

PROCEEDINGS OF SPIE

Fourth International Conference on Network Communication and Information Security (ICNCIS 2024)

**Ljiljana Trajkovic
Pascal Lorenz**
Editors

**23–25 August 2024
Hangzhou, China**

*Organized by
Zhejiang University of Science and Technology (China)*

*Sponsored by
AEIC Academic Exchange Information Centre (China)*

*Published by
SPIE*

Volume 13516

Proceedings of SPIE 0277-786X, V. 13516

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

The papers in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. Additional papers and presentation recordings may be available online in the SPIE Digital Library at SPIDigitalLibrary.org.

The papers reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from these proceedings:

Author(s), "Title of Paper," in *International Conference on Network Communication and Information Security (ICNCIS 2024)*, edited by Ljiljana Trajkovic, Pascal Lorenz, Proc. of SPIE 13516, Seven-digit Article CID Number (DD/MM/YYYY); (DOI URL).

ISSN: 0277-786X

ISSN: 1996-756X (electronic)

ISBN: 9781510688254

ISBN: 9781510688261 (electronic)

Published by

SPIE

P.O. Box 10, Bellingham, Washington 98227-0010 USA

Telephone +1 360 676 3290 (Pacific Time)

SPIE.org

Copyright © 2025 Society of Photo-Optical Instrumentation Engineers (SPIE).

Copying of material in this book for internal or personal use, or for the internal or personal use of specific clients, beyond the fair use provisions granted by the U.S. Copyright Law is authorized by SPIE subject to payment of fees. To obtain permission to use and share articles in this volume, visit Copyright Clearance Center at copyright.com. Other copying for republication, resale, advertising or promotion, or any form of systematic or multiple reproduction of any material in this book is prohibited except with permission in writing from the publisher.

Printed in the United States of America by Curran Associates, Inc., under license from SPIE.

Publication of record for individual papers is online in the SPIE Digital Library.

**SPIE. DIGITAL
LIBRARY**

SPIDigitalLibrary.org

Paper Numbering: A unique citation identifier (CID) number is assigned to each article in the Proceedings of SPIE at the time of publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online and print versions of the publication. SPIE uses a seven-digit CID article numbering system structured as follows:

- The first five digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B ... 0Z, followed by 10-1Z, 20-2Z, etc. The CID Number appears on each page of the manuscript.

Contents

vii *Conference Committee*

NETWORK COMMUNICATION AND INTELLIGENT PROCESSING TECHNOLOGY

- 13516 02 **Comparative study of link bandwidth scheduling algorithms suitable for UV optical communication networks** [13516-5]
- 13516 03 **Attack detection and positioning algorithm based on improved decision tree support vector machine** [13516-33]
- 13516 04 **A method of service content prefetching based on node portrait** [13516-24]
- 13516 05 **Research on security for multidomain communication in space-air-ground integrated network** [13516-8]
- 13516 06 **Joint detection algorithm based on electromagnetic leakage signal and knock frequency** [13516-29]
- 13516 07 **Development and implementation of a power wireless private network communication terminal based on domestic microcontroller** [13516-42]
- 13516 08 **Hybrid genetic algorithm with rank sorting for obtaining bijective S-boxes with good cryptographic properties** [13516-20]
- 13516 09 **IEEE1588 clock synchronization accuracy analysis** [13516-32]
- 13516 0A **Differential evolution-based resource allocation for D2D communications in cellular networks with system capacity and fairness tradeoff** [13516-47]
- 13516 0B **Research on technology of multipath cross-band regenerative frequency coherent retransmission** [13516-9]
- 13516 0C **Efficient cloud-assisted revocable identity-based broadcast encryption in IoT** [13516-52]
- 13516 0D **Research on operations of electronic countermeasures against drone swarm** [13516-53]
- 13516 0E **IAAD: integrated anti-anti-drone mechanics with cryptography utilized in power grid inspection** [13516-25]
- 13516 0F **Artificial noise-assisted frequency array for covert communication** [13516-12]
- 13516 0G **Construction technology of 5G special test network for flight test** [13516-45]

- 13516 OH **Research on target detection algorithm based on fusion of LiDAR and camera** [13516-38]
- 13516 OI **A bit-level color image encryption algorithm based on PWLCM chaotic maps** [13516-16]
- 13516 OJ **Auxiliary decision system for power grid asset operation based on microservice architecture and container technology** [13516-41]
- 13516 OK **Enhancing trusted computing operation efficiency based on parallel file verification techniques** [13516-43]
- 13516 OL **A distributed machine learning dynamic remote proof scheme that resists collusion attacks** [13516-7]
- 13516 OM **Cloud workload prediction by the DE-based nonstationary transformer model** [13516-31]
- 13516 ON **An improved asymptotic denoising algorithm for infrared images of electrical equipment based on nonlocal means** [13516-3]
- 13516 OO **Supermarket decision-making model based on improved genetic algorithm and XGBoost** [13516-34]
- 13516 OP **Method for determining the importance of customer requirements based on preference consensus and trust relations** [13516-26]

NETWORK INFORMATION SECURITY AND RISK MONITORING

- 13516 OQ **A subway signal data encryption scheme based on blockchain** [13516-21]
- 13516 OR **Research on risk identification of malicious threats to large-scale industrial control network equipment assets** [13516-36]
- 13516 OS **Research on feature classification of network intrusion detection based on deep learning** [13516-49]
- 13516 OT **Mining and research on security vulnerabilities of HTML functions in websites** [13516-46]
- 13516 OU **On the security of NDN's privacy access control framework** [13516-2]
- 13516 OV **A digital certificate-based authentication system for multilevel security environment** [13516-27]
- 13516 OW **Real-time monitoring technology of flight test risks throughout the entire process based on a layered safety model** [13516-13]
- 13516 OX **Prediction of instruction SDC vulnerability in routing algorithms based on graph convolutional network** [13516-40]

- 13516 0Y **Design of campus security management and control based on ZigBee** [13516-48]
- 13516 0Z **Detecting advanced persistent threats via casual graph neural network** [13516-28]
- 13516 10 **On the security risk analysis method of open source software supply chain** [13516-51]
- 13516 11 **Federated learning-based intrusion detection system for industrial Internet of Things: enhancing security and efficiency** [13516-50]
- 13516 12 **Comprehensive approach to identifying and mitigating DoS vulnerabilities in PHP: from CVE analysis to model-based automated detection** [13516-35]
- 13516 13 **Quantum secret sharing scheme with single quantum state** [13516-44]
- 13516 14 **Design and implementation of network security defense system based on deep learning** [13516-39]
- 13516 15 **Network security situational awareness analysis based on machine learning** [13516-37]
- 13516 16 **Federated learning under differential privacy with effective clipping and analytic Gaussian mechanism** [13516-4]
- 13516 17 **Group authentication algorithm based on region grouping and aggregate signcryption** [13516-17]
- 13516 18 **Research on dynamic network security detection technology based on SDN** [13516-18]
- 13516 19 **Hybrid neural networks for network security situation prediction: the CNN-LSTM-MuIAHNet model** [13516-1]
- 13516 1A **Service similarity-based k-anonymity location privacy preserving method for Internet of Vehicles** [13516-19]
- 13516 1B **Blockchain-based secure crowdsourcing scheme to support solution reuse** [13516-6]
- 13516 1C **An efficient formal verification method for concurrent programs** [13516-14]