

**2021 51st Annual IEEE/IFIP  
International Conference on  
Dependable Systems and  
Networks Workshops  
(DSN-W 2021)**

**Virtual Conference  
21 – 24 June 2021**



**IEEE Catalog Number: CFP2141K-POD  
ISBN: 978-1-6654-3951-0**

**Copyright © 2021 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

|                         |                   |
|-------------------------|-------------------|
| IEEE Catalog Number:    | CFP2141K-POD      |
| ISBN (Print-On-Demand): | 978-1-6654-3951-0 |
| ISBN (Online):          | 978-1-6654-3950-3 |
| ISSN:                   | 2325-6648         |

**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  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN- W)

## DSN-W 2021

### Table of Contents

|                                       |       |
|---------------------------------------|-------|
| Message from the Workshop Chairs      | ix    |
| Message from the DCDS 2021 Organizers | xii   |
| Message from the SSIV 2021 Organizers | xiii  |
| Message from the AITS 2021 Organizers | xiv   |
| Message from the DSML 2021 Organizers | xvi   |
| Message from the SAS 2021 Organizers  | xvii  |
| Sponsors                              | xviii |

### Workshop on Data-Centric Dependability and Security (DCDS)

|  |    |
|--|----|
| USB-IDS-1: A Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation   | 1  |
| <i>Marta Catillo (Università degli Studi del Sannio, Italy), Andrea Del Vecchio (Università degli Studi del Sannio, Italy), Luciano Ocone (Università degli Studi del Sannio, Italy), Antonio Pecchia (Università degli Studi del Sannio, Italy), and Umberto Villano (Università degli Studi del Sannio, Italy)</i> |    |
| SMS Goes Nuclear: Fortifying SMS-Based MFA in Online Account Ecosystem   | 7  |
| <i>Weizhao Jin (Zhejiang University, China), Xiaoyu Ji (Zhejiang University, China), Ruiwen He (Zhejiang University, China), Zhou Zhuang (Zhejiang University, China), Wenyuan Xu (Zhejiang University, China), and Yuan Tian (University of Virginia, USA)</i>  |    |
| Statistical Approach For Cloud Security: Microsoft Office 365 Audit Logs Case Study  | 15 |
| <i>Louis-Simon Létourneau (Université de Sherbrooke, Canada), Chaymae El Jabri (Université de Sherbrooke, Canada), Marc Frappier (Université de Sherbrooke, Canada), Pierre-Martin Tardif (Université de Sherbrooke, Canada), Guy Lépine (Sherweb, Canada), and Guillaume Boisvert (Sherweb, Canada)</i>             |    |

## Workshop on Safety and Security in Intelligent Vehicles (SSIV)

|   |  |
|---|--|
| Vehicular Platoon Communication: Cybersecurity Threats and Open Challenges .19.....   |  |
| <i>Sean Joe Taylor (Coventry University, UK), Farhan Ahmad (Coventry University, UK), Hoang Nga Nguyen (Coventry University, UK), Siraj Ahmed Shaikh (Coventry University, UK), David Evans (IDIADA Automotive Technology UK, UK), and David Price (IDIADA Automotive Technology UK, UK)</i>                                  |  |
| SaSeVAL: A Safety/Security-Aware Approach for Validation of Safety-Critical Systems .27.....  |  |
| <i>Christian Wolschke (Fraunhofer IESE, Germany), Behrooz Sangchoolie (RISE Research Institutes of Sweden, Sweden), Jacob Simon (CEVT, China Euro Vehicle Technology, Sweden), Stefan Marksteiner (AVL List GmbH, Austria), Tobias Braun (Fraunhofer IESE, Germany), and Hayk Hamazaryan (ZF Friedrichshafen AG, Germany)</i> |  |
| Suraksha: A Quantitative AV Safety Evaluation Framework to Analyze Safety Implications of Perception Design Choices .35.....  |  |
| <i>Hengyu Zhao (University of California, San Diego), Siva Kumar Sastry Hari (NVIDIA), Timothy Tsai (NVIDIA), Michael B. Sullivan (NVIDIA), Stephen W. Keckler (NVIDIA), and Jishen Zhao (University of California, San Diego)</i>  |  |
| Evaluation of a Fail-Over Mechanism for 1oo2D Architectures in Highly-Automated Driving .39.....  |  |
| <i>Rupert Schorn (TTTech Auto AG, Austria) and Wilfried Steiner (TTTech Computertechnik AG, Austria)</i>  |  |
| Safety Verification of Neural Network Controlled Systems .47.....   |  |
| <i>Arthur Clavière (Collins Aerospace, France), Eric Asselin (Collins Aerospace, France), Christophe Garion (ISAE-SUPAERO, France), and Claire Pagetti (ONERA, France)</i>  |  |
| Certifying Emergency Landing for Safe Urban UAV .55.....  |  |
| <i>Joris Guerin (Université Toulouse, France), Kevin Delmas (ONERA, France), and Jérémie Guiochet (Université of Toulouse, France)</i>  |  |
| CyberGSN: A Semi-Formal Language for Specifying Safety Cases .63.....   |  |
| <i>Tewodros A. Beyene (fortiss - Research Institute of the Free State of Bavaria, Germany) and Carmen Carlan (fortiss - Research Institute of the Free State of Bavaria, Germany)</i>   |  |
| A Safety Architecture for Centralized E/E Architectures .67.....  |  |
| <i>Victor Bandur (McMaster University, Canada), Vera Pantelic (McMaster University, Canada), Timofey Tomashevskiy (McMaster University, Canada), and Mark Lawford (McMaster University, Canada)</i>   |  |

## Workshop on Application of Intelligent Technology in Security (AITS)

|  |  |
|--|--|
| Ant Hole: Data Poisoning Attack Breaking out the Boundary of Face Cluster .71.....   |  |
| <i>Zhiqiu Huang (University of Chinese Academy of Sciences, China), Yuqing Zhang (University of Chinese Academy of Sciences, China; Hainan University, China; Yanshan University, China), Wenjie Wang (University of Chinese Academy of Sciences, China), and Haitao He (University of Chinese Academy of Sciences, China)</i> |  |

|   |   |
|---|---|
| Authenticating Mobile Wireless Device Through Per-Packet Channel State Information .78.....                           |   |
|   | <i>Bing Chen (Southeast University; Key Laboratory of Computer Network Technology of Jiangsu Province; Purple Mountain Laboratories), Yubo Song (Southeast University; Key Laboratory of Computer Network Technology of Jiangsu Province; Purple Mountain Laboratories), Zhenchao Zhu (Southeast University; Key Laboratory of Computer Network Technology of Jiangsu Province; Purple Mountain Laboratories), Shang Gao (The Hong Kong Polytechnic University), Junbo Wang (Southeast University; Purple Mountain Laboratories), and Aiqun Hu (Southeast University; Purple Mountain Laboratories)</i> |
| Whether the Sensitive Information Statement of the IoT Privacy Policy is Consistent with the Actual Behavior .85..... |   |
|   | <i>Xiao Yu (Xidian University, China; University of Chinese Academy of Sciences, China), Yiyu Yang (University of Chinese Academy of Sciences, China), Wenjie Wang (University of Chinese Academy of Sciences, China), and Yuqing Zhang (University of Chinese Academy of Sciences, China)</i>  |
| BBregLocator: A Vulnerability Detection System Based on Bounding Box Regression .93.....                              |   |
|   | <i>Junfeng Tian (Hebei University, China), Junkun Zhang (Hebei University, China), and Fanming Liu (Hebei University, China)</i>  |
| Insight into Traffic Security: A Correlation Discovery of Urban Spatial Features and Traffic flow Patterns .101.....  |   |
|   | <i>Juhua Pu (Beihang University, China), Zhuang Liu (Beihang University, China), Yue Wang (Beihang University, China), and Xingwu Liu (University of Chinese Academy of Sciences, Dalian University of Technology)</i>  |
| Automatically Constructing Peer Slices via Semantic- and Context-Aware Security Checks in the Linux Kernel .108.....  |   |
|   | <i>Yongzhi Liu (Peking University, China), Xiarun Chen (Peking University, China), Zhou Yang (Peking University, China), and Weiping Wen (Peking University, China)</i>   |
| Detection Algorithm of the Mimicry Attack Based on Variational Auto-Encoder .114.....                                 |   |
|   | <i>Qunke Wang (Southeast University, China), Lanting Fang (Southeast University, China; Purple Mountain Laboratory, China), Zhenchao Zhu (Southeast University, China; Purple Mountain Laboratory, China; Jiangsu Provincial Key Laboratory of Network and Information Security, China), and Jie Huang (Southeast University, China; Purple Mountain Laboratory, China)</i>   |
| Sensitive Instruction Detection Based on the Context of IoT Sensors .121.....   |   |
|   | <i>Yucheng Wang (Xidian University, China; University of Chinese Academy of Sciences, China), Xuejun Li (Xidian University, China), Peiyang Jia (Xidian University, China; University of Chinese Academy of Sciences, China), Yiyu Yang (University of Chinese Academy of Sciences, China), and He Wang (Xidian University, China)</i>  |

Network Intrusion Detection Based on Active Semi-Supervised Learning .129.....  
Yong Zhang (Beijing University of Posts and Telecommunication), Jie  
Niu (Beijing University of Posts and Telecommunication), Guojian He  
(Physical Hebei University of Economics and Business), Lin Zhu (China  
Mobile Research Institute, Beijing), and Da Guo (Beijing University of  
Posts and Telecommunication)

A Statistical Learning Model with Deep Learning Characteristics .137.....  
Lei Liao (University of Chinese Academy of Sciences, China), Zhiqiu  
Huang (University of Chinese Academy of Sciences, China), and Wenjie  
Wang (University of Chinese Academy of Sciences, China)

## **Workshop on Dependable and Secure Machine Learning (DSML)**

A Queueing Analysis of Multi-model Multi-input Machine Learning Systems .141.....  
Yuta Makino (University of Tsukuba, Japan), Tuan Phung-Duc (University  
of Tsukuba, Japan), and Fumio Machida (University of Tsukuba, Japan)

An Approach for Peer-to-Peer Federated Learning .150.....  
Tobias Wink (Karlsruhe University of Applied Sciences, Germany) and  
Zoltan Nocht (Karlsruhe University of Applied Sciences, Germany)

Poisoning Attacks via Generative Adversarial Text to Image Synthesis .158.....  
Keshav Kasichainula (University of Houston, USA), Hadi Mansourifar  
(University of Houston, USA), and Weidong Shi (University of Houston,  
USA)

Fault-Tolerant Low-Precision DNNs using Explainable AI .166.....  
Muhammad Sabih (Friedrich-Alexander University Erlangen-Nürnberg  
(FAU), Germany), Frank Hannig (Friedrich-Alexander University  
Erlangen-Nürnberg (FAU), Germany), and Jürgen Teich  
(Friedrich-Alexander University Erlangen-Nürnberg (FAU), Germany)

Byzantine Fault-Tolerant Distributed Machine Learning with Norm-Based Comparative Gradient  
Elimination .175.....  
Nirupam Gupta (EPFL, Switzerland), Shuo Liu (Georgetown University,  
USA), and Nitin Vaidya (Georgetown University, USA)

RADICS: Runtime Assurance of Distributed Intelligent Control Systems .182.....  
Brian Wheatman (Johns Hopkins University, USA), Jerry Chen (Johns  
Hopkins University, USA), Tamim Sookoor (Johns Hopkins Applied Physics  
Lab), and Yair Amir (Johns Hopkins University, USA)

Detecting Deep Neural Network Defects with Data Flow Analysis .188.....  
Jiazhen Gu (Fudan University, China), Huanlin Xu (Fudan University,  
China), Haochuan Lu (Fudan University, China), Yangfan Zhou (Fudan  
University, China), and Xin Wang (Fudan University, China)

**Author Index 197** .....