ACM WiseML 2019

CALL FOR PAPERS

ACM Workshop on Wireless Security and Machine Learning (WiseML 2019)

In Conjunction with ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019)

May 14, 2019, Miami, FL, USA

https://wisec19.fiu.edu/workshops-wiseml

The ACM Workshop on Wireless Security and Machine Learning (WiseML 2019) will be held in conjunction with the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019) in Miami, USA, on May 14, 2019.

Scope and background:

Artificial Intelligence (AI) and Machine Learning (ML) have been found to be invaluable tools for a diverse and far-reaching set of applications ranging from traditionally thought of image recognition and natural language processing applications to cyber security and autonomous navigation. In recent years, applications of AI/ML have emerged in the wireless communications domain, forming a major ingredient of a more general topic area, colloquially referred to as Radio Frequency Machine Learning (RFML). In particular, ML systems based upon state-of-the-art deep learning architectures, powered by the ever-increasing hardware accelerations for computing, have been deployed for spectrum sensing applications (signal detection, estimation, classification, and identification), channel estimation, emitter identification, cognitive jamming and anti-jamming, among many others.

In the more established AI/ML domains, recent research has demonstrated the efficacy of utilizing Adversarial Machine Learning (AML) to negatively impact the performance of AI/ML systems. Additionally, vulnerabilities to the privacy and security of these systems, and the data used to train the systems, has been exposed. However, the impact of these concepts to RFML technologies is at present underdeveloped. Therefore, it is a timely research effort to investigate the interaction of RFML with wireless security, privacy, and robustness.

Given these facts, the purpose of this workshop is to bring together members of the AI/ML, RFML, privacy, security, and wireless communications communities from around the world in order for them 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 in security techniques, architectures, and algorithms for AI/ML in wireless communications.

Topics of Interest (but not limited to):

- *Adversarial ML Techniques*
  - Evasion attacks
  - Poisoning attacks
  - Trojan/backdoor attacks
  - Generative adversarial learning
- *Hardening ML Solutions*
  - Intrusion detection
  - Physical unclonable function (PUF)
  - Privacy-preserving learning
  - Secure learning
  - Hardware and software implementations
  - Testbeds and experiments
  - Datasets
- *Privacy & Security Issues of ML Solutions*
  - Membership inference attacks
  - Model inversion
  - Physical layer privacy/privacy
- *Relevant ML Applications*
  - Device identification
  - RF fingerprinting
  - Smart jamming
  - Localization
  - Covert communications
  - Authentication
  - Anonymity
  - Intrusion detection
  - IoT security

Workshop Chairs:

Dr. William C. Headley, Virginia Tech
Dr. Zhuo Lu, University of South Florida
Dr. Yalin E. Sagduyu, Intelligent Automation Inc.
Dr. Yi Shi, Intelligent Automation Inc. and Virginia Tech

Steering Committee:

Dr. Wenjing Lou, Virginia Tech
Dr. Alan Michaels, Virginia Tech
Dr. George Stantchev, Naval Research Laboratory
Dr. Sennur Ulukus, University of Maryland

Submission Guidelines:

Submission site: https://wiseml19.hotcrp.com
Workshop Extended Abstracts must be written in English, must be formatted in the standard ACM conference style, and are not to exceed three pages.
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 Adobe PDF files will be accepted for the review process of both abstracts and papers.

Important Dates:

Extended Abstract Submission Deadline:	April 15, 2019
Acceptance Notification:	April 25, 2019
Camera-Ready Paper Submission:	May 2, 2019
Workshop Event:	May 14, 2019