Special Issue Proposal for Concurrency and Computation: Practice and Experience

--- Special Issue on Machine Learning for Cyber-security

Cyber security has become a very hot topic in the recent few years. Many communities, groups and governments start to realize the importance and urgency to deal with the ever-changing cyber attacks. Experts in the industry and scholars in the academia strive to innovate the next generation solutions. Among the technical solutions, machine learning based methods receive an increasingly popular favor due to its superior efficiency comparing with manual analysis. The general approach of machine-learning based cyber security solutions includes establishment of ground truth data, feature extraction and engineering, and model tuning. To perform these steps, one needs domain-specific knowledge in cyber security and insights to machine learning principles and skills.
Issues of combining machine learning and cyber security remain understudied particularly in the design and implementation of cyber security applications and solutions using machine learning, data mining and big data technologies.

Topics

The aim of the proposed Special Issue of CCPE is to promote research and reflect the most recent advances of cyber security applications and solutions using machine learning, data mining and big data technologies, with emphasis on the following aspects, but certainly not limited to:

- Malware detection and/or classification
- Spam and phishing detection
- Botnet detection
- Intrusion detection and intrusion prevention
- Social network abuse
- Cyber forensics
- Anomaly detection
- Vulnerability identification and/or testing
- Game theory related to machine learning and/or security
- Privacy issues related to machine learning for cyber security
- User authentication
- Adversarial machine learning

Paper Solicitation

This issue is an open special issue where everyone is encouraged to submit papers. We will solicit papers through two ways: conference and open call-for-papers.

1. **Selected Papers from the Australasian Workshop on Machine Learning for Cyber-security (AWMLC 2018)**

AWMLC 2018 covers research on theoretical and practical aspects related to machine learning for cyber security. The aim of AWMLC is to provide a cutting-edge forum to foster interaction and collaboration between researchers and industry practitioners with the machine learning and cyber security communities, and to give attendees an opportunity to interact with experts in academia, industry, and governments. The conference website is

http://nsclab.org/conferences/awmlc.html

We plan to select the papers relevant to cyber security issues from the accepted papers based on the reviews (comments and scores with respect to originality and correctness) and the presentations during the conferences. Each selected paper must be substantially extended, with at least 50% difference from its conference version.

2. **Open Call-For-Papers**

We plan to publicize an open call-for-papers (CFP) by listing the CFP in major academic announcement mailing lists/websites and by sending the CFP to researchers in the areas around the world. We estimate there will be a number of submissions via the open call-for-papers. Then we plan to select another a few papers from the submissions.

Each paper (including the selected papers from the conference) will go through a rigorous peer-review process by at least three international researchers. In total, we plan to include 8-12 papers in this special issue. The acceptance rate will be fairly low but we regard quality as our top priority. The anticipated readers of this Special Issue include both academic and industrial researchers working in relevant areas of security and privacy preserving.

Important Dates

Submission Due	August 1, 2018
1st Round Notification	October 1, 2018
Final Notification	November 1, 2018
Publication	2018/2019

Proposed Guest Editors

Dr. Lei Pan, E-mail: l.pan@deakin.edu.au
Deakin University, Australia

Dr. Jun Zhang, E-mail: junzhang@swin.edu.au
Swinburne University of Technology, Australia

Dr. Jonathan Oliver, E-mail: jon_oliver@trendmicro.com
Data Scientist and Director of Machine Learning Group, Trend Micro

Brief Biography of Guest Editors

Dr. Lei Pan received the Ph.D. degree in computer forensics from Deakin University, Melbourne, Australia, in 2008. He is with Deakin University, Burwood, Victoria, Australia. He is leading cyber security courses at Deakin University since 2015. He is the course director for Master of Cyber Security degree and deputy course director for Bachelor of Cyber Security degree. Dr. Pan has been coaching and mentoring students to participate security hackathons (Capture-The-Flag competitions) at the national and the international levels.

His research interests include the areas of cyber security and privacy, software security testing, the applications of analytics in security and privacy. He has an extensive list of published papers in international peer-reviewed conferences and high-ranking journals including

Nature's Scientific Reports, IEEE Transactions on Big Data, Science China, Elsevier Computers and Security, and so on.

He is also an active educator of cyber security on futurelearn.com. One of his designed course --- Cyber Security for Small and Medium Enterprises: Identifying Threats and Preventing Attacks, https://www.futurelearn.com/courses/cyber-security-business, has reached out 20,000+ learners from various sectors in business and security communities.

Dr. Jun Zhang received the Ph.D. degree in computer science from the University of Wollongong, Wollongong, Australia, in 2011. He is an Associate Professor in School of Software and Electrical Engineering, and the Deputy Director of Swinburne Cybersecurity Lab, Swinburne University of Technology, Australia. His research interests include cybersecurity and applied machine learning. He has published more than 80 research papers in refereed international journals and conferences, such as the IEEE/ACM Transactions on Networking (ToN), IEEE Transactions on Image Processing (TIP), IEEE Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Information Forensics and Security (TIFS), The ACM Conference on Computer and Communications Security (CCS) and ACM Asia Conference on Computer & Communications Security (ASIACCS). Dr Zhang has been internationally recognized as an active researcher in cybersecurity, evidenced by his chairing (PC Chair, workshop Chair, or Publicity Chair) of 7 international conferences from 2013, and presenting of invited keynote addresses in 2 conferences and an invited lecture in IEEE SMC Victorian Chapter.

Dr. Jonathan Oliver has been at Trend Micro for 11 years. His research has most recently focusing on machine learning modules for malware. Previous work has included machine learning and big data for the identification of ransomware outbreaks, BlackHole Exploit kit spam runs, and creating the antispam pattern.
Prior to joining Trend Micro, Dr Oliver served as Chief Spam Fighter and Director of Research at Mailfrontier; and as a data mining consultant in the Silicon Valley for organizations such as NASA and the FAA.
Jonathan Oliver holds a doctorate in information theoretic approaches to machine learning from Monash University, Melbourne. He holds more than 100 patents for technological designs.

Potential Reviewers

Potential reviewers are the experts in the research areas all over the world, who will be mainly selected from AWMLC 2018 program committees.