Journal of Computer Networks and Communications

Hindawi

Special Issue on
Advances in Machine Learning for Cybersecurity

CALL FOR PAPERS

Cybersecurity encompasses the protection of physical and cyber assets from damage and theft, as well as preventing the misdirection or disruption of services provided by electronic means. Damage can occur in several ways and forms, including via code and data injection, network access, or even malpractice by operators. Cybersecurity tasks, based on Gartner's PPDR model, can be split into five categories: prediction, prevention, detection, response, and monitoring.

Modern cyberattacks utilize sophisticated techniques to bypass security countermeasures. To overcome these in prediction, prevention, detection, and monitoring tasks, state-of-the-art security techniques are integrated with artificial intelligence in order to sense anomalies and model and detect threats. This is achieved by deploying diverse machine learning methods.

Pairing cybersecurity solutions with machine learning is the most advanced approach to identify flaws and weaknesses, especially in large organizations where the large number of devices and users increases the potential for security breaches. This new approach includes turning to big data platforms to extend data accessibility and machine learning for detection of advanced persistent threats. However, this combination does not yet always work perfectly, and it requires continuous adjustments to refine and improve its monitoring capabilities and boost its functionality in finding and mitigating actual breaches before serious damage has occurred.

Potential topics include but are not limited to the following:

- Machine learning techniques for network intrusion detection
- Machine learning techniques for phishing detection
- Machine learning techniques for malware detection
- Machine learning techniques for spam and fake profile detection in social networks
- Machine learning techniques for steganalysis and cryptography
- Machine learning techniques for testing security properties of protocols
- Machine learning techniques for authentication systems
- Machine learning techniques for smart meter energy consumption profiling
- Machine learning techniques for identification and protection of IoT vulnerabilities
- Machine learning techniques for identifying exploits and zero-day threats

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

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

Lead Guest Editor
Mazdak Zamani, Felician University, New Jersey, USA
zamani.mazdak@gmail.com

Guest Editors
Saman S. Chaeikar, K. N. Toosi University of Technology, Tehran, Iran
sschaeikar@mail.kntu.ac.ir

Arash H. Lashkari, University of New Brunswick, Fredericton, Canada
a.habibi.l@unb.ca

Submission Deadline
Friday, 7 June 2019

Publication Date
October 2019