhou, "Label-Only Membership Inference Attacks and Defenses In Semantic Segmentation Models", **IEEE Transactions on Dependable and Secure Computing**, 20(2): 1435-1449 (2023).
23. Chi Liu, Tianqing Zhu, Sheng Shen, Wanlei Zhou, "Towards Robust Gan-Generated Image Detection: A Multi-View Completion Representation". **IJCAI 2023**: 464-472.

- **2022**

1. Lefeng Zhang, Tianqing Zhu, Ping Xiong, Wanlei Zhou and Philip S. Yu, "More than Privacy: Adopting Differential Privacy in Game-theoretic Mechanism Design", **ACM Computing Surveys**. 54:7, Article 136 (2022).
2. Zishuo Cheng, Dayong Ye, Tianqing Zhu, Wanlei Zhou, Philip S. Yu, Congcong Zhu, "Multi-agent reinforcement learning via knowledge transfer with differentially private noise". **International Journal of Intelligent Systems,** 37(1): 799-828 (2022).
3. Jing Li, Weifa Liang, Wenzheng Xu, Zichuan Xu, Xiaohua Jia, Wanlei Zhou, and Jin Zhao, "Maximizing User Service Satisfaction for Delay-Sensitive IoT Applications in Edge Computing", **IEEE Transactions on Parallel and Distributed Systems**, 33(5): 1199-1212 (2022).
4. Yuan Zhao, Bo Liu, Tianqing Zhu, Ming Ding, Wanlei Zhou, "Private-Encoder: Enforcing Privacy in Latent Space for Human Face Images", **Concurrency and Computation: Practice and Experience**, 34(3) (2022).
5. Tianqing Zhu, Guangsheng Zhang, Bo Liu, Andi Zhou, Wanlei Zhou, "Visual Privacy Attacks and Defenses in Deep Learning: a Survey" **Artificial Intelligence Review** (2022). https://doi.org/10.1007/s10462-021-10123-y
6. Dayong Ye; Tianqing Zhu; Sheng Shen; Wanlei Zhou; Philip Yu. “Differentially Private Multi-Agent Planning for Logistic-like Problems”, **IEEE Transactions on Dependable and Secure Computing**. 19(2): 1212 – 1226. March/April 2022.
7. Shi-Jinn Horng, Julian Supardi, Wanlei Zhou, Chin-Teng Lin, Bin Jiang, "Recognizing Very Small Face Images Using Convolution Neural Networks", **IEEE Transactions on Intelligent Transportation Systems**, 23(3): 2103-2115. March 2022.
8. Dayong Ye, Shen Sheng, Tianqing Zhu, Bo Liu and Wanlei Zhou, "One Parameter Defense - Defending Data Inference Attacks via Differential Privacy". **IEEE Transactions on Information Forensics and Security**, Vol. 17, pp. 1466-1480.
9. Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou, Philip Yu, "More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence", **IEEE Transactions on Knowledge and Data Engineering**, Vol 34, No 6, pp. 1041-4347. June 2022. DOI: 10.1109/TKDE.2020.3014246
10. Tianqing Zhu, Jin Li, Xiangyu Hu, Ping Xiong, Wanlei Zhou, "The Dynamic Privacy-preserving Mechanisms for Online Dynamic Social Networks". **IEEE Transactions on Knowledge and Data Engineering**, Vol 34, No 6, pp. 2962-2974. June 2022. DOI: 10.1109/TKDE.2020.3015835
11. Shi-Jinn Horng, Dinh-Trung Vu, Thi-Van Nguyen, Wanlei Zhou, and Chin-Teng Lin (2022), "Recognizing Palm Vein in Smartphones Using RGB Images", **IEEE Transactions on Industrial Informatics**, Vol. 18, No. 9, pp. 5992-6002.
12. Zichuan Xu, Lizhen Zhou, Haipeng Dai, Weifa Liang, Wanlei Zhou, Pan Zhou, Wenzheng Xu, Guowei Wu (2022), "Energy-Aware Collaborative Service Caching in a 5G-Enabled MEC with Uncertain Payoffs," **IEEE Transactions on Communications**, pp.1058-1071, Feb. 2022.
13. Tao Zhang, Tianqing Zhu, Jing Li, Mengde Han, Wanlei Zhou, Philip Yu (2022), "Fairness in Semi-supervised Learning: Unlabeled Data Help to Reduce Discrimination", **IEEE Transactions on Knowledge and Data Engineering**, 34(4), pp. 1763-1774.
14. Tao Zhang, Tianqing Zhu, Mengde Han, Jing Li, Wanlei Zhou and Philip Yu, "Fairness in Graph-

based Semi-supervised Learning". **Knowledge and Information Systems**, published online October 1, 2022, https://doi.org/10.1007/s10115-022-01738-w

15. Jing Li, Weifa Liang, Zichuan Xu, Xiaohua Jia, Wanlei Zhou, "Service Provisioning for Multi-source IoT Applications in Mobile Edge Computing". **ACM Transactions on Sensor Networks** 18(2): 17:1-17:25 (2022).
16. Tianrui Zong, Juan Zhao, Yong Xiang, Iynkaran Natgunanathan, Longxiang Gao, Wanlei Zhou, "Desynchronization-attack-resilient audio watermarking mechanism for stereo signals using the linear correlation between channels". **World Wide Web** 25(1): 357-379 (2022).
17. Congcong Zhu, Dayong Ye, Tianqing Zhu, Wanlei Zhou, "Time-optimal and privacy preserving route planning for carpool policy". **World Wide Web** 25(3): 1151-1168 (2022).
18. Dayong Ye, Tianqing Zhu, Zishuo Cheng, Wanlei Zhou and Philip S. Yu, "Differential Advising in Multiagent Reinforcement Learning", **IEEE Transactions on Cybernetics**, 52(6): 5508-5521 (2022).
19. Tao Zhang, Tianqing Zhu, Renping Liu, Wanlei Zhou, "Correlated data in differential privacy: Definition and analysis". **Concurrency and Computation: Practice and Experience**, 34(16) (2022).
20. Sheng Shen, Tianqing Zhu, Di Wu, Wei Wang, Wanlei Zhou, "From distributed machine learning to federated learning: In the view of data privacy and security". **Concurrency and Computation: Practice and Experience**, 34(16) (2022).
21. Guangsheng Zhang, Bo Liu, Tianqing Zhu, Andi Zhou, Wanlei Zhou, "Visual privacy attacks and defenses in deep learning: a survey". **Artificial Intelligence Review** 55(6): 4347-4401 (2022).
22. Huan Tian, Tianqing Zhu, Wei Liu, Wanlei Zhou, "Image fairness in deep learning: problems, models, and challenges. **Neural Computing and Applications** 34(15): 12875-12893 (2022)
23. Huan Tian, Tianqing Zhu and Wanlei Zhou, "Fairness and privacy preservation for facial images: GAN-based methods", **Computer and Security**, Elsevier, Vol. 122, Nov. 2022, 102902. https://doi.org/10.1016/j.cose.2022.102902
24. Weifa Liang, Yu Ma, Wenzheng Xu, Zichuan Xu, Xiaohua Jia, and Wanlei Zhou, "Request Reliability Augmentation with Service Function Chain Requirements in Mobile Edge Computing", **IEEE Transactions on Mobile Computing**, Vol. 21, No. 12, December 2022, pp. 4541-4554.
25. Zichuan Xu, Haozhe Ren, Weifa, Qiufen Xia, Wanlei Zhou, Pan Zhou, Wenzheng Xu, Guowei Wu, Mingchu Li, "Near Optimal Learning-Driven Mechanisms for Stable NFV Markets in Multitier Cloud Networks", **IEEE/ACM Transactions on Networking**, Vol. 30, No. 6, p.1-15, December 2022.

- **2021**

1. Tianrui Zong, Yong Xiang, Iynkaran Natgunanathan, Longxiang Gao, Guang Hua, Wanlei Zhou, "Non-linear-echo Based Anti-collusion Mechanism for Audio Signals", **IEEE/ACM Transactions on Audio, Speech and Language Processing**, Vol. 29, 2021, pp. 969-984.

2. Juan Zhao, Tianrui Zong, Yong Xiang, Longxiang Gao, Wanlei Zhou, Gleb Beliakov, "Desynchronization Attacks Resilient Watermarking Method Based on Frequency Singular Value Coefficient Modification". **IEEE/ACM Transactions on Audio, Speech and Language Processing** 29: 2282-2295 (2021).

3. Jianghua Liu, Jingyu Hou, Wenjie Yang, Yang Xiang, Wanlei Zhou, Wei Wu, and Xinyi Huang, "Leakage-Free Dissemination of Authenticated Tree-Structured Data with Multi-Party Control", **IEEE Transactions on Computers**, Vol. 70, No. 7, July 2021.

4. Jianghua Liu, Jinhua Ma, Yang Xiang, Wanlei Zhou, and Xinyi Huang, "Authenticated Medical Documents Releasing with Privacy Protection and Release Control". **IEEE Transactions on Dependable and Secure Computing,** Jan/Feb 2021, Volume: 18, Issue: 1, pp. 448-459.

5. Dayong Ye, Tianqing Zhu, Sheng Shen, Wanlei Zhou: "A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries". **IEEE Transactions on Information Forensics and Security**. 16: 569-584 (2021).

6. Aneesh Chivukula, Xinghao Yang, Wei Liu, Tianqing Zhu, Wanlei Zhou, "Game Theoretical Adversarial Deep Learning with Variational Adversaries". Accepted by **IEEE Transactions on Knowledge and Data Engineering**, Vol. 33, No. 11, pp. 3568-3581 (2021).

7. Youyang Qu, Shui Yu, Wanlei Zhou, Shiping Chen, and Jun Wu, "Customizable Reliable Privacy-Preserving Data Sharing in Cyber-Physical Social Network", **IEEE Transactions on Network Science and Engineering**, Vol. 8, No. 1, January-March 2021, pp. 269-281.

8. Lu-Xing Yang, Pengdeng Li, Xiaofan Yang, Yong Xiang, Frank Jiang and Wanlei Zhou, "Effective quarantine and recovery scheme against advanced persistent threat," **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, Vol. 51, No. 10, pp. 5977-5991 (2021).
9. Jianchao Lu, Xi Zheng, Lihong Tang, Tianyi Zhang, Quan Z. Sheng, Chen Wang, Jiong Jin, Shui Yu, Wanlei Zhou, "Can Steering Wheel Detect Your Driving Fatigue", **IEEE Transactions on Vehicular Technology**, 70(6): 5537-5550 (2021).
10. Juan Zhao, Tianrui Zong, Yong Xiang, Iynkaran Natgunanathan, Longxiang Gao, Wanlei Zhou, "Desynchronization-attack-resilient audio watermarking mechanism for stereo signals using the linear correlation between channels", **The World Wide Web Journal**. pp. 1-23, doi: 10.1007/s11280-021-00897-0 (2021).
11. Zichuan Xu, Haozhe Ren, Weifa Liang, Qiufen Xia, Wanlei Zhou, Guowei Wu, Pan Zhou, "Near Optimal and Dynamic Mechanisms Towards a Stable NFV Market in Multi-Tier Cloud Networks". **INFOCOM** 2021: 1-10.
12. Wanlei Zhou, Yi Mu, "Advances in Web-Based Learning - Proceedings of the 20th International Conference, ICWL 2021", Macau, China, November 13-14, 2021, **Lecture Notes in Computer Science,** Vol. 13103, Springer, ISBN 978-3-030-90784-6 (2021).

- **2020**

1. Yanxin Zhang, Yulei Sui, Shirui Pan, Zheng Zheng, Baodi Ning, Ivor W. Tsang, Wanlei Zhou, "Familial Clustering for Weakly-Labeled Android Malware Using Hybrid Representation Learning". **IEEE Transactions on Information Forensics and Security.** 15: 3401-3414 (2020)
2. Tao Zhang, Tianqing Zhu, Ping Xiong, Huan Huo, Zahir Tari, Wanlei Zhou, "Correlated Differential Privacy: Feature Selection in Machine Learning". **IEEE Transactions on Industrial Informatics.** 16(3): 2115-2124 (2020).
3. Dayong Ye, Tianqing Zhu, Wanlei Zhou, and Philip S. Yu, "Differentially Private Malicious Agent Avoidance in Multiagent Advising Learning", **IEEE Transactions on Cybernetics**, 50(10): 4214-4227 (2020).
4. Shi-Jinn Horng, Cheng-Chung Lu and Wanlei Zhou, "An Identity-based and Revocable Data-sharing Scheme in VANETs", **IEEE Transactions on Vehicular Technology**, Vol. 69, No. 12, December 2020, pp. 15933-15946.
5. Youyang Qu, Shui Yu, Wanlei Zhou, and Yonghong Tian, " swordDriven Personalized Spatial-Temporal Private Data Sharing in Cyber-Physical Social Systems", **IEEE Transactions on Network Science and Engineering**, Vol. 7, Issue: 4, pp. 2576-2586 (2020).
6. Tianqing Zhu, Ping Xiong, Gang Li, Wanlei Zhou, Philip S. Yu, "Differentially private model publishing in cyber physical systems". **Future Generation of Computer Systems**. 108: 1297-1306 (2020)
7. Ping Xiong, Lefeng Zhang, Tianqing Zhu, Gang Li, Wanlei Zhou, "Private collaborative filtering under untrusted recommender server". **Future Generation of Computer Systems**. 109: 511-520 (2020)
8. Xuemeng Zhai, Wanlei Zhou, Gaolei Fei, Cai Lu, Guangmin Hu, "Network sparse representation: Decomposition, dimensionality-reduction and reconstruction". **Information Sciences**. 521: 307-325 (2020)
9. Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, Wanlei Zhou, "Security and privacy in 6G networks: New areas and new challenges", **Digital Communications and Networks**, Volume 6, Issue 3, August 2020, pp. 281-291.
10. Kasra Majbouri Yazdi, Adel Majbouri Yazdi, Saeid Khodayi, Jingyu Hou, Wanlei Zhou, Saeed Saedy, Mehrdad Rostami, "Prediction optimization of diffusion paths in social networks using integration of ant colony and densest subgraph algorithms". **Journal of High Speed Networks** 26(2): 141-153 (2020)
11. Mohammad Reza Nosouhi, Shui Yu, Wanlei Zhou, Marthie Grobler, Habiba Keshtiar, "Blockchain for secure location verification". **Journal of Parallel and Distributed Computing**. 136: 40-51 (2020)
12. Shigang Liu, Jun Zhang, Yang Xiang, Wanlei Zhou, Dongxi Xiang: "A study of data pre-processing techniques for imbalanced biomedical data classification". **International Journal of Bioinformatics Research and Applications**. 16(3): 290-318 (2020)
13. Linjing Wu, Qingtang Liu, Wanlei Zhou, Gang Mao, Jingxiu Huang, Huan Huang: "A Semantic Web-Based Recommendation Framework of Educational Resources in E-Learning". **Technology,**

Knowledge and Learning. 25(4): 811-833 (2020).

14. Peng Li, Toshiaki Miyazaki, Wanlei Zhou, "Secure Balance Planning of Off-blockchain Payment Channel Networks". **INFOCOM** 2020: 1728-1737.

- **2019**

1. Lu-Xing Yang, Pengdeng Li, Yushu Zhang, Xiaofan Yang, Yong Xiang, Wanlei Zhou: "Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach". **IEEE Transactions on Information Forensics and Security** 14(7): 1713-1728 (2019).
2. Derek Wang, Tingmin Wu, Sheng Wen, Xiaofeng Chen, Yang Xiang, and Wanlei Zhou, "STC: Exposing Hidden Compromised Devices in Networked Sustainable Green Smart Computing Platforms by Partial Observation". **IEEE Transactions on Sustainable Computing**. 4(2): 178-190 (2019).
3. Xianjiao Zeng, Guangquan Xu, Xi Zheng, Yang Xiang, Wanlei Zhou, "E-AUA: An Efficient Anonymous User Authentication Protocol for Mobile IoT." **IEEE Internet of Things Journal** 6(2): 1506-1519 (2019).
4. Rajkumar Buyya, Satish Narayana Srirama, Giuliano Casale, Rodrigo N. Calheiros, Yogesh Simmhan, Blesson Varghese, Erol Gelenbe, Bahman Javadi, Luis Miguel Vaquero, Marco A. S. Netto, Adel Nadjaran Toosi, Maria Alejandra Rodriguez, Ignacio Martín Llorente, Sabrina De Capitani di Vimercati, Pierangela Samarati, Dejan S. Milojicic, Carlos A. Varela, Rami Bahsoon, Marcos Dias de Assunção, Omer Rana, Wanlei Zhou, Hai Jin, Wolfgang Gentzsch, Albert Y. Zomaya, Haiying Shen: "A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade". **ACM Computing Survey**. 51(5): 105:1-105:38 (2019).
5. Yunyun Wu, Jingyu Hou, Jing Liu, Wanlei Zhou, Shaowen Yao: *Novel Multi-Keyword Search on Encrypted Data in the Cloud*. **IEEE Access** 7: 31984-31996 (2019).
6. Bo Liu, Ming Ding, Tianqing Zhu, Yong Xiang, Wanlei Zhou, "Adversaries or allies? Privacy and deep learning in big data era." **Concurrency and Computation: Practice and Experience** 31(19) (2019).
7. Chee Keong Ng, Frank Jiang, Leo Yu Zhang, Wanlei Zhou, "Static malware clustering using enhanced deep embedding method." **Concurrency and Computation: Practice and Experience** 31(19) (2019).
8. Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H. Deng: "A blockchain-based location privacy-preserving crowdsensing system". **Future Generation of Computer Systems**. 94: 408-418 (2019).
9. Xuemeng Zhai, Wanlei Zhou, Gaolei Fei, Cai Lu, Sheng Wen, Guangmin Hu: *Edge-based stochastic network model reveals structural complexity of edges*. **Future Generation of Computer Systems** 100: 1073-1087 (2019).
10. Mohammad Reza Nosouhi, Shui Yu, Wanlei Zhou, Marthie Grobler, Habiba Keshtiar, Blockchain for secure location verification, **Journal of Parallel and Distributed Computing**, Volume 136, 2020, Pages 40-51, ISSN 0743-7315.

- **2018**

1. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, and Wanlei Zhou, "Rumor Source Identification in Social Networks with Time-varying Topology", **IEEE Transactions on Dependable and Secure Computing.** Volume: 15, Issue: 1, pp. 166-179, Jan.-Feb. 1 2018
2. Bo Liu, Wanlei Zhou, Longxiang Gao, Haibo Zhou, Tom Luan, and Sheng Wen, "Malware Propagations in Wireless Ad Hoc Networks". **IEEE Transactions on Dependable and Secure Computing,** 15(6): 1016-1026 (2018).
3. Tianqing Zhu, Gang Li, Ping Xiong, Wanlei Zhou, "Answering differentially private queries for continual datasets release", **Future Generation Computer Systems**, 87: 816-827 (2018).
4. Jiannong Cao, Aniello Castiglione, Giovanni Motta, Florin Pop, Yanjiang Yang, Wanlei Zhou: "Human-Driven Edge Computing and Communication: Part 2". **IEEE Communications Magazine** 56(2): 134-135 (2018).
5. Tingmin Wu, Sheng Wen, Yang Xiang, Wanlei Zhou: "Twitter spam detection: Survey of new approaches and comparative study". **Computers & Security** 76: 265-284 (2018).
6. Youyang Qu, Shui Yu, Longxiang Gao, Wanlei Zhou, Sancheng Peng: "A Hybrid Privacy Protection Scheme in Cyber-Physical Social Networks". **IEEE Transactions on Computational Social Systems**

5(3): 773-784 (2018).

7. Youyang Qu, Shui Yu, Wanlei Zhou, Sancheng Peng, Guojun Wang, Ke Xiao: "Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things". **IEEE Wireless Communications**. 25(6): 91-97 (2018).
8. Derek Wang, Tingmin Wu, Sheng Wen, Donghai Liu, Yang Xiang, Wanlei Zhou, Houcine Hassan, Abdulhameed Alelaiwi: Pokémon GO in Melbourne CBD: A case study of the cyber-physical symbiotic social networks. **Journal of Computational Science** 26: 456-467 (2018).
9. Mengmeng Yang, Tianqing Zhu, Yang Xiang, and Wanlei Zhou, "Density-Based Location Preservation for Mobile Crowdsensing With Differential Privacy", **IEEE Access**, Volumn 6: Issue 1, pp. 14779-14789 (2018),
10. Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, and Yong Xiang, "Location Privacy and the Applications: A Systematical Study," **IEEE Access**, Volume 6: Issue 1, pp. 17606-17624 (2018).

- **2017**

1. Shigang Liu, Jun Zhang, Yang Xiang, and Wanlei Zhou, "Fuzzy-Based Information Decomposition for Incomplete and Imbalanced Data Learning", **IEEE Transactions on Fuzzy Systems,** Volume: 25, Issue:6, Page(s): 1476-1490, DECEMBER 2017.
2. Chao Chen, Yu Wang, Jun Zhang, Yang Xiang, and Wanlei Zhou, and Geyong Min, "Statistical Features Based Real-time Detection of Drifted Twitter Spam". **IEEE Transactions on Information Forensics and Security**. Vol 12, No. 4, pp. 914-925, April 2017.
3. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, and Wanlei Zhou, "Identifying Propagation Sources in Networks: State-of-the-Art and Comparative Studies", **IEEE Communications Surveys and Tutorials**. Vol. 19, No. 1, pp. 465-481, First Quarter 2017.
4. Longxiang Gao, Tom H. Luan, Shui Yu, Wanlei Zhou, and Bo Liu , "FogRoute: DTN-based Data Dissemination Model in Fog Computing", **IEEE Internet of Things Journal**, 4(1): 225-235 (2017).
5. Sheng Wen, Jiaojiao Jiang, Bo Liu, Yang Xiang and Wanlei Zhou, "Using epidemic betweenness to measure the influence of users in complex networks", **Journal of Network and Computer Applications**, Volume 78, January 2017, Pages 288-299.
6. Bo Liu, Wanlei Zhou, Tianqing Zhu, Haibo Zhou, Xiaodong Lin, "Invisible Hand: Economic Model based Trajectory Privacy Preserving Schemes in Mobile Crowd Sensing Applications". **IEEE Transactions on Vehicular Technology**. VOL. 66, NO. 5, pp.4410-4423, MAY 2017.
7. Tianqing Zhu, Gang Li, Wanlei Zhou, and Philip S. Yu, "Differentially Private Data Publishing and Analysis: a Survey". **IEEE Transactions on Knowledge and Data Engineering**. Vol. 29, No. 8, pp. 1619-1638, August 2017.
8. Tianqing Zhu, Gang Li, Wanlei Zhou, and Philip S. Yu, **Differential Privacy and Its Applications**, ISBN 978-3-319-62002-2, Springer, 2017.
9. Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, Wanlei Zhou, "A secure search protocol for low cost passive RFID tags". **Computer Networks**, Vol 122 (2017), pp. 70-82.
10. Jiao Jiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, Wanlei Zhou, and Houcine Hassan, "The structure of communities in scale-free networks". **Concurrency and Computation: Practice and Experience**. 29(14), pp. 1-16, July 2017.

- **2016**

1. Shui Yu, Wanlei Zhou, Song Guo, Minyi Guo, "A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking", **IEEE Transactions on Computers**. VOL. 65, NO. 5, MAY 2016, pp. 1418-1427.
2. Chao Chen, Jun Zhang, Yang Xiang, Wanlei Zhou, Jonathan Oliver, "Spammers Are Becoming 'Smarter' on Twitter". **IEEE IT Professional**, 18(2): 66-70 (2016).
3. Tianqing Zhu, Gang Li, Wanlei Zhou, Ping Xiong, and Cao Yuan, "Privacy-preserving topic model for tagging recommender systems", **Knowledge and Information Systems** (Springer), January 2016, Volume 46, Issue 1, pp 33-58.
4. Guangyan Huang, Jing He, Wanlei Zhou, Guang-Li Huang, Limin Guo, Xiangmin Zhou, Feiyi Tang, "Discovery of Stop Regions for Understanding Repeat Travel Behaviors of Moving Objects", **Journal of Computer and System Sciences**, 82 (2016) 582–593.
5. Song Han, Shuai Zhao, Qinghua Li, Chunhua Ju and Wanlei Zhou, "PPM-HDA: Privacy-preserving and multifunctional health data aggregation with fault tolerance for cloud assisted WBANs", **IEEE**

Transactions on Information Forensics and Security. VOL. 11, NO. 9, pp. 1940-1955, SEPTEMBER 2016.

6. Mohammad Sayad Haghighi, Sheng Wen, Yang Xiang, Barry Quinn, and Wanlei Zhou, "On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks". **IEEE Transactions on Information Forensics and Security**. Volume 11, Issue 12, pp. 2854-2865, DECEMBER.2016.
7. Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, Tom H. Luan, and Haibo Zhou, "Silence is Golden: Enhancing Privacy of Location-Based Services by Content Broadcasting and Active Caching in Wireless Vehicular Networks", **IEEE Transactions on Vehicular Technology**. VOL. 65, NO. 12, December 2016, pp. 9942-9953.
8. Faizal Riaz-ud-Din, Wanlei Zhou, and Robin Doss, "Query verification schemes for cloud-hosted databases: a brief survey", **International Journal of Parallel, Emergent and Distributed Systems**, 31:6, 543-561, 2016.

- **2015**
  1. Longxiang Gao, Shui Yu, Tom H. Luan, and Wanlei Zhou, **Delay Tolerant Networks**, ISBN 978-3-319-18108-0, Springer, 2015. http://www.springer.com/gb/book/9783319181073
  2. Tianqing Zhu, Ping Xiong, Gang Li and Wanlei Zhou, "Correlated Differential Privacy: Hiding Information in Non-IID Dataset," **IEEE Transactions on Information Forensics and Security**, Vol 10, No 2, February 2015, pp229-242.
  3. Sheng Wen, Mohammad Sayad Haghighi, Chao Chen, Yang Xiang, Wanlei Zhou, and Weijia Jia, "A Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks", **IEEE Transactions on Computers**, Vol. 64, No. 3, pp. 640-653, March 2015.
  4. Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, and Wanlei Zhou, "Secure Tag Search in RFID Systems Using Mobile Readers", **IEEE Transactions on Dependable and Secure Computing**, Vol. 12, No. 2, pp. 230-242, March/April 2015.
  5. Yong Xiang, Tianrui Zong, Iynkaran Natgunanathan, Song Guo, Wanlei Zhou and Gleb Beliakov, "Robust Histogram Shape Based Method for Image Watermarking", **IEEE Transactions on Circuits and Systems for Video Technology**, Vol. 25, No. 5, pp. 717-729, May 2015.
  6. Saravanan Sundaresan, Robin Doss, Wanlei Zhou, and Selwyn Piramuthu, "Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy", **Computer Communications** (Elsevier), pp. 112-124, Vol 55. January 2015.
  7. Xueqi Cheng, Jinhong Yuan, Ali Tajer, Aiqun Hu, and Wanlei Zhou, "Special issue on recent advances in network and information security - security and communication networks journal". **Security and Communication Networks** (Wiley) Volume 8, Issue 1, 2015, pp. 1.
  8. Sheng Wen, Di Wu, Ping Li, Yang Xiang, Wanlei Zhou and Guiyi Wei, "Detecting stepping stones by abnormal causality probability", **Security and Communication Networks** (Wiley), Volume 8, Issue 10, 2015, pp. 1831–1844.
  9. Yongli Ren, Gang Li, and Wanlei Zhou, "A Survey of Recommendation Techniques Based on Off-line Data Processing" **Concurrency and Computation: Practice and Experience**, Volume 27, Issue 15, October 2015, Pages 3915–3942.
  10. Jun Zhang, Xiao Chen, Yang Xiang, Wanlei Zhou, and Jie Wu, "Robust Network Traffic Classification," **IEEE/ACM Transactions on Networking**, Volume 23, Issue 4, pp. 1257-1270. August 2015.
  11. Saravanan Sundaresan, Robin Doss, and Wanlei Zhou, "Zero Knowledge Grouping Proof Protocol for RFID EPC C1G2 Tags", **IEEE Transactions on Computers**, Volume:64, Issue: 10, pp. 2994-3008, October 2015.
  12. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, and Wanlei Zhou, "K-center: An Approach on the Multi-source Identification of Information Diffusion", **IEEE Transactions on Information Forensics and Security**. Volume:10, Issue: 12, pp. 2616-2626, 2015.
  13. Shui Yu, Guojun Wang, and Wanlei Zhou, "Modelling Malicious Activities in Cyber Space", **IEEE Network**, Volume:29, Issue:6, pp. 83-87, November/December 2015.
  14. Chao Chen, Yang Xiang, Jun Zhang, Wanlei Zhou, and Xie Yi, "A Performance Evaluation of Machine Learning Based Streaming Spam Tweets Detection", **IEEE Transactions on**

Computational Social Systems. VOL. 2, NO. 3, SEPTEMBER 2015, pp.65-76.

15. Guangyan Huang, Jing He, Yanchun Zhang, Wanlei Zhou, Hai Liu, Peng Zhang, Zhiming Ding, Yue You, Jian Cao, "Mining streams of short text for analysis of world-wide event evolutions". **World Wide Web** 18(5): 1201-1217 (2015).

- **2014**
  1. Yini Wang, Sheng Wen, Yang Xiang, and Wanlei Zhou, "Modeling the Propagation of Worms in Networks: A Survey", **IEEE Communications Surveys and Tutorials**, Volume:16, Issue: 2, 2014, pp 942-960.
  2. Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, and Wanlei Zhou, "A Robust Grouping Proof Protocol for RFID EPC C1G2 Tags", **IEEE Transactions on Information Forensics and Security**, VOL. 9, NO. 6, 2014, pp 961-975.
  3. Silvio Cesare, Yang Xiang, and Wanlei Zhou, "Control Flow-based Malware Variant Detection", **IEEE Transactions on Dependable and Secure Computing**, VOL. 11, NO. 4, JULY/AUGUST 2014, pp. 304-317.
  4. Sheng Wen, Wei Zhou, Jun Zhang, Yang Xiang, Wanlei Zhou, Weijia Jia, and Cliff C.Zou "Modeling and Analysis on the Propagation Dynamics of Modern Email Malware", **IEEE Transactions on Dependable and Secure Computing**, VOL. 11, NO. 4, JULY/AUGUST 2014, pp. 361-374.
  5. Yong Xiang, Iynkaran Natgunanathan, Song Guo, Wanlei Zhou, and Saeid Nahavandi, "Patchwork-Based Audio Watermarking Method Robust to De-synchronization Attacks", **IEEE Transactions on Audio, Speech and Language Processing**, VOL. 22, NO. 9, 2014. PP. 1413-1423.
  6. Yu Wang, Yang Xiang, Wanlei Zhou, Jun Zhang, "Internet traffic clustering with side information", **Journal of Computer and System Sciences**, Volume 80 (2014), Pages 1021-1036.
  7. Tianqing Zhu, Yongli Ren, Wanlei Zhou, Jia Rong, Ping Xiong, "An Effective Privacy Preserving Algorithm for Neighborhood-based Collaborative Filtering", **Future Generation Computer System**, Volume 36 (2014), Pages 142-155.
  8. YongHong Tian, Shui Yu, Chin-Yung Lin, Wen Gao, and Wanlei Zhou, "Special Issue on Social Multimedia Computing: Challenges, Techniques, and Applications: Guest Editorial", **Journal of Multimedia**, Vol 9, No 1 (2014), pp. 1-3.
  9. Wei Zhou, Weijia Jia, Sheng Wen, Yang Xiang, Wanlei Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic", **Future Generation Computer System**, Volume 38, 2014, Pages 36-46.
  10. Yongli Ren, Gang Li, Jun Zhang and Wanlei Zhou, "The Maximum Imputation Framework for Neighborhood-based Collaborative Filtering", **Social Network Analysis and Mining** (Springer), (2014) 4:207.
  11. Tianqing Zhu, Gang Li, Lei Pan, Yongli Ren, and Wanlei Zhou, "Privacy preserving collaborative filtering for KNN attack resisting", **Social Network Analysis and Mining** (Springer), (2014) 4:196.
  12. Sheng Wen, Jiaojiao Jiang, Yang Xiang, Shui Yu, and Wanlei Zhou, "Are the Popular Users Always Important for the Information Dissemination in Online Social Networks?" **IEEE Network**, pp. 64-67, September/October 2014.
  13. Theerasak Thapngam, Shui Yu, Wanlei Zhou, and S. Kami Makki, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis", **Peer-to-Peer Networking and Applications** (Springer), Volume 7, Issue 4, December 2014, pp. 346-358.
  14. Yu Wang, Yang Xiang, Jun Zhang, Wanlei Zhou, Guiyi Wei, and Laurence Yang, "Internet Traffic Classification Using Constrained Clustering", **IEEE Transactions on Parallel and Distributed Systems**, VOL. 25, NO. 11, NOVEMBER 2014. pp. 2932-2943.
  15. Sheng Wen, Jiaojiao Jiang, Yang Xiang, Shui Yu, Wanlei Zhou and Weijia Jia, "To shut them up or to clarify: restraining the spread of rumours in Online Social Networks", **IEEE Transactions on Parallel and Distributed Systems**, Vol. 25, No. 12, pp. 3306-3316, 2014.

- **2013**
  1. Jun Zhang, Yang Xiang, Yu Wang, Wanlei Zhou, Yong Xiang, and Yong Guan, "Network Traffic Classification Using Correlation Information", **IEEE Transactions on Parallel and Distributed Systems**, VOL. 24, NO. 1, JANUARY 2013, pp. 104-117.
  2. R. Doss, S. Sundaresan and W. Zhou, "A Practical Quadratic Residues Based Scheme for Authentication and Privacy in Mobile RFID Systems", **Ad Hoc Networks** (Elsevier), Volume 11,

Issue 1, January 2013, Pages 383-396.

3. Jun Zhang, Chao Chen, Yang Xiang, Wanlei Zhou, and Yong Xiang, "Internet Traffic Classification by Aggregating Correlated Naive Bayes Predictions", **IEEE Transactions on Information Forensics and Security**, VOL. 8, NO. 1, JANUARY 2013, pp. 5-15.
4. R. Doss, W. Zhou, and S. Yu, "Secure RFID Tag Ownership Transfer based on Quadratic Residues", **IEEE Transactions on Information Forensics and Security**, VOL. 8, NO. 2, FEBRUARY 2013, pp. 390-401.
5. Jun Zhang, Yang Xiang, Wanlei Zhou, Yu Wang, "Unsupervised Traffic Classification Using Flow Statistical Properties and IP Packet Payload", **Journal of Computer and System Sciences** (Elsevier), Volume 79, Issue 5, August 2013, Pages 573-585.
6. Silvio Cesare, Yang Xiang, and Wanlei Zhou, "Malwise - An Effective and Efficient Classification System for Packed and Polymorphic Malware", **IEEE Transactions on Computers**, Vol. 62, Issue 6. pp.1193-1206, June 2013.
7. Sheng Wen, Wei Zhou, Jun Zhang, Yang Xiang, Wanlei Zhou, and Weijia Jia, "Modeling Propagation Dynamics of Social Network Worms", **IEEE Transactions on Parallel and Distributed Systems**, vol. 24, no. 8, pp. 1633-1643, Aug. 2013.
8. Jun Zhang, Chao Chen, Yang Xiang, Wanlei Zhou, and Athanasios V. Vasilakos, "An Effective Network Traffic Classification Method with Unknown Flow Detection", **IEEE Transactions on Network and Service Management**, VOL. 10, NO. 2, JUNE 2013, pp. 133-147.
9. Longxiang Gao, Ming Li, Alessio Bonti, Wanlei Zhou, and Shui Yu, "Multi-Dimensional Routing Protocol in Human Associated Delay-Tolerant Networks", **IEEE Transactions on Mobile Computing**, VOL. 12, NO. 11, NOVEMBER 2013, pp. 2132-2144.
10. Jun Zhang, Lei Ye, Yang Xiang, Wanlei Zhou, "Robust Image Retrieval with Hidden Classes," **Computer Vision and Image Understanding**, vol. 117, no. 6, pp. 670-679, 2013.
11. Guojun Wang, Wanlei Zhou, and Laurence T. Yang, "Trust, security and privacy for pervasive applications," **Journal of Supercomputing**, vol. 64, no. 3, pp. 661-663, 2013.
12. Ashish Saini, Jingyu Hou, and Wanlei Zhou, "Hub-Based Reliable Gene Expression Algorithm to Classify ER+ and ER- Breast Cancer Subtypes," **International Journal of Bioscience, Biochemistry and Bioinformatics**, Vol. 3, No. 1, pp. 20-26, January 2013.
13. Yongli Ren, Gang Li, and Wanlei Zhou, "A learning method for Top-N recommendations with incomplete data", **Social Network Analysis and Mining** (Springer), December 2013, Volume 3, Issue 4, pp 1135-1148.
14. Yongli Ren, Gang Li, Jun Zhang, and Wanlei Zhou, "Lazy Collaborative Filtering for Data Sets with Missing Values", **IEEE Transactions on Cybernetics**, VOL. 43, NO. 6, pp. 1822-1834, DECEMBER 2013.

- **2012**
  1. Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", **IEEE Transactions on Parallel and Distributed Systems**, VOL. 23, NO. 6, JUNE 2012. pp. 1073-1080.
  2. Yong Xiang, Iynkaran Natgunanathan, Dezhong Peng, Wanlei Zhou, and Shui Yu, "A Dual-Channel Time-Spread Echo Method for Audio Watermarking", **IEEE Transactions on Information Forensics and Security**, Vol. 7, No. 2, April 2012, pp. 383 - 392.
  3. Iynkaran Natgunanathan, Yong Xiang, Yue Rong, Wanlei Zhou, and Song Guo, "Robust Patchwork-Based Embedding and Decoding Scheme for Digital Audio Watermarking", **IEEE Transactions on Audio, Speech and Language Processing,** Volume: 20 , Issue: 8 Page(s): 2232 - 2239.
  4. Sheng Wen, Wei Zhou, Yini Wang, Wanlei Zhou, and Yang Xiang, "Locating Defense Positions for Thwarting the Propagation of Topological Worms", **IEEE Communication Letters**, VOL. 16, NO. 4, pp. 560-563, APRIL 2012.
  5. Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, "Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures", **Journal of Networking and Computer Applications** (Elsevier), Volume 35, Issue 3, May 2012, Pages 867-880.
  6. Yu Wang, Yang Xiang, Wanlei Zhou, and Shunzheng Yu, "Generating Regular Expression Signatures for Network Traffic Classification in Trusted Network Management", **Journal of Network and Computer Applications** (Elsevier), Volume 35, Issue 3, May 2012, Pages 992-1000.

7. Shui Yu, Wanlei Zhou, Weijia Jia, and Jiankun Hu, "Attacking Anonymous Web Browsing at Local Area Networks Through Browsing Dynamics", **The Computer Journal**, Vol. 55 No. 4, 2012. pp. 410- 421.
8. Sheng Wen, Wei Zhou, Yang Xiang and Wanlei Zhou, "CAFS: A Novel Lightweight Cache-based Scheme for Large-Scale Intrusion Alert Fusion", **Concurrency and Computation: Practice and Experience** (Wiley), Vol. 24, Issue 10, July 2012, pp. 1137-1153.
9. Longxiang Gao, Ming Li, Alessio Bonti, Wanlei Zhou, and Shui Yu, "M-Dimension: Multi Characteristics Based Routing Protocol in Human Associated Delay-Tolerant Networks with Improved Performance over One Dimensional Classic Models", **Journal of Networking and Computer Applications** (Elsevier), Volume 35, Issue 4, July 2012, Pages 1285-1296.
10. R. Doss, W. Zhou, S. Sundaresan, S. Yu and L. Gao, "Minimum Disclosure Approach to Authentication and Privacy in RFID Systems", **Computer Networks** (Elsevier), Volume 56, Issue 15, 15 October 2012, Pages 3401-3416.
11. Jun Zhang, Chao Chen, Yang Xiang, and Wanlei Zhou, "Semi-supervised and compound classification of network traffic," **International Journal of Security and Networks**, vol. 7, no. 4, pp.252-261, 2012.