ACM WiseML 2021

CALL FOR PAPERS

ACM Workshop on Wireless Security and Machine Learning (WiseML 2021)

In conjunction with ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2021)

July 2, 2021

https://sites.nyuad.nyu.edu/wisec21/wiseml2021/

The ACM Workshop on Wireless Security and Machine Learning (WiseML 2021) will be held in conjunction with the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2021). The workshop will be held virtually with online presentations. Accepted papers will appear in the conference proceedings and the ACM digital library.

Scope and background:

Artificial intelligence (AI) and machine learning (ML) have proven to be invaluable tools for a diverse and far-reaching set of applications in wireless communications, networking, security, and situational awareness. ML systems based upon state-of-the-art neural network architectures, powered by the ever-more powerful hardware accelerators for computing, have been deployed for spectrum sensing applications (signal detection, estimation, classification, and identification), channel estimation and feedback, coding, waveform design, emitter identification, cognitive jamming and anti-jamming, among many others.

ML has emerged as a viable solution to effectively learn from spectrum data, solve complex tasks for IoT, 5G and beyond, and secure the emerging communication systems against adversaries. Recent research has demonstrated the efficacy of adversarial ML (AML) techniques to negatively impact the performance of ML based wireless systems. Consequently, the impact of AML on wireless technologies requires better understanding. On the other hand, the proliferation of wireless devices operating with diverse communication technologies in heterogenous spectrum environments has made them susceptible targets to various attacks. Harnessing efficient, robust AI/ML algorithms for wireless security that can operate under constrained power and computational resources, is of paramount importance for guaranteeing the integrity of wireless communications. Undoubtedly, an effort to investigate the interactions between ML and wireless security, privacy, and robustness, would be both timely and indispensable.

The purpose of this workshop is to bring together members of the ML, privacy, security, wireless communications and networking communities from around the world and offer them the opportunity to share the latest research findings in these emerging and critical areas, as well as to exchange ideas and foster research collaborations, in order to further advance the state-of-the-art.

Topics of Interest (but not limited to):

- *Adversarial ML Techniques*
  - Adversarial examples
  - Poisoning attacks
  - Trojan/backdoor attacks
  - Generative adversarial learning
  - Spoofing attacks
  - Defense techniques
  - Adversarial reinforcement learning
- *Strengthening ML Solutions*
  - Datasets
  - Data augmentation
  - Privacy-preserving learning
  - Secure learning
  - Federated learning
  - Certified defense
  - Uncertainty quantification
  - Information discovery
  - Cognitive radio
  - Hardware solutions
  - Embedded computing
  - Experiments and testbeds
- *Privacy & Security Issues of ML Solutions*
  - Differential privacy
  - Information theoretic privacy
  - Physical layer privacy
  - Membership inference attacks
  - Model inversion
- *ML Applications*
  - 5G/IoT security
  - Network slicing
  - Network virtualization
  - Anonymity
  - Authentication
  - Covert communications
  - Device identification
  - Intrusion detection
  - Localization
  - RF fingerprinting
  - Smart jamming and spoofing
  - Security for mobile autonomous multi-agent platforms

Workshop Chairs:

Dr. Deniz Gunduz, Imperial College London
Dr. M Cenk Gursoy, Syracuse University
Dr. Brian Jalaian, US Army Research Laboratory
Dr. Yalin E. Sagduyu, Intelligent Automation Inc.
Dr. Yi Shi, Virginia Tech
Dr. George Stantchev, US Naval Research Laboratory

Steering Committee:

Dr. Wenjing Lou, Virginia Tech
Dr. Alan Michaels, Virginia Tech
Dr. Stephen Russell, US Army Research Lab

Dr. Sennur Ulukus, University of Maryland
Dr. K.P. (Suba) Subbalakshmi, Stevens Institute of Technology

Submission Guidelines:

Submission site: https://wiseml21.hotcrp.com
Workshop Papers must be written in English, must be formatted in the standard ACM conference style, and are not to exceed **six** pages. Accepted papers will appear in the conference proceedings and the ACM digital library.
Only PDF files will be accepted for the review process. All papers must be thoroughly anonymized for double-blind reviewing.

Important Dates:

Paper Submission Deadline:	April 1, 2021
Acceptance Notification:	May 1, 2021
Camera-Ready Paper Submission:	June 1, 2021
Workshop Event:	July 2, 2021