

**Title:**

AI-driven Network Detection, Defence and Testing

Abstract:

In recent years, artificial intelligence (AI), which has been considered as an emerging research field, is attracting a considerable amount of attention from both academia and industry. As a typical application, AI-driven network security plays an increasingly significant role in enhancing security of multiple network architectures, such as Software-Defined Networking (SDN), Internet of Things (IoT) and industrial Internet. In order to resolve various issues caused by malicious attacks or intrusions, recent emerging AI algorithms or approaches greatly promote the research and development of more powerful cyber security technologies, for example, various machine learning approaches are designed and recognized as critical intrusion detection engines to identify anomalous system activities. Additionally, AI-driven security technologies can improve their own performance to acquire more excellent effects on network detection, defence and testing.

Therefore, the target of this workshop is to focus on the state-of-art works with respect to AI-driven security technologies and applications, which can provide efficient solutions for the key security challenges of multiple network architectures.

Scope and Topics:

In this workshop, we aim to explore and debate recent advances related to all aspects of AI-driven security technologies, especially network detection, defence and testing. Moreover, we target to address challenges related to developing AI-driven security algorithms and approaches to guarantee the security of multiple network architectures. This workshop focuses on building a platform to share and discuss recent advances and future trends, and the workshop solicits novel papers on a broad range of topics, including but not limited to:

- ✧ AI-assisted Debugging, testing and security evaluation of SDN
- ✧ Security issues and AI-enhancements in SDN
- ✧ AI-assisted security applications over SDN
- ✧ AI-driven security and privacy in IoT
- ✧ AI-enabled authentication and access control in IoT
- ✧ AI-assisted edge trusted computing in IoT
- ✧ AI-driven intrusion detection in Industrial Internet
- ✧ AI-assisted vulnerabilities analysis and risk assessment in Industrial Internet
- ✧ AI-enabled prevention, awareness and resilience models for Industrial Internet



Program Committee Chairs:

Jiangyuan Yao, Hainan University, China

yaojy@hainu.edu.cn

<https://www.linkedin.com/in/jiangyuan-yao/>

Jiangyuan Yao, received the B.E, M.E and Ph.D. degrees from Shandong University of Science and Technology, Beijing Jiaotong University and Tsinghua University, in 2007, 2009 and 2015, respectively. He is now working as an Associate Professor in the School of Computer Science and Cyberspace Security, Hainan University. His research interests include protocol testing and cyberspace security.

Zhiliang Wang, Tsinghua University, China

wzl@cernet.edu.cn

<http://netarchlab.tsinghua.edu.cn/~wzl/index.html>

Zhiliang Wang received the B.E., M.E. and Ph.D. degrees in computer science from Tsinghua University, China in 2001, 2003 and 2006 respectively. Currently he is an Associate Professor in the Institute for Network Sciences and Cyberspace at Tsinghua University. His research interests include formal methods and protocol testing, next generation Internet, network measurement.

Arun Kumar Sangaiah, VIT University, India

arunkumarsangaiah@gmail.com

<https://in.linkedin.com/in/dr-arun-kumar-sangaiah-081452a9>

ARUN KUMAR SANGAIAH had received his Ph.D. degree in computer science and engineering from the VIT University, Vellore, India. He is presently working as an associate professor in School of Computer Science and Engineering, VIT University, India. His area of interest includes software engineering, computational intelligence, wireless networks, bio-informatics, and embedded systems.

Ming Wan, Liaoning University, China

wanming@lnu.edu.cn

<http://enweb.lnu.edu.cn/info/15074/1963.htm>

Ming Wan received the B.S. degree from Beijing Jiaotong University in 2007, and the Ph.D. degree in communication and information system from the National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, in 2013. He also worked at the Key Laboratory of Networked Control System, Shenyang Institute of Automation, Chinese Academy of Sciences from 2013 to 2017. Now, he is an Associate Professor at School of Information, Liaoning University. Since 2018, he become one expert of ICSISIA think-tank, and is an industrial information security expert of Liaoning Province. His research interests include network and information security, machine learning and industrial control network security.



Program Committee:

Haijun Geng, Shanxi University, China

Guangwu Hu, Shenzhen Institute of Information Technology, China

Fuliang Li, Northeastern University, China

Changhua Pei, Ali Research Institute, China

Meng Shen, Beijing Institute of Technology, China

Xingang Shi, Tsinghua University, China

Wenqi Sun, Huawei Technologies Co., LTD, China

Tian Pan, Beijing University of Posts and Telecommunications, China

Jianming Zhao, Shenyang Institute of Automation, Chinese Academy of Sciences,
China

Sen Wang, Chongqing University, China

Yang Xu, New York University, USA

Shenglin Zhang, Nankai University, China