WiseML ’20
Proceedings of the 2nd ACM Workshop on
Wireless Security and Machine Learning

Sponsored by:

ACM SIGSAC in cooperation with ACM SIGMOBILE

Supported by:

Johannes Kepler University Linz, Institute of Networks and Security
Message from the Chairs

We are very pleased to welcome you to the 2nd ACM Workshop on Wireless Security and Machine Learning. This year’s WiseML is a virtual workshop and we are both excited to try out this workshop format and regretful not to be able to welcome you in the beautiful city of Linz, Austria, due to the ongoing COVID-19 pandemic. ACM WiseML 2020 continues to be the premier venue to bring together members of the AI/ML, privacy, security, wireless communications and networking communities from around the world, and to offer them the opportunity to share their 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. The program will be presented online in a single track. WiseML 2020 will be open at no extra cost to everyone and we are trying out new formats such as a mixture of live streams, pre-recorded talks, and interactive Q/A sessions.

The technical program this year features 14 outstanding papers that cover a wide variety of security and privacy problems in adversarial machine learning relating to wireless networking, mobile networks, IoT systems, cyber physical systems, cognitive radios, and emerging applications. These papers were carefully reviewed by 8 technical program committee (TPC) chairs and external experts from academia, industrial research labs, and federal organizations. Despite the ongoing COVID-19 pandemic, we managed to stick to our timeline with tight time constraints on the review and decision process. We would also like to thank authors for finalizing their papers promptly despite the tight timeline. WiSec's exciting technical program is enriched by two keynote talks delivered by distinguished leaders in the field of machine learning for wireless and mobile security and privacy: Dr. Charles Clancy from MITRE Corporation, Virginia, US and Prof. Mauro Conti from the University of Padua, Padua, Italy. Warm thanks to both keynote speakers for joining us.

There has been a great team work effort to make WiseML 2020 a success. We would like to thank authors, reviewers, and WiSec 2020 organizing team for their hard work and contributions. First, we thank all the authors who submitted their great research to the workshop. We are truly grateful to all the reviewers who contributed to the decision process. We also thank the WiSec 2020 organizing team, especially the General Chairs Rene Mayrhofer and Michael Roland, the Publication Co-Chairs Max Maaß and Yao Zheng, the Web Chair Daniel Hofer, for their tremendous support for the WiseML workshop. We also thank and appreciate the WiseML Steering Committee for their technical guidance. Finally, welcome to WiseML 2020 and enjoy the first online WiseML!
René Mayrhofer
General Co-Chairs
Johannes Kepler University Linz
Linz, AT

Michael Roland
General Co-Chairs
Johannes Kepler University Linz
Linz, AT

Deniz Gunduz
Program Co-Chairs
Imperial College London
London, UK

Brian Jalaian
Program Co-Chairs
Army Research Laboratory
Adelphi, US

Marc Kurz
Program Co-Chairs
University of Applied Sciences Upper Austria
Hagenberg, AT

Berhard Moser
Program Co-Chairs
Software Competence Center
Hagenberg, AT

Yalin E. Sagduyu
Program Co-Chairs
Intelligent Automation Inc.
Rockville, US

Yi Shi
Program Co-Chairs
Intelligent Automation Inc.
Rockville, US

George Stantchev
Program Co-Chairs
Naval Research Laboratory
Washington, DC, US

Max Maaß
Publication Co-Chairs
TU-Darmstadt
Darmstadt, DE

Yao Zheng
Publication Co-Chairs
University of Hawaii at Manoa
Honolulu, US
### Contents

**Generative Adversarial Attacks Against Intrusion Detection System Using Active Learning** ........................................ 1  
Dule Shu (Carnegie Mellon University); Nandi Leslie, Charles Kamhoua (Army Research Laboratory (ARL)); Conrad Tucker (Carnegie Mellon University)

**Open Set Recognition through Unsupervised and Class-Distance Learning** .................................................. 7  
Andrew Draganov, Carter Brown, Enrico Mattei, Cass Dalton (Expedition Technology); Jaspreet Ranjit (Department of Computer Science, University of Virginia, Charlottesville, VA)

**Adversarial machine learning based partial-model attack in IoT** ................................................................. 13  
Zhengping Luo, Shangqing Zhao, Zhuo Lu (University of South Florida); Yalin E. Sagduyu (Intelligent Automation Inc.); Jie Xu (University of Miami)

**Wideband Spectral Monitoring Using Deep Learning** .................................................................................. 19  
Horacio Franco, Chris Cobo-Kroenke, Stephanie Welch, Martin Graciarena (SRI International)

**Machine Learning-Driven Intrusion Detection for Contiki-NG-Based IoT Networks Exposed to NSL-KDD Dataset** ................................................................. 25  
Jinxin Liu, Burak Kantarci, Carlisle Adams (University of Ottawa)

**Data Augmentation with Conditional GAN for Automatic Modulation Classification** .................................. 31  
Mansi Patel, Xuyu Wang (California State University, Sacramento); Shiwen Mao (Auburn University)

**Algorithm Selection Framework for Cyber Attack Detection** ................................................................. 37  
Marc Chale (AFIT); Nathaniel Bastian (Army Cyber Institute); Jeffery D Weir (AFIT)

**Investigating a Spectral Deception Loss Metric for Training Machine Learning-based Evasion Attacks** .................................................................................. 43  
Matthew DelVecchio, William C. Headley, Vanessa Arndorfer (Virginia Tech Hume Center)

**Generalized Wireless Adversarial Deep Learning** .................................................................................. 49  
Francesco Restuccia, Salvatore D’Oro, Amani Alshawabka, Bruno Costa Rendon, Kaushik Chowdhury, Stratis Ioannidis, Tommaso Melodia (Northeastern University)

**Encrypted Rich-data Steganography using Generative Adversarial Networks** ........................................ 55  
Dule Shu (Carnegie Mellon University); Weilin Cong, Jiaming Chai (Penn State); Conrad Tucker (Carnegie Mellon University)

**Over-the-Air Membership Inference Attacks as Privacy Threats for Deep Learning-based Wireless Signal Classifiers** ................................................................. 61  
Yi Shi, Kemal Davaslioglu, Yalin Sagduyu (Intelligent Automation Inc.)

**A Network Security Classifier Defense: Against Adversarial Machine Learning Attacks** .................. 67  
Michael J. De Lucia (U.S. Army Research Laboratory); Chase Cotton (University of Delaware)

**Deep Learning Based Wiretap Coding via Mutual Information Estimation** ........................................ 74  
Rick Fritschek (Freie Universität Berlin); Rafael F. Schaefer (Technische Universität Berlin); Gerhard Wunder (Freie Universität Berlin)
Detecting Acoustic BackDoor Transmission of Inaudible Messages Using Deep Learning

Silvija Kokalj-Filipovic (Perspecta Labs, Inc); Morriel Kasher, Michael Zhao, Predrag Spasojevic (Rutgers University)