The 3rd International Workshop on Machine Learning for Trust, Security and Privacy in Computing and Communications (MLTrustCom 2022)

In conjunction with
The 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications
(IEEE TrustCom 2022)

28-23 October 2022, Wuhan, China

Scope

In recent years, supervised machine learning methods (e.g. k nearest neighbors, Bayes' theorem, decision tree, support vector machine, random forest, neural network, convolutional neural network, recurrent neural network, long short-term memory network, gated recurrent unit network), unsupervised machine learning methods (e.g. association rules, k-means, density-based spatial clustering of applications with noise, hierarchical clustering, deep belief networks, deep Boltzmann machine, auto-encoder, de-noising auto-encoder, etc.), reinforcement learning methods (e.g. generative adversarial network, deep Q network, trust region policy optimization, etc.) and federated learning methods have been applied to trust, security and privacy in computing and communications. For instance, machine learning methods have been used to analyze the behaviors of the data stream in networks and extract the patterns of malicious activities (packet dropping, worm propagation, jammer attacks, etc.) for generating rules in intrusion detection systems. Furthermore, time-series methods (e.g. local outlier factor, cumulative sum, adaptive online thresholding, etc.) have been proposed to retrieve the time-series features of anomalous behaviors for preventing cyber-attacks and malfunctions.

While the area of machine learning methods for trust, security and privacy in computing and communications is a rapidly expanding field of scientific research, several open research questions are still needed to be discussed and studied. For instance, using and improving machine learning methods for malicious activity detection, attack detection, mobile endpoint analyses, repetitive security task automation, zero-day vulnerability prevention and other security applications are the important issues in computing and communications. In addition, with the development of chip technology and network technology, all kinds of wireless communication terminals are booming. Wireless communication terminal needs the support of wireless network, so wireless signal coverage becomes more and more important, and its security problem becomes more and more prominent. This workshop named "Machine Learning for Trust, Security and Privacy in Computing and Communications" in conjunction with the 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2022) will solicit papers on the following topics across various disciplines of trust, security and privacy in computing and communications.

Topics

- New unsupervised machine learning methods for trust, security and privacy in computing and communications
- New reinforcement learning methods for trust, security and privacy in computing and communications
- New federated learning methods for trust, security and privacy in computing and communications

- New optimization methods for trust, security and privacy in computing and communications
- Intelligent Traffic System：
- New machine learning methods for trust, security and privacy in car following model
- New machine learning methods for trust, security and privacy in communication of intelligent connected vehicles
- The security of the connected and autonomous vehicles model
- Security analysis of connected and autonomous vehicles
- New machine learning methods for indoor location signal coverage
- New safety methods for indoor signal strength
- New machine learning methods for trust, security and Privacy optimization in indoor signal communication

Important Dates:

Paper Submission Deadline	July 1, 2022
Author Notification	August 15, 2022
Camera-Ready Paper Due	September 22, 2021
Conference Dates	October 28-23, 2022

Organizing Committee

Steering Committee

- Prof. Jun-Huai Li (Xi'an University of Technology, China)
- Prof. Xinhong Hei (Xi'an University of Technology, China)

General Chairs

- Prof. Rong Fei (Xi'an University of Technology, China)

Session Chairs

- Prof. Qing-Zheng Xu (National University of Defense technology, China)
- Prof. Feng-Jang Hwang (University of Technology Sydney, Australia)

Technical Program Committee

- Prof. Yong You (Northwestern Polytechnical University, China)
- Prof. Xiguo Yuan (Xidian University, China)
- Prof. Qiang Yu (Xidian University, China)
- Prof. Li Zhao (Beijing Technology and Business University, China)
- Prof. Chi-Hua Chen (Fuzhou University, China)

Contact

Prof. Rong Fei, Email: annyfei@xaut.edu.cn

Submission

Papers should be submitted through the EDAS-
https://edas.info/newPaper.php?c=29933&track=113491