Security and Communication Networks

Special Issue on
AI-Driven Cyber Security Analytics and Privacy Protection

WILEY | Hindawi

CALL FOR PAPERS

The cyber security techniques have gone through a rapid development in today's internet connected world. With the wide application of the booming technologies such as the Internet of things (IoT) and cloud computing, huge amount of data is generated and collected. While the data can be used to better serve the corresponding business needs, it also poses big challenges for the cyber security and privacy protection. It becomes difficult to discover the malicious behavior among the big data in real time. Thus, this gives rise to the cyber security solutions which are driven by AI-based technologies, such as machine learning, statistical inference, big data analysis, and deep learning.

AI-driven cyber security analytics has already found its applications in the next generation firewall, automatic intrusion detection system, encrypted traffic identification, malicious software detection and so on. Researchers are now assisted by the AI-driven solution to optimize the algorithm design and reduce the cryptanalysis effort. Also automatic data protection solution based on the deep learning technology starts to appear in academia. On the other hand, individual's privacy is under threat given the AI-based systems. The rise of AI-enabled cyberattacks is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses. This brings the concern to defend AI-driven attacks by using AI-driven techniques, which could possibly lead to an AI arms race. AI-driven security solution is among the fastest growing fields which bring together researchers from multiple areas such as machine learning, statistics, big data analytics, network, and cryptography to fight against the advanced cyber security threats.

This special issue is focused on the cutting-edge research from both academia and industry, with a particular emphasis on the new tools, techniques, concepts, and applications concerning the AI-driven cyber security analytics and privacy protection. Only technical papers describing previously unpublished, original, state-of-the-art research and not currently under review by a conference or a journal will be considered. Extended work must have a significant number of "new and original" contributions along with more than 60% brand "new" material.

Potential topics include but are not limited to the following:

- Applications of machine learning in network security and privacy
- Automated design of cryptographic primitives
- Automated and intelligent cryptanalysis
- Automated Vulnerability Assessment/ Penetration Testing
- Cloud computing and social media security and privacy
- Cybercrime and cyberwar
- Denial of Service/ Distributed Denial of Service (DoS/DDoS)
- Intrusion detection/prevention systems
- Intelligent encrypted traffic identification
- Malware (Virus, Worms, Trojans, Backdoors) analysis
- Multiparty/multiagent access control
- Privacy and personal information protection

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/adcsa/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Jiageng Chen, Central China Normal University, Hubei, China
chinkako@gmail.com

Guest Editors
Chunhua Su, University of Aizu, Aizuwakamatsu, Japan
suchunhua@gmail.com

Zheng Yan, Xidian University, Xi'an, China
zheng.yan@aalto.fi

Submission Deadline
Friday, 12 October 2018

Publication Date
March 2019