Lecture Notes in Computer Science 12486

Founding Editors

Gerhard Goos
Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis
Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino
Purdue University, West Lafayette, IN, USA

Wen Gao
Peking University, Beijing, China

Bernhard Steffen
TU Dortmund University, Dortmund, Germany

Gerhard Woeginger
RWTH Aachen, Aachen, Germany

Moti Yung
Columbia University, New York, NY, USA

More information about this series at http://www.springer.com/series/7410

Xiaofeng Chen · Hongyang Yan ·
Qiben Yan · Xiangliang Zhang (Eds.)

Machine Learning for Cyber Security

Third International Conference, ML4CS 2020
Guangzhou, China, October 8–10, 2020
Proceedings, Part I

Springer

Editors
Xiaofeng Chen
Xidian University
Xi'an, China

Qiben Yan
Michigan State University
East Lansing, MI, USA

Hongyang Yan
Guangzhou University
Guangzhou, China

Xiangliang Zhang
Division of Computer, Electrical
and Mathematical Sciences and Engineering
King Abdullah University of Science
Thuwal, Saudi Arabia

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-62222-0 ISBN 978-3-030-62223-7 (eBook)
https://doi.org/10.1007/978-3-030-62223-7

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The Third International Conference on Machine Learning for Cyber Security (ML4CS 2020) was held in Guangzhou, China, during October 8–10, 2020. ML4CS is a well-recognized annual international forum for AI-driven security researchers to exchange ideas and present their works. This volume contains papers presented at ML4CS 2020.

The conference received 360 submissions. The committee accepted 118 regular papers and 40 short papers to be included in the conference program. The proceedings contain revised versions of the accepted papers. While revisions are expected to take the referees comments into account, this was not enforced and the authors bear full responsibility for the content of their papers.

ML4CS 2020 was organized by the Institute of Artificial Intelligence and Blockchain, Guangzhou University, China. Furthermore, ML4CS 2020 was supported by the Peng Cheng Laboratory, Shenzhen, China. The conference would not have been such a success without the support of these organizations, and we sincerely thank them for their continued assistance and support.

We would also like to thank the authors who submitted their papers to ML4CS 2020, and the conference attendees for their interest and support. We thank the Organizing Committee for their time and effort dedicated to arranging the conference. This allowed us to focus on the paper selection and deal with the scientific program. We thank the Program Committee members and the external reviewers for their hard work in reviewing the submissions; the conference would not have been possible without their expert reviews. Finally, we thank the EasyChair system and its operators, for making the entire process of managing the conference convenient.

September 2020

Fengwei Zhang
Jin Li

Organization

General Chairs

Fengwei Zhang	Southern University of Science and Technology, China
Jin Li	Guangzhou University, China

Program Chairs

Xiaofeng Chen	Xidian University, China
Qiben Yan	Michigan State University, USA
Xiangliang Zhang	King Abdullah University of Science and Technology, Saudi Arabia

Track Chairs

Hao Wang	Shandong Normal University, China
Xianmin Wang	Guangzhou University, China
Yinghui Zhang	Xi'an University of Posts and Telecommunications, China
Wei Zhou	Yunnan University, China

Workshop Chairs

Sheng Hong	Beihang University, China
Ting Hu	Queen's University, Canada
Nan Jiang	East China Jiaotong University, China
Liangqun Li	Shenzhen University, China
Jungang Lou	Hunan Normal University, China
Hui Tian	Huaqiao University, China
Feng Wang	Wuhan University, China
Zhi Wang	Nankai University, China
Tao Xiang	Chongqing University, China

Publication Chairs

Hongyang Yan	Guangzhou University, China
Yu Wang	Guangzhou University, China

Publicity Chair

Lianyong Qi	Qufu Normal University, China

Steering Committee

Xiaofeng Chen	Xidian University, China
Iqbal Gondal	Federation University Australia, Australia
Ryan Ko	University of Waikato, New Zealand
Jonathan Oliver	Trend Micro, USA
Islam Rafiqul	Charles Sturt University, Australia
Vijay Varadharajan	The University of Newcastle, Australia
Ian Welch	Victoria University of Wellington, New Zealand
Yang Xiang	Swinburne University of Technology, Australia
Jun Zhang	Swinburne University of Technology, Australia
Wanlei Zhou	Deakin University, Australia

Program Committee

Silvio Barra	University of Salerno, Italy
M. Z. Alam Bhuiyan	Guangzhou University, China
Carlo Blundo	University of Salerno, Italy
Yiqiao Cai	Huaqiao University, China
Luigi Catuogno	University of Salerno, Italy
Lorenzo Cavallaro	King's College London, UK
Liang Chang	Guilin University of Electronic Technology, China
Fei Chen	Shenzhen University, China
Xiaofeng Chen	Xidian University, China
Zhe Chen	Singapore Management University, Singapore
Xiaochun Cheng	Middlesex University, UK
Frédéric Cuppens	Télécom Bretagne, France
Changyu Dong	Newcastle University, UK
Guangjie Dong	East China Jiaotong University, China
Mohammed EI-Abd	American University of Kuwait, Kuwait
Wei Gao	Yunnan Normal University, China
Dieter Gollmann	Hamburg University of Technology, Germany
Zheng Gong	South China Normal University, China
Zhitao Guan	North China Electric Power University, China
Zhaolu Guo	Chinese Academy of Sciences, China
Jinguang Han	Queen's University Belfast, UK
Saeid Hosseini	Singapore University of Technology and Design Singapore
Chingfang Hsu	Huazhong University of Science and Technology, China
Haibo Hu	The Hong Kong Polytechnic University, Hong Kong
Teng Huang	Guangzhou University, China
Xinyi Huang	Fujian Normal University, China
Wenchao Jiang	Guangdong University of Technology, China
Lutful Karim	Seneca College of Applied Arts and Technology, Canada

Hadis Karimipour	University of Guelph, Canada
Sokratis Katsikas	Open University of Cyprus, Cyprus
Neeraj Kumar	Thapar Institute of Engineering and Technology, India
Ping Li	South China Normal University, China
Tong Li	Guangzhou University, China
Wei Li	Jiangxi University of Science and Technology, China
Xuejun Li	Anhui University, China
Kaitai Liang	University of Surrey, UK
Hui Liu	University of Calgary, Canada
Wei Lu	Sun Yat-sen University, China
Xiaobo Ma	Xi'an Jiaotong University, China
Fabio Martinelli	IIT-CNR, Italy
Ficco Massimo	Second University of Naples, Italy
Weizhi Meng	Technical University of Denmark, Denmark
Vincenzo Moscato	University of Naples, Italy
Francesco Palmieri	University of Salerno, Italy
Fei Peng	Hunan University, China
Hu Peng	Wuhan University, China
Lizhi Peng	Jinan University, China
Umberto Petrillo	Sapienza University of Rome, Italy
Lianyong Qi	Qufu Normal University, China
Shahryar Rahnamayan	Ontario Tech University, Canada
Khaled Riad	Guangzhou University, China
Yu Sun	Guangxi University, China
Yu-An Tan	Beijing Institute of Technology, China
Zhiyuan Tan	Edinburgh Napier University, UK
Ming Tao	Dongguan University of Technology, China
Donghai Tian	Beijing Institute of Technology, China
Chundong Wang	Tianjin University of Technology, China
Ding Wang	Peking University, China
Hui Wang	Nanchang Institute of Technology, China
Jianfeng Wang	Xidian University, China
Jin Wang	Soochow University, China
Licheng Wang	Beijing University of Posts and Telecommunications, China
Lingyu Wang	Concordia University, Canada
Tianyin Wang	Luoyang Normal University, China
Wei Wang	Beijing Jiaotong University, China
Sheng Wen	Swinburne University of Technology, Australia
Yang Xiang	Swinburne University of Technology, Australia
Run Xie	Yibin University, China
Xiaolong Xu	Nanjing University of Information Science and Technology, China
Li Yang	Xidian University, China
ShaoJun Yang	Fujian Normal University, China
Zhe Yang	Northwestern Polytechnical University, China

Yanqing Yao	Beihang University, China
Xu Yuan	University of Louisiana at Lafayette, USA
Qikun Zhang	Beijing Institute of Technology, China
Xiao Zhang	Beihang University, China
Xiaosong Zhang	Tangshan University, China
Xuyun Zhang	Macquarie University, Australia
Yuan Zhang	Nanjing University, China
Xianfeng Zhao	Chinese Academy of Sciences, China
Lei Zhu	Huazhong University of Science and Technology, China
Tianqing Zhu	China University of Geosciences, China

Track Committee

Jin Cao	Xidian University, China
Hui Cui	Murdoch University, Australia
Rui Guo	Xi'an University of Posts and Telecommunications, China
Qi Li	Nanjing University of Posts and Telecommunications, China
Muhammad Baqer Mollah	Nanyang Technological University, Singapore
Ben Niu	Chinese Academy of Sciences, China
Fatemeh Rezaeibagha	Murdoch University, Australia

Contents – Part I

Dynamic Adjusting ABC-SVM Anomaly Detection Based on Weighted Function Code Correlation 1
Ming Wan, Jinfang Li, Hao Luo, Kai Wang, Yingjie Wang, and Bailing Wang

AndrOpGAN: An Opcode GAN for Android Malware Obfuscations 12
Xuetao Zhang, Jinshuang Wang, Meng Sun, and Yao Feng

An Anomalous Traffic Detection Approach for the Private Network Based on Self-learning Model 26
Weijie Han, Jingfeng Xue, Fuquan Zhang, and Yingfeng Zhang

A Malware Classification Method Based on the Capsule Network 35
Ziyu Wang, Weijie Han, Yue Lu, and Jingfeng Xue

A Novel Intrusion Detection System for Malware Based on Time-Series Meta-learning 50
Fangwei Wang, Shaojie Yang, Changguang Wang, and Qingru Li

DAD: Deep Anomaly Detection for Intelligent Monitoring of Expressway Network 65
Juan Wang, Meng Wang, Guanxiang Yin, and Yuejin Zhang

A Two-Phase Cycle Algorithm Based on Multi-objective Genetic Algorithm and Modified BP Neural Network for Effective Cyber Intrusion Detection 73
Yiguang Gong, Yunping Liu, Chuanyang Yin, and Zhiyong Fan

An Improved Localization Algorithm Based on Invasive Weed Optimization for WSNs 89
Yaming Zhang and Yan Liu

A Scientometric Analysis of Malware Detection Research Based on CiteSpace 100
Budong Xu, Yongqin Li, and Xiaomei Yu

Malware Detection Based on Static and Dynamic Features Analysis 111
Budong Xu, Yongqin Li, and Xiaomei Yu

Classification of Malware Variant Based on Ensemble Learning 125
Hui Guo, Shu-guang Huang, Min Zhang, Zu-lie Pan, Fan Shi, Cheng Huang, and Beibei Li

Detection of Malicious Domains in APT via Mining Massive DNS Logs 140
Lu Huang, Jingfeng Xue, Weijie Han, Zixiao Kong, and Zequn Niu

Spatio-Temporal Graph Convolutional Networks for DDoS Attack Detecting 153
Qian Xie, Zheng Huang, Jie Guo, and Weidong Qiu

Cerebral Microbleeds Detection Based on 3D Convolutional Neural Network 160
Meng Zhao, Chen Jin, Lingmin Jin, Shenghua Teng, and Zuoyong Li

Liver Tumor Segmentation of CT Image by Using Deep Fully Convolutional Network 170
Lingmin Jin, Rui Ma, Meng Zhao, Shenghua Teng, and Zuoyong Li

Machine Learning Based SDN-enabled Distributed Denial-of-Services Attacks Detection and Mitigation System for Internet of Things 180
Muhammad Aslam, Dengpan Ye, Muhammad Hanif, and Muhammad Asad

A New Lightweight CRNN Model for Keyword Spotting with Edge Computing Devices 195
Yungen Wei, Zheng Gong, Shunzhi Yang, Kai Ye, and Yamin Wen

Machine Learning Agricultural Application Based on the Secure Edge Computing Platform 206
Wu Fan, Zhuoqun Xu, Huanghe Liu, and Zhu Zongwei

QoS Investigation for Power Network with Distributed Control Services 221
Shen Jin, Xuesong Liang, and Hao Tian

Fog Server Placement for Multimodality Data Fusion in Neuroimaging 234
Xuan Yan, Xiaolong Xu, Yu Zheng, and Fei Dai

Event-Triggered Control for Distributed Optimal in Multi-agent Systems with External Disturbance 249
Yuanshan Liu, Hongyong Yang, Yize Yang, and Yuling Li

Towards Privacy-Preserving Aggregated Prediction from SPDZ 262
Qi Zhao, Bo Zhang, Anli Yan, Shan Jing, and Chuan Zhao

A Secure Neural Network Prediction Model with Multiple Data Providers . . . 272
Fengtian Kuang, Bo Mi, and Darong Huang

GAN-Based Image Privacy Preservation: Balancing Privacy and Utility 287
Zhenfei Chen, Tianqing Zhu, Chenguang Wang, Wei Ren, and Ping Xiong

A Novel Color Image Encryption Scheme Based on Controlled Alternate Quantum Walks and DNA Sequence Operations 297
Ting Yan and Dan Li

Cloud-Assisted Privacy Protection for Data Retrieval Against Keyword Guessing Attacks 307
Zhenwei Chen, Yinghui Zhang, Gang Han, Jiangyong He, Rui Guo, and Dong Zheng

Deep Learning Algorithms Design and Implementation Based on Differential Privacy. 317
Xuefeng Xu, Yanqing Yao, and Lei Cheng

Building Undetectable Covert Channels Over Mobile Networks with Machine Learning 331
Xiaosong Zhang, Ling Pang, Linhong Guo, and Yuanzhang Li

An Improved Privacy-Preserving Stochastic Gradient Descent Algorithm 340
Xianfu Cheng, Yanqing Yao, and Ao Liu

Recommender Systems with Condensed Local Differential Privacy 355
Ao Liu, Yanqing Yao, and Xianfu Cheng

Exploiting Bluetooth to Enquire Close Contacts Without Privacy Leakage . . . 366
Suhang Wang, Chen Wang, and Jian Xu

A Differentially Private Random Decision Tree Classifier with High Utility. 376
Datong Wu, Taotao Wu, and Xiaotong Wu

Research on Blind Signature Based Anonymous Electronic Cash Scheme . . . 386
Ying Wang, Haojia Zhu, and Fengyin Li

A Verifiable E-Lottery Scheme. 393
Yin Zhang, Fanglin An, Kejie Zhao, and Jun Ye

Re-Training and Parameter Sharing with the Hash Trick for Compressing Convolutional Neural Networks 402
Xu Gou, Linbo Qing, Yi Wang, and Mulin Xin

Survey on Privacy-Preserving Machine Learning Protocols. 417
Ruidi Yang

Efficient Privacy-Preserving Binary Tree Search 426
Ruidi Yang and Maohua Sun

Privacy-Preserving Classification of Personal Data with Fully Homomorphic Encryption: An Application to High-Quality Ionospheric Data Prediction 437
Zheng Li and Maohua Sun

An Improved Method for Data Storage Based on Blockchain Smart Contract 447
Dongxiang Song and Mingju Yuan

Security Problems and Countermeasures of Network Accounting Information System 461
Yanling Hu

Analysis on Industrial Internet Traffic Characteristics. 470
Shiyu Chen, Qianmu Li, Huaqiu Long, and Jian Jiang

User Personalized Location *k* Anonymity Privacy Protection Scheme with Controllable Service Quality 484
Ting Liu, Guanghui Yan, Gang Cai, Qiong Wang, and Mingjie Yang

Attack and Repair Strategies for Computer Network About Viruses. 500
Sheng Hong and Yue Wang

Vulnerability Variants and Matching in Networks 511
Meihui Lan and Wei Gao

A File-Level Continuous Data Protection Scheme for Enforcing Security Baseline 519
Xiangxiang Jiang, Yuxi Ma, Gang Zhao, Xiaohui Kuang, Yuanzhang Li, and Ruyun Zhang

A Novel Method of Network Security Situation Assessment Based on Evidential Network 530
Xiang Li, Xinyang Deng, and Wen Jiang

Research and Application of Digital Signature Technology. 540
Yanli Wang, Ying Zheng, and Fengyin Li

A Low Energy-Consuming Security Data Aggregation Protocol 547
Hui Dou, Yuling Chen, Yangyang Long, and Yuanchao Tu

Research on Blockchain-Based Identity Authentication Scheme in Social Networks 558
Xinying Yu, Rui Ge, and Fengyin Li

A Secure Multi-party Computational Adversary Selection Model Based on Time-Varying of Entropy 566
Xinyu Zhang, YuJun Liu, Yuling Chen, and Zhan Wang

An Efficient Public Batch Auditing Scheme for Data Integrity in Standard Model 578
Haining Yang, Ye Su, Jing Qin, Jinhua Ma, and Huaxiong Wang

A Block Chain Dynamic Key Sharing and Updating Scheme Based on the (t, n) Threshold 593
Wei Tang, Yu-Ling Chen, and Yun Yang

Attribute Propagation Enhanced Community Detection Model for Bitcoin De-anonymizing 607
Jiming Wang, Xueshuo Xie, Yaozheng Fang, Ye Lu, Tao Li, and Guiling Wang

A Secure and Moderate Data Synchronization Method Based on Network Isolation 623
Bing Zhang, Zhiyong Guo, Yangdan Ni, Meng Yang, Ruiying Cheng, and Yu Xiao

Secret Image Sharing Based on Chinese Remainder Theorem over a Polynomial Ring 634
Shuai Zhang and Fuyou Miao

Author Index 645

Contents – Part II

Vulnerability Variants and Path Factors in Networks 1
Linli Zhu, Haci Mehmet Baskonus, and Wei Gao

A Variant of Sun Toughness and the Existence of Path Factors in Networks 12
Linli Zhu, Haci Mehmet Baskonus, and Wei Gao

Network Adjacency Condition for Fractional (g, f, n', m)-Critical Covered Graphs 20
Yu Pan, Haci Mehmet Baskonus, and Wei Gao

An Effective Remote Data Disaster Recovery Plan for the Space TT&C System 31
Weijie Han, Jingfeng Xue, Fuquan Zhang, and Zhonghui Sun

Research on Progress and Inspiration of Entity Relation Extraction in English Open Domain 42
Xu Jian, Yao Xianming, Gan Jianhou, and Sun Yu

A SEU Immune Flip-Flop with Low Overhead 56
Zhengfeng Huang, Xiandong Li, Shangjie Pan, Min Wang, and Tianming Ni

An Information and Power Simultaneous Transfer Strategy in UAV and Wireless Rechargeable Sensor Networks 66
Zhi Li, Jifeng Feng, Jian Li, and Xu Gou

Research on Adaptive Beacon Transmitting Power Based on Vehicle Forecast Error 79
Meng Wang, Guanxiang Yin, Fei Du, Juan Wang, and Yuejin Zhang

Analysis of the Effective Scatters for Hyperloop Wireless Communications Using the Geometry-Based Model 87
Jiachi Zhang, Liu Liu, Kai Wang, Botao Han, Zheyan Piao, and Dong Wang

Finite-Time Consensus of Second-Order Multi-agent Systems with External Disturbances and Without Velocity Measurements 98
Yuling Li, Hongyong Yang, Yize Yang, and Yuanshan Liu

A Comparative Study on Key Technologies of Ultra-Reliable Low Latency Communication 112
Mingju Yuan, Dongxiang Song, and Bing Li

Research on the Construction of College Campus Sports Culture and the Participation of College Students in Sports Activities 125
Guan Li and Xin Xin Huang

Group Movement of Multi-agent Systems with Diverse Delays 137
Yize Yang, Hongyong Yang, Fei Liu, and Li Liu

Online Task Allocation in Mobile Crowdsensing with Sweep Coverage and Stability Control 147
Jiaang Duan, Shasha Yang, Jianfeng Lu, Wenchao Jiang, Haibo Liu, and Shuo Zhang

Max-Min Fairness Multi-task Allocation in Mobile Crowdsensing 164
Shasha Yang, Wenchao Jiang, Jiaang Duan, Zhengjie Huang, and Jianfeng Lu

Research on High Reliable Wireless Channel Data Cleaning Method 180
Lingfan Zhuang, Liu Liu, Shuoshuo Dong, Yuanyuan Fan, and Jiachi Zhang

A New Health Assessment Approach of Lithium-Ion Batteries Under Variable Operation Conditions 190
Sheng Hong and Yining Zeng

Health Evaluation of Lithium Ion Battery Based on Weighted Kalman Filter Algorithm 201
Sheng Hong and Tianyu Yue

Location Planning of UAVs for WSNs Data Collection Based on Adaptive Search Algorithm 214
Xueqiang Li and Ming Tao

Covid-19 Public Opinion Analysis Based on LDA Topic Modeling and Data Visualization 224
Li Chen, Xin Huang, Hao Zhang, and Ben Niu

A Capacitated Vehicle Routing Problem with Order Release Time Based on a Hybrid Harmony Search 235
Ling Liu, Sen Liu, Ben Niu, and Hui Tan

An Adaptive Data Protection Scheme for Optimizing Storage Space 250
Meng Ming, Gang Zhao, Xiaohui Kuang, Lu Liu, and Ruyun Zhang

The Thinned Rectangular Array Based on Modified Interger Genetic Algorithm 261
Qingling Liu, Ding Yuan, and Shubin Wang

A Novel Method to Classify Videos Based VBR Trace 270
Xiaojie Yu, Min Qiu, and Lizhi Peng

Research on Friendvertising-Counter Technology in Big Data. 283
Pei Ren, Hui Liu, and Fengyin Li

A Survey of Researches on Personalized Bundle Recommendation Techniques 290
Miao Li, Xuguang Bao, Liang Chang, Zhoubo Xu, and Long Li

Estimation of Motor Imagination Based on Consumer-Grade EEG Device . . . 305
Zhenzhen Luo, Zhongyi Hu, and Zuoyong Li

An Overview of Key Technologies and Challenges of 6G 315
Qingling Liu, Shahid Sarfraz, and Shubin Wang

Q-Learning-Based Adaptive Bacterial Foraging Optimization 327
Ben Niu and Bowen Xue

Counterfactual Retrieval for Augmentation and Decisions 338
Nwaike Kelechi and Shuang Geng

Firefly Algorithm Based on Dynamic Step Change Strategy 347
Jing Wang, Fuqi Song, Aihua Yin, and Hui Chen

Earthquakes Detection Scheme by Dynamic Time Warping on Smartphones. 356
Yuqin Zhu, Jiaxin Yang, Bingjie Shao, Liang Wang, and Zhaohui Yuan

Towards Accurate Seismic Events Detection Using Motion Sensors on Smartphones 370
Qingping Cao, Yuqin Zhu, Mei He, and Zhaohui Yuan

A SEIR Model Optimization Using the Differential Evolution 384
Dejiang Wang, Yafeng Sun, Ji Song, and Ying Huang

Multi-term Multi-task Allocation for Mobile Crowdsensing with Weighted Max-Min Fairness. 393
Haibo Liu, Wenchao Jiang, Shasha Yang, Jianfeng Lu, and Dongjun Ning

An Improved Sensor Pattern Noise Estimation Method Based on Edge Guided Weighted Averaging. 405
Wen-Na Zhang, Yun-Xia Liu, Jin Zhou, Yang Yang, and Ngai-Fong Law

Analysis of the Influence of Stylized-CIFAR10 Dataset on ResNet 416
Dexin Wu, Jian Xu, and Heng Liu

A Multi-objective Ant Colony Optimization Algorithm with Local Optimum Avoidance Strategy 427
Ying Wu, Zibo Qi, Ling Jiang, Changsheng Zhang, and Jian Xu

Education for Bilingual Children in the Age of Artificial Intelligence 436
Weiwei Zhou

Application of Fuzzy Comprehensive Evaluation in Environmental Adaptability of Poultry House. 443
Fenghang Zhang, Linze Li, Yuxuan Jiang, Zhunan Zhou, and Xiuli Wang

Performance Evaluation of Multirotor UAV by Considering the Balanced Pattern 452
Min Lv, Cong Lin, Tianran Ma, and Sheng Hong

AdvJND: Generating Adversarial Examples with Just Noticeable Difference 463
Zifei Zhang, Kai Qiao, Lingyun Jiang, Linyuan Wang, Jian Chen, and Bin Yan

Squeeze Criterion GANs: Double Adversarial Learning Method 479
Yan Gan, Tao Xiang, and Mao Ye

A Feature-Based Detection System of Adversarial Sample Attack 494
Fangwei Wang, Yuanyuan Lu, Qingru Li, and Changguang Wang

GF-Attack: A Strategy to Improve the Performance of Adversarial Example 501
Jintao Zhang, Zhenghao Liu, Liren Wu, Liwen Wu, and Qing DuanJunhui Liu

War: An Efficient Pre-processing Method for Defending Adversarial Attacks 514
Zhaoxia Yin, Hua Wang, and Jie Wang

A High-Recall Membership Inference Attack Based on Confidence-Thresholding Method with Relaxed Assumption 525
Lulu Wang, Xiaoyu Zhang, Yi Xie, Xu Ma, and Meixia Miao

Smart Watchdog: A Lightweight Defending Mechanism Against Adversarial Transfer Learning. 540
Yong Ding, Wenyao Liu, Yi Qin, and Yujue Wang

A Poisoning Attack Against the Recognition Model Trained by the Data Augmentation Method 550
Yunhao Yang, Long Li, Liang Chang, and Tianlong Gu

Adversarial Text Generation via Probability Determined Word Saliency. 562
Gang Ma, Lingyun Shi, and Zhitao Guan

Adversarial Example Attacks in the Physical World 572
Huali Ren and Teng Huang

Querying Little Is Enough: Model Inversion Attack
via Latent Information 583
Kanghua Mo, Teng Huang, and Xiaoyu Xiang

Efficient Defense Against Adversarial Attacks and Security Evaluation
of Deep Learning System. 592
Na Pang, Sheng Hong, Yang Pan, and Yuqi Ji

Author Index 603

Contents – Part III

Deep Convolutional Neural Network Based Image Segmentation for Salt Mine Recognition 1
Ming Tao, Xueqiang Li, and Kai Ding

Optimization of Collaborative Filtering Algorithm in Movie Recommendation System 11
Jiao Peng and Shu Gong

TagRec: Trust-Aware Generative Adversarial Network with Recurrent Neural Network for Recommender Systems 20
Honglong Chen, Shuai Wang, Nan Jiang, Zhe Li, Na Yan, and Leyi Shi

Software Entity Recognition Method Based on BERT Embedding 33
Chao Sun, Mingjing Tang, Li Liang, and Wei Zou

A Classification Method of Land Cover Based on Support Vector Machines 48
Kai Ding, Chisheng Wang, Ming Tao, Huijuan Xiao, Chao Yang, and Peican Huang

Temporal Consistency Based Deep Face Forgery Detection Network 55
Chunlei Peng, Wenbo Zhang, Decheng Liu, Nannan Wang, and Xinbo Gao

CBOW and LSTM Based User Mobile Trajectory Prediction 64
Geng Sun and Ming Tao

Framework Optimization for Face Recognition 74
Chao Chen, Xin Wang, and Yong-Xin He

Machine Learning Assisted OSP Approach for Improved QoS Performance on 3D Charge-Trap Based SSDs 86
Zongwei Zhu, Chao Wu, Cheng Ji, and Xianmin Wang

A Location Method for Reliability-Critical Paths Based on Monte Carlo Search Tree 100
Ziwen Sun, Qiou Ji, Zecheng Wu, and Aizhu Liu

Research of Expressway Vehicle Detection Based on Faster R-CNN and Domain Adaptation 115
Meng Yu, Yong Hu, Guanxiang Yin, Fei Du, Meng Wang, and Yuejin Zhang

A Short-Term Traffic Flow Forecasting Method Based on Support Vector Regression Optimized by Genetic Algorithm 125
Aiyun Zhan, Fei Du, Guanxiang Yin, Meng Wang, and Yuejin Zhang

Short-Term Traffic Flow Prediction Based on Hybrid Model 135
Yong Hu, Meng Yu, Guanxiang Yin, Fei Du, Meng Wang, and Yuejin Zhang

Uneven Clustering Routing Protocol for Geological Disaster Monitoring Sensor Network 144
Yicheng Wei, Xun Wang, Xu Gou, Zhaoma Pan, and Zhi Li

Clustering Analysis Method of Ethnic Cultural Resources Based on Deep Neural Network Model 160
Mingjing Tang, Chao Sun, and Li Liang

Optimal Group Consensus of Second-Order Multi-agent Systems 171
Yize Yang, Hongyong Yang, Yuling Li, and Yuanshan Liu

A Novel Game Machine Learning Method for Calculating Optimal Response for Edge Server 183
Rui Zhang, Hui Xia, Ju-fu Cui, Yi-zhe Li, Shu-shu Shao, and Hang Ren

SDUW-Net: An Effective Retinal Vessel Segmentation Model 193
Hongkai Lin, Hongliang Kang, and Xinrong Cao

A New Mobility Model Based on Markov Chain for MANETs 203
Tieyuan Liu, Tianlong Gu, Liang Chang, and Hongzhuan Zhao

Image Dust Storm Synthetic Method Based on Optical Model 215
Jiayan Huang, Zuoyong Li, and Chuansheng Wang

Research on Classification Model of Government Big Data Based on Deep Learning 227
Qiong Yuan, Duqiang Mai, Ying Sun, and Peiyu Liang

Research of Paper Recommendation System Based on Citation Network Model. 237
Sun Jing and Sun Yu

CellIdNet: Automatic Cell Instance Segmentation and Classification in Bone Marrow Examination with Double Backbone Networks 248
Shiyin He, Zheng Huang, Kai Chen, Jie Guo, and Weidong Qiu

Mathematical Subject Information Entity Recognition Method Based on BiLSTM-CRF 259
Haoze Li, Tianwei Xu, and Juxiang Zhou

A Facial Fatigue Expression Recognition Method Based on Sparse Representation on the Low-Resolution Image 269
Ling Zhang, Xiao-lu Tian, Wenchao Jiang, and Dongjun Ning

Spontaneous Expression Recognition Based on Visual Attention Mechanism and Co-salient Features 279
Ling Zhang, Qiumin Ji, Wenchao Jiang, and Dongjun Ning

Single Image Super-Resolution Reconstruction Using Nonlocal Low-Rank Prior 290
Zhongxing Zhang, Hui Liu, Qiang Guo, and Yuxiu Lin

Product Consistency Joint Detection Algorithm Based on Deep Learning 297
Bo Liu, Jianhou Gan, Jun Wang, and Bin Wen

Research on Image Recognition Method of Ethnic Costume Based on VGG. 312
Qinchuan Lei, Bin Wen, Zhaoxiang Ouyang, Jianhou Gan, and Kangwei Wei

National Defense Education Resource Recommender of High Education Institutions Based on Knowledge-Aware Generative Adversarial Network . . . 326
Lin Tang and Lin Liu

Dictionary Learning Based on Structural Self-similarity and Convolution Neural Network 336
Ling Zhang, Wenchao Jiang, and Wen Xiang

Short-Text Feature Expansion and Classification Based on Non-negative Matrix Factorization 347
Ling Zhang, Wenchao Jiang, and Zhiming Zhao

Cross-Project Software Defect Prediction Based on Feature Selection and Transfer Learning 363
Tianwei Lei, Jingfeng Xue, and Weijie Han

A Swarm Enhanced Light Gradient Boosting Machine for Crowdfunding Project Outcome Prediction 372
Shuang Geng, Miaojia Huang, and Zhibo Wang

Satellite Signal Blind Detection Method Based on Time-Frequency Diagrams Semantic Segmentation 383
Zheyu Dong, Hao Luo, Zhigang Wu, and Shuzhang Zhang

A Hybrid Distributed Frequent Itemset Mining Method with Its Application in Medical Diagnosis. 394
Mingxue Zhang and Fuyuan Xiao

A DNS Server Classification Method Based on Long-Term Behavior Features 404
Rui Wang, Hao Luo, Zhigang Wu, and Shuzhang Zhang

Medical Image Segmentation Algorithm Based on Information Combined Level Set 413
Lin Ye, Liu Qingling, and Muhammad Ayoob Dars

A Novel Two Dimensional Pythagorean Fuzzy Sets Model with Its Application in Multi-attribute Decision Making. 419
Yi Fan and Fuyuan Xiao

Utilization of CNN-LSTM Model in Prediction of Multivariate Time Series for UCG 429
Yuteng Xiao, Hongsheng Yin, Kaijian Xia, Yundong Zhang, and Honggang Qi

An Imbalanced Learning Based Method for Esophageal Squamous Cell Carcinoma (ESCC) Distant Metastasis Predicting 441
Xuemei Li, Bo Yang, Lizhi Peng, Baosheng Li, and Jian Zhu

A Deep Learning Approach to Radar Extrapolation 454
Lei Yi, Wei Tian, Xiang Wang, and Xiaolong Xu

Peripheral Blood Leukocyte Image Segmentation Based on Deep Convolutional Neural Network 464
Yuanyuan Chen, Shenghua Teng, and Zuoyong Li

Machine Learning Based Tongue Image Recognition for Diabetes Diagnosis. 474
Xiaohui Lin, Zhaochai Yu, Zuoyong Li, and Weina Liu

Remote Sensing Image Fusion Based on Multi-morphological Convolutional Neural Network 485
Meng Zhu, Jindong Xu, and Zhaowei Liu

From Sentiment to Well-Being: Internet Users in an Uncertain and Risky Environment 496
Ge Zhan, Shuang Geng, and Ruowen Wang

Channel Parameters Extraction Based on Back Propagation Neural Network 503
Huiting Li, Liu Liu, Jiachi Zhang, Kai Wang, Yiqian Li, Tao Zhou, and Jiahui Qiu

Automatic Vibration Waveform Recognition Using Convolutional Neural Network 516
Wei Ding, Heng Liu, Dijing Wang, and Yong Jiang

A Prediction Method for Soil Moisture Time Series 526
XiaoXia Yang, Song Jia, and Chengming Zhang

Research on Automatic Target Detection and Recognition System Based on Deep Learning Algorithm 538
Qinghui Zhang, Hongbin Xu, Zhengyu Li, Xiaobin Liu, Yuxi Li, and Yingjie Jiao

Author Index 549