IJCIS: Call for Papers Special Issue 'Adversarial Attack and Defense for Intelligence Systems'

ATLANTIS PRESS

Guest Editors:

Matthew Wright
Rochester Institute of Technology, US.
Email: mkwics@rit.edu

Qi Yu
Rochester Institute of Technology, US.
Email: qi.yu@rit.edu

Xiangnan He
University of Science and Technology of China, China
Email: xiangnanhe@gmail.com

Liang Chen
Sun Yat-Sen University, China
Email: chenliang6@mail.sysu.edu.cn

Aims and Scope

With the accumulation of massive data and the enhancement of computing power, the technology of computational intelligence has been widely developed and applied, which brings convenience to people's lives, but also produces security and privacy problems. In security-sensitive domains, attackers may attempt to mislead intelligence systems, causing its data leakage and reducing its reasoning ability. Therefore, it is imperative to seek theory, algorithms, methods, frameworks and application for the security of intelligence systems.

This special issue focuses on bringing together researchers and practitioners from both industry and academia to tackle the security and privacy problem in intelligence systems. This special issue targets to provide a forum in which to publish state-of-the-art achievements in adversarial attack and defense for intelligence systems.

Main Topics and Quality Control

This special issue will contain the high-quality papers in adversarial attack and defense for intelligence systems. Main topics of interest include, but are not limited to:

- Adversarial attacks and defense on computational intelligence models and algorithms
- Adversarial example generation and protection against adversarial attacks
- Computational intelligence based security, privacy, and trust issues
- Detection of adversarial attacks against computational intelligence models and algorithms
- Increasing robustness of computational intelligence models and algorithms to adversarial attacks

IJCIS: Call for Papers Special Issue 'Adversarial Attack and Defense for Intelligence Systems'

ATLANTIS PRESS

- Security of intelligence systems and complex networks
- computational intelligence based anomalous behavior detection
- Data anonymization/de-anonymization
- Big data analytics for the security of intelligence systems
- Privacy-preserving data mining
- Attack and defense model generation based on computational intelligence
- Computational intelligence based intrusion and malware detection
- The robustness and data integrity of models
- Architectures and protocols for scalable, secure, robust and privacy enhancing
- Novel learning and data science methods for the security of intelligence systems
- Data mining and statistical modeling for the security of intelligence systems
- Data based metrics and risk assessment approaches for the security of intelligence systems

Full papers will be subject to a strict review procedure for final selection to this special issue based on the following criteria:

- Quality, originality and relevance in theory and methodology of adversarial attack and defense for intelligence systems;
- Extended papers must contain at least 40% new material (qualitative) relative to the conference paper.

Important Dates

Submission of papers:	**30 July 2020**
Notification of review results:	30 Sep 2020
Submission of revised papers:	30 Oct 2020
Notification of final review results:	30 Dec 2020

Submit your paper

All papers have to be submitted via the Editorial Manager online submission and peer review system. Instructions will be provided on screen and you will be stepwise guided through the process of uploading all the relevant article details and files associated with your submission. All manuscripts must be in the English language.

To access the online submission site for the journal, please visit https://www.editorialmanager.com/ij-cis/default.aspx. Note that if this is the first time that you submit to the International Journal of Computational Intelligence Systems, you need to register as a user of the system first.

NOTE: Before submitting your paper, please make sure to review the journal's Author Guidelines first.

IJCIS: Call for Papers Special Issue 'Adversarial Attack and Defense for Intelligence Systems'

ATLANTIS PRESS

Introduction of the guest editor(s)

Matthew Wright is the Director of the Center for Cybersecurity at RIT and a Professor of Computing Security. He graduated with his PhD from the Department of Computer Science at the University of Massachusetts in May, 2005. His dissertation work examined attacks and defenses for systems that provide anonymity online. His other interests include adversarial machine learning and understanding the human element of security. He has been the lead investigator on over $5.7 million in funded projects, including an NSF CAREER award, and he has published 100 peer-reviewed papers, including numerous contributions in the most prestigious venues focused on computer security and privacy.

Qi Yu is an Associate Professor from the Golisano College of Computing and Information Sciences at Rochester Institute of Technology, Rochester, New York, United States. He received the PhD degree in computer science from the Virginia Polytechnic Institute and State University (Virginia Tech). His current research interests lie in the areas of machine learning and data mining with applications in service computing and computing security. His publications have mainly appeared in top-tier venues in the field, including NeurIPS, ICML, IJCAI, and ICDM.

Xiangnan He is currently a Professor at School of Information Science and Technology in University of Science and Technology of China, He Fei, China. He received his Ph.D. in Computer Science from NUS. His research interests Adversarial Attack and Defense, Span Recommender System, Information Retrieval, Natural Language Processing and Multimedia. His work on recommender system has received the Best Paper Award Honorable Mention in WWW 2018 and SIGIR 2016. Moreover, he has served as the PC member for top-tier conferences including SIGIR, WWW, MM, KDD, WSDM, CIKM, AAAI, and ACL, and the invited reviewer for prestigious journals including TKDE, TOIS, TKDD, TMM, and WWWJ.

Liang Chen is an Associate Professor at School of Data and Computer Science in Sun Yat-Sen University, Guang Zhou, China. He received a PhD and a Bachelor's degree from Advanced Computing and System Laboratory (CCNT), College of Computer Science &Technology at Zhejiang University, China, respectively in 2015 and 2009. His research area includes Adversarial Learning, Graph Computing, Service Oriented Computing, Recommender System, and Edge Intelligence. His work on service recommendation has received the Best Paper Award Honorable Mention in ICSOC 2016. Moreover, he serves as the PC member of top conferences including SIGIR, ICWS, ICSOC, and the invited reviewer for journals including TNNLS, TKDD, TII, TSC, TKDE, and IOTJ.