Call for papers
Special Issue on

Interactions between artificial intelligence and cybersecurity to protect future networks

Lead Guest Editor

Dr. Gregory Blanc, Associate Professor, Institut Mines-Télécom/Télécom SudParis, Institut Polytechnique de Paris, France

Guest Editors

Dr. Yang Liu, Professor, Nanyang Technological University, Singapore
Dr. Rongxing Lu, Associate Professor, University of New Brunswick, Canada
Dr. Takeshi Takahashi, Research Manager, Cybersecurity Laboratory, National Institute of Information and Communications Technology, Koganei, Japan
Dr. Zonghua Zhang, Expert, Huawei France Research Center, Paris, France

Topics of interest include, but are not restricted to:

- AI for the Cybersecurity of next-generation networks
  - Anomaly detection
  - Malware detection
  - Botnet detection
  - Root cause analysis
  - Security information and event management
  - DPI and network forensics, including encrypted traffic analysis
  - Countermeasure selection
  - Moving Target Defense

    - Intelligent honeypots
    - Dataset generation
    - Attack generation
    - Adversarial examples and Robustness
    - Critical analysis of AI/ML applied to Cybersecurity
- Security of AI-based next-generation networks
    - Security and privacy in AI algorithms
    - Security in intelligent systems
    - Trust in AI platforms
    - Security and privacy of BigData processing
    - Formal verification of AI algorithms
    - Evasion/Deception of AI algorithms
    - Adversarial examples and Robustness

Artificial intelligence is the most dynamic research domain of this last decade, and as such has been increasingly penetrating other research domains, and all sectors of society. There is not a single application that AI researchers have not thought of improving with machine intelligence, from disease prognosis to crop management, to autonomous vehicles and facial recognition. Given the wealth of information produced in the era by next-generation networks (incl. virtualized networks, 5G, IoT), AI is expected to discover patterns and make predictions that no human can make, enhancing the efficiency of such networks on one hand, while offering new services on the other hand. In fact, it enables automation through the advance of AI-based decision-making. As such, reasoning is even more important than data analytics in assessing situations. Next-generation networks are thus critical assets that need to be protected as the society will be gradually relying on it, connecting every sector, from the home or workplace to the transport system or the hospital.

Cybersecurity may as well benefit from AI approaches for diverse tasks such as malware analysis, intrusion detection, log analysis, threat classification, with a goal to enhance the cybersecurity situation of next-generation networks. Amalgamations between AI and Cybersecurity have been ongoing for more than three decades, and both of them are recently experiencing a blooming stage due to the increasing deployment of next- generation networks in the society. On the one hand, AI offers tremendous capabilities to analyze the threats, risks and attacks in various networking systems, enabling comprehensive and in-depth defense strategies. For example, both supervised and unsupervised machine learning algorithms have been frequently used to detect intrusion, while reinforcement learning has the potential to discover optimal security countermeasures for a particular attack. There is also an emerging trend on utilizing AI to assess and improve cybersecurity measures, e.g., by generating evaluation datasets, which Cybersecurity is direly lacking, or predict new malware. On the

other hand, AI platforms, algorithms, and systems are attracting significant attention from the Cybersecurity community because of their increasing development, deployment, and application in our ICT infrastructure and services. For instance, the lack of interpretability of many deep learning models makes it extremely hard to defend against a sophisticated attack that either poisons data inputs and transformation, or exploits algorithm parameters and underlying software bugs. Recently, adversarial machine learning approaches have also prompted considerations for more critical thinking with respect to the adoption of AI-based systems, as next-generation network infrastructures that depend on them could be crippled by AI-related incidents then.

This special issue is focused at the intersection between AI and Cybersecurity for the benefit of next-generation networks, with an objective to bringing together the engineers, researchers, and practitioners from both AI and Cybersecurity communities in industry and academy, as well as stakeholders in next-generation networks, to explore together the emerging issues, topics, and solutions in the subjects listed above.

Papers must describe original research that advances state-of-the-art research and must not be simultaneously submitted to a journal or a conference with proceedings. Papers must be written in excellent English and should not exceed 20 pages. Previously published or accepted conference papers must contain at least 50% new material to be considered for the special issue. A covering letter to the Guest editors clearly describing the extensions made must accompany these types of submissions. All submissions must be made using the instructions available at:

http://annalsoftelecommunications.wp.mines-telecom.fr/how-to-publish/

The authors can directly submit their papers at: https://www.editorialmanager.com/ante/ and must select “Open Topic” in the menu “Choose Article Type” and then in the questionnaire on the “Additional Information” section, they will be able to select the item “CfP: Interactions between artificial intelligence and cybersecurity to protect future networks”.

Proposed Schedule

Manuscript Submission:	~~November 2, 2020~~, Extended to May 31, 2021
Author notification:	July 5, 2021
Revised papers submission:	August 30, 2021
Final acceptance:	September 30, 2021
Online with DOI	As soon as accepted
Printed issue	Second half of 2021

Dr. Gregory Blanc
Associate Professor
Institut Mines-Télécom/Télécom SudParis,
Institut Polytechnique de Paris
Evry-Courcouronnes, France
https://scholar.google.com/citations?user=9Tf1a1cAAAAJ

Gregory Blanc is currently an associate professor at Télécom SudParis, a school from the Institut Mines-Télécom (IMT), and a member of Institut Polytechnique de Paris. He is responsible for the last year specialization in networks and systems security of the engineering degree in ICT (Master's level) at Télécom SudParis since 2020. Dr. Blanc holds an engineering degree in ICT and a specialized Master in networks and information security from ESIEA, France, and a Ph.D degree obtained in 2012 from NAIST, Japan. He has been awarded the Lavoisier Japan Grant from the French Ministry of Foreign Affairs in 2009 and a grant for Non-Japanese Researcher from NEC C&C in 2011. Dr. Blanc has led the Security for Web 2.0 Application (SWAN) Working Group at the WIDE project, Japan from 2010 to 2012. His research interests mainly focus on cybersecurity, in particular network security with topics ranging from anomaly detection and access control to countermeasure selection and orchestration. Application areas focus on future and virtualized networks (5G, SDN/NFV, IoT). He has been coordinating and involved in several national and international (European, and jointly with Japan) research projects. Dr. Blanc is also a steering committee member of a domestic cybersecurity research and education conference, RESSI, and has served as TPC member in several cybersecurity conferences and journals.

Dr. Yang Liu
Professor
Nanyang Technological University
Singapore
https://scholar.google.com/citations?user=_Pvgwd0AAAAJ

Yang Liu obtained his bachelor and Ph.D degrees at the National University of Singapore in 2005 and 2010, respectively. In 2012, he joined Nanyang Technological University as a Nanyang Assistant Professor. He is currently a full professor, director of the cybersecurity laboratory, and Program Director of HP-NTU Corporate Lab, as well as Deputy Director of the National Satellite of Excellence of Singapore. In 2019, he received the University Leadership Forum Chair professorship at NTU. Dr. Liu specializes in software verification, security and software engineering. His research has bridged the gap between the theory and practical usage of formal methods and program analysis to evaluate the design and implementation of software for high assurance and security. By now, he has more than

300 publications in top-tier conferences and journals. He has received a number of prestigious awards including MSRA Fellowship, TRF Fellowship, Nanyang Assistant Professorship, Tan Chin Tuan Fellowship, Nanyang Research Award (2019), ACM Distinguished Speaker, NRF Investigatorship, and 10 best paper awards and one Most Influence System Award in top software engineering conferences (incl. ASE, FSE and ICSE).

Dr. Rongxing Lu

Associate Professor

University of New Brunswick, Fredericton, New Brunswick, Canada

https://scholar.google.com/citations?user=DeBXK0UAAAAJ

Rongxing Lu is an associate professor at the Faculty of Computer (FCS), University of New Brunswick (UNB), Canada. Before joining UNB in August 2016, he also worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore, from April 2013 to August 2016. Dr. Lu worked as a postdoctoral fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his Ph.D degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He is presently a senior member of IEEE Communications Society. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise (with 19,500+ citations and an h-index of 69, according to Google Scholar, as of June 2020), and was the recipient of 9 best (student) paper awards from some reputable journals and conferences. Currently, Dr. Lu serves as the Vice-Chair (conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). He is the winner of the 2016-17 Excellence in Teaching Award, FCS, UNB.

Dr. Takeshi Takahashi

Research Manager

Cybersecurity Laboratory, Cybersecurity Research Institute, National Institute of Information and Communications Technology, Koganei, Japan

https://scholar.google.com/citations?user=4AHBDgUAAAAJ

Takeshi Takahashi received a Ph.D degree in telecommunications from Waseda University in 2005. He was with Tampere University of Technology as a researcher from 2002 to 2004, and Roland Berger Ltd. as a business consultant from 2005 to 2009. Since 2009, he has been with the National Institute of Information and Communications Technology (NICT), Japan, where he is currently a research manager. In 2019-2020, he stayed at the University of California, Santa Barbara as a Visiting Research Scholar. His primary focus is

on cybersecurity. He has been leading a project on machine-learning- based cybersecurity since 2017. He is also active in standardization activities and serves as the IETF MILE Working Group chair and ITU-T Q.6/17 Associate Rapporteur. He received several awards including the Funai Information Technology Incentive Award and ITU Association Japan Incentive Award. He holds a CISSP certification.

Dr. Zonghua Zhang
Expert
Huawei France Research Center, Paris, France
https://scholar.google.com/citations?user=tPDhFn0AAAAJ

Zonghua Zhang is now working as an expert at Paris Research Center, Huawei Technologies France. Before diving into the industry, Zonghua has spent more than 15 years in academia at different institutions (professor at IMT, researcher at NICT). He holds an HDR diploma (UPMC, France) in computer science, and a Ph.D degree (JAIST, Japan) in information science. Dr. Zhang has been actively working at the intersection of networking, security, and machine learning. He has contributed, either as PI or key contributor, to more than a dozen national and international research projects, with topics ranging from anomaly detection, root cause analysis, and network forensics, to trust management, and eventually to autonomic cyberdefense. He has served as general chair or program chair for tens of international conferences, TPC member for numerous conferences, as well as editorial board member of four international journals. He is an IEEE senior member.

Springer
Published by Springer, *Annals of telecommunications*
is indexed in ISI and Scopus Databases, 2018 Impact Factor: 1.55
2087 *Journal Citation Reports* ® Science Edition (Thomson Reuters, 2019)
Institut Mines-Télécom