

July 13, 2020
Linz (Virtual Event), Austria



Association for
Computing Machinery

Advancing Computing as a Science & Profession



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



**Association for
Computing Machinery**

Advancing Computing as a Science & Profession

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York, New York 10121-0701

Copyright © 2020 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from permissions@acm.org or Fax +1 212 869-0481.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through www.copyright.com.

Notice to Past Authors of ACM-Published Articles

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-8007-2

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: +1 800 342-6626 (USA and Canada)

+1 212 626-0500 (Global)

Fax: +1 212 944-1318

Email: acmhelp@acm.org

Hours of Operation: 8:30 am–4:30 pm ET

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

Deniz Gunduz

Program Co-Chairs
Imperial College London
London, UK

Marc Kurz

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

Yalin E. Sagduyu

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

Michael Roland

General Co-Chairs
Johannes Kepler University Linz
Linz, AT

Brian Jalaian

Program Co-Chairs
Army Research Laboratory
Adelphi, US

Berhard Moser

Program Co-Chairs
Software Competence Center
Hagenberg, AT

Yi Shi

Program Co-Chairs
Intelligent Automation Inc.
Rockville, US

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 (<i>Carnegie Mellon University</i>); Nandi Leslie, Charles Kamhoua (<i>Army Research Laboratory (ARL)</i>); Conrad Tucker (<i>Carnegie Mellon University</i>)	
Open Set Recognition through Unsupervised and Class-Distance Learning	7
Andrew Draganov, Carter Brown, Enrico Mattei, Cass Dalton (<i>Expedition Technology</i>); Jaspreet Ranjit (<i>Department of Computer Science, University of Virginia, Charlottesville, VA</i>)	
Adversarial machine learning based partial-model attack in IoT	13
Zhengping Luo, Shangqing Zhao, Zhuo Lu (<i>University of South Florida</i>); Yalin E. Sagduyu (<i>Intelligent Automation Inc.</i>); Jie Xu (<i>University of Miami</i>)	
Wideband Spectral Monitoring Using Deep Learning	19
Horacio Franco, Chris Cobo-Kroenke, Stephanie Welch, Martin Graciarena (<i>SRI International</i>)	
Machine Learning-Driven Intrusion Detection for Contiki-NG-Based IoT Networks Exposed to NSL-KDD Dataset	25
Jinxin Liu, Burak Kantarci, Carlisle Adams (<i>University of Ottawa</i>)	
Data Augmentation with Conditional GAN for Automatic Modulation Classification	31
Mansi Patel, Xuyu Wang (<i>California State University, Sacramento</i>); Shiwen Mao (<i>Auburn University</i>)	
Algorithm Selection Framework for Cyber Attack Detection	37
Marc Chale (<i>AFIT</i>); Nathaniel Bastian (<i>Army Cyber Institute</i>); Jeffery D Weir (<i>AFIT</i>)	
Investigating a Spectral Deception Loss Metric for Training Machine Learning-based Evasion Attacks	43
Matthew DelVecchio, William C. Headley, Vanessa Arndorfer (<i>Virginia Tech Hume Center</i>)	
Generalized Wireless Adversarial Deep Learning	49
Francesco Restuccia, Salvatore D'Oro, Amani Alshawabka, Bruno Costa Rendon, Kaushik Chowdhury, Stratis Ioannidis, Tommaso Melodia (<i>Northeastern University</i>)	
Encrypted Rich-data Steganography using Generative Adversarial Networks	55
Dule Shu (<i>Carnegie Mellon University</i>); Weilin Cong, Jiaming Chai (<i>Penn State</i>); Conrad Tucker (<i>Carnegie Mellon University</i>)	
Over-the-Air Membership Inference Attacks as Privacy Threats for Deep Learning-based Wireless Signal Classifiers	61
Yi Shi, Kemal Davaslioglu, Yalin Sagduyu (<i>Intelligent Automation Inc.</i>)	
A Network Security Classifier Defense: Against Adversarial Machine Learning Attacks	67
Michael J. De Lucia (<i>U.S. Army Research Laboratory</i>); Chase Cotton (<i>University of Delaware</i>)	
Deep Learning Based Wiretap Coding via Mutual Information Estimation	74
Rick Fritschek (<i>Freie Universität Berlin</i>); Rafael F. Schaefer (<i>Technische Universität Berlin</i>); Gerhard Wunder (<i>Freie Universität Berlin</i>)	

Detecting Acoustic BackDoor Transmission of Inaudible Messages Using Deep Learning 80

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