AAAI Workshops 2018

Technical Report WS-08

New Orleans, Louisiana, USA
2 – 3 February 2018

ISBN: 978-1-7138-2750-4

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571

Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2018) by Association for the Advancement of Artificial Intelligence
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact Association for the Advancement of Artificial Intelligence
at the address below.

Association for the Advancement of Artificial Intelligence
2275 East Bayshore Road
Suite 160
Palo Alto, California 94303
USA

Phone: 1-650-328-3123
Fax: 1-650-321-4457

https://aaai.org/Press/press.php

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

EVALUATION OF PREDICTIVE MODELS FOR WILDLIFE POACHING ACTIVITY THROUGH CONTROLLED FIELD TEST IN UGANDA 344
Shahrzad Gholami, Benjamin Ford, Debarun Kar, Fei Fang, Milind Tambe, Andrew Plumptre, Margaret Driciru, Fred Wanyama, Aggrey Rwetsiba, Mustapha Nsubaga, Joshua Mabonga

AUTONOMOUS MODEL MANAGEMENT VIA REINFORCEMENT LEARNING 348
Elad Liebman, Eric Zavesky, Peter Stone

CAN WE ACHIEVE OPEN CATEGORY DETECTION WITH GUARANTEES? 356
Si Liu, Risheek Garrepalli, Alan Fern, Thomas G. Dietterich

DENOISING DICTIONARY LEARNING AGAINST ADVERSARIAL PERTURBATIONS 364
John Mitro, Derek Bridge, Steven Prestwich

OPTIMIZING HIERARCHICAL CLASSIFICATION WITH ADAPTIVE NODE COLLAPSES 372
Sujan Perera, Orna Raz, Ramani Routray, Shenghua Bao, Marcel Zalmanovici

MTDEEP: BOOSTING THE SECURITY OF DEEP NEURAL NETS AGAINST ADVERSARIAL ATTACKS WITH MOVING TARGET DEFENSE 376
Sailik Sengupta, Tathagata Chakraborti, Subbarao Kambhampati

MULTIPLE-IMPLEMENTATION TESTING OF SUPERVISED LEARNING SOFTWARE 384
Siwakorn Srisakaokul, Zhengkai Wu, Angello Astorga, Oreoluwa Alebiosu, Tao Xie

CLIMBING THE KAGGLE LEADERBOARD BY EXPLOITING THE LOG-LOSS ORACLE 392
Jacob Whitehill

TELEMADE: A TESTING FRAMEWORK FOR LEARNING-BASED MALWARE DETECTION SYSTEMS 400
Wei Yang, Tao Xie

DISTRIBUTED DEEP LEARNING UNDER DIFFERENTIAL PRIVACY WITH THE TEACHER-STUDENT PARADIGM 404
Jun Zhao

Author Index