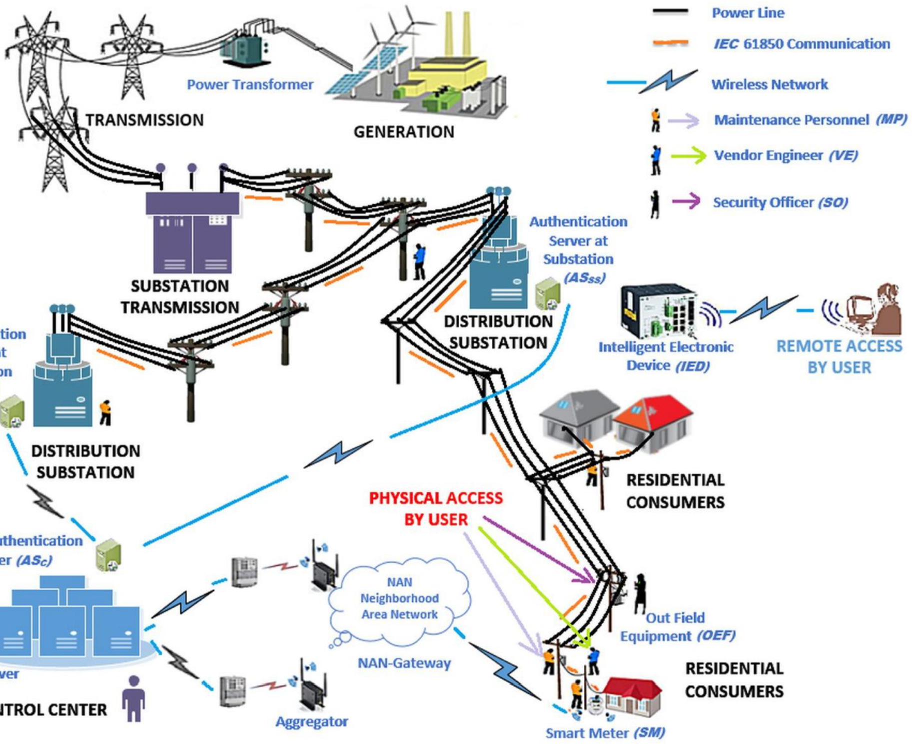
IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

A PUBLICATION OF THE IEEE SIGNAL PROCESSING SOCIETY

IEEE Signal Processing Society

www.signalprocessingsociety.org

MAY 2016 VOLUME 11 NUMBER 5 ITIFA6 (ISSN 1556-6013)
JUNE 2016 VOLUME 11 NUMBER 6



Smart grid system model consisting of various devices and users connected by communication networks, as seen in "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid" by N. Saxena *et al.*, p. 907.

For the May 2016 issue, see p. 873 for Table of Contents.
For the June 2016 issue, see p. 1089 for Table of Contents.

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

A PUBLICATION OF THE IEEE SIGNAL PROCESSING SOCIETY

www.signalprocessingsociety.org

JUNE 2016 VOLUME 11 NUMBER 6 ITIFA6 (ISSN 1556-6013)

PAPERS

Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem .... *C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt* 1093

Remanence Decay Side-Channel: The PUF Case .... *S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A.-R. Sadeghi* 1106

Generating Correlated Digital Certificates: Framework and Applications .... *W.-T. Zhu and J. Lin* 1117

Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach .... *Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik* 1128

Simultaneously Generating Secret and Private Keys in a Cooperative Pairwise-Independent Network .... *P. Xu, Z. Ding, X. Dai, and G. K. Karagiannidis* 1139

Against Double Fault Attacks: Injection Effort Model, Space and Time Randomization Based Countermeasures for Reconfigurable Array Architecture .... *B. Wang, L. Liu, C. Deng, M. Zhu, S. Yin, and S. Wei* 1151

Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud .... *H. Wang, D. He, and S. Tang* 1165

Creating Secrets Out of Packet Erasures .... *I. Safaka, L. Czap, K. Argyraki, and C. Fragouli* 1177

Specific Emitter Identification via Hilbert–Huang Transform in Single-Hop and Relaying Scenarios .... *J. Zhang, F. Wang, O. A. Dobre, and Z. Zhong* 1192

Fingerprint Liveness Detection Using Convolutional Neural Networks .... *R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado* 1206

(Contents Continued on Page 1090)

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (ISSN 1556-6013) is published monthly by the Institute of Electrical and Electronics Engineers, Inc. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society/Council, or its members. **IEEE Corporate Office:** 3 Park Avenue, 17th Floor, New York, NY 10016-5997. **IEEE Operations Center:** 445 Hoes Lane, Piscataway, NJ 08854-4141. **NJ Telephone:** +1 732 981 0060. **Price/Publication Information:** Individual copies: IEEE Members $20.00 (first copy only), nonmembers $339.00 per copy. (Note: Postage and handling charge not included.) Member and nonmember subscription prices available upon request. **Copyright and Reprint Permissions:** Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons, provided the per-copy fee of $31.00 is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For all other copying, reprint, or republication permission, write to Copyrights and Permissions Department, IEEE Publications Administration, 445 Hoes Lane, Piscataway, NJ 08854-4141. Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved. **Postmaster:** Send address changes to IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, 445 Hoes Lane, Piscataway, NJ 08854-4141. GST Registration No. 125634188. CPC Sales Agreement #40013087. Return undeliverable Canada addresses to: Pitney Bowes IMEX, P.O. Box 4332, Stanton Rd., Toronto, ON M5W 3J4, Canada. IEEE prohibits discrimination, harassment and bullying. For more information visit http://www.ieee.org/nondiscrimination. Printed in U.S.A.

(Contents Continued from Page 1089)

Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion .... *H. Salmani and M. M. Tehranipoor* 1214

One-Class Writer-Independent Offline Signature Verification Using Feature Dissimilarity Thresholding .... *A. Hamadene and Y. Chibani* 1226

Imperfect and Perfect Secrecy in Compound Multiple Access Channel With Confidential Message .... *H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, and M. R. Aref* 1239

ICCDetector: ICC-Based Malware Detection on Android .... *K. Xu, Y. Li, and R. H. Deng* 1252

An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing .... *S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie* 1265

Artificial-Noise-Aided Message Authentication Codes With Information-Theoretic Security .... *X. Wu, Z. Yang, C. Ling, and X.-G. Xia* 1278

Design, Evaluation, and Optimization of Physical Unclonable Functions Based on Transient Effect Ring Oscillators .... *A. Cherkaoui, L. Bossuet, and C. Marchand* 1291

MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers .... *R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra* 1306

A Dummy-Based Approach for Preserving Source Rate Privacy .... *A. Diyanat, A. Khonsari, and S. P. Shariatpanahi* 1321

A Game-Theoretic Framework for Optimum Decision Fusion in the Presence of Byzantines .... *A. Abrardo, M. Barni, K. Kallas, and B. Tondi* 1333

Private Cell Retrieval From Data Warehouses .... *X. Yi, R. Paulet, E. Bertino, and G. Xu* 1346

Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates .... *J. Yu, K. Ren, and C. Wang* 1362

EDICS—Editor's Information Classification Scheme 1376

Information for Authors 1377

ANNOUNCEMENTS

Call for Papers—IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS Special Issue on Distributed Information Processing in Social Networks 1379

Call for Papers—IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING Special Issue on Signal Processing and Machine Learning for Education and Human Learning at Scale 1380