

# **2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS 2018)**

**Salvador, Brazil  
2 – 5 October 2018**



**IEEE Catalog Number: CFP18059-POD  
ISBN: 978-1-5386-8302-6**

**Copyright © 2018 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:	CFP18059-POD
ISBN (Print-On-Demand):	978-1-5386-8302-6
ISBN (Online):	978-1-5386-8301-9
ISSN:	1060-9857

**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

# 2018 IEEE 37th International Symposium on Reliable Distributed Systems **SRDS 2018**

## Table of Contents

Message from the General Chair .....	x
Message from the Technical Program Co-Chairs .....	xi
Symposium Organization .....	xii
Technical Program Committee .....	xiv
Reviewers .....	xv
Acknowledgements .....	xvi

### Session 1. Attacks

Abusing CDNs for Fun and Profit: Security Issues in CDNs' Origin Validation .....	1
<i>Run Guo (Tsinghua University), Jianjun Chen (Tsinghua University), Baojun Liu (Tsinghua University), Jia Zhang (Tsinghua University), Chao Zhang (Tsinghua University), Haixin Duan (Tsinghua University, Tsinghua University-360 Enterprise Security Group Joint Research Center), Tao Wan (Huawei Canada), Jian Jiang (Shape Security), Shuang Hao (University of Texas, Dallas), and Yaoqi Jia (Zilliqa Research)</i>	
Impact of Man-In-The-Middle Attacks on Ethereum .....	11
<i>Parinya Ekparinya (University of Sydney, Australia), Vincent Gramoli (University of Sydney, Australia), and Guillaume Jourjon (Data61-CSIRO, Sydney, Australia)</i>	
US-AID: Unattended Scalable Attestation of IoT Devices .....	21
<i>Ahmad Ibrahim (TU Darmstadt), Ahmad-Reza Sadeghi (TU Darmstadt), and Gene Tsudik (University of California, Irvine)</i>	
A Scalable and Efficient Correlation Engine to Detect Multi-Step Attacks in Distributed Systems .....	31
<i>David Lanoe (CentraleSupélec, INRIA, IRISA), Michel Hurfin (INRIA, Univ Rennes, IRISA), and Eric Totel (CentraleSupélec, INRIA, IRISA)</i>	

### Session 2. Distributed Protocols

Practical Continuous Aggregation in Wireless Edge Environments .....	41
<i>Pedro Ákos Costa (NOVA LINES &amp; DI/FCT/NOVA University of Lisbon) and João Leitão (NOVA LINES &amp; DI/FCT/NOVA University of Lisbon)</i>	
Breaking the Scalability Barrier of Causal Broadcast for Large and Dynamic Systems .....	51
<i>Brice Nédelec (Université de Nantes, LS2N), Pascal Molli (Université de Nantes, LS2N), and Achour Mostéfaoui (Université de Nantes, LS2N)</i>	

Policy-Based Adaptation of a Byzantine Fault Tolerant Distributed Graph Database .....	61
<i>Manuel Bravo (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa), Luís Rodrigues (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa), Ray Neiheiser (DAS, INE, Federal University of Santa Catarina), and Luciana Rech (DAS, INE, Federal University of Santa Catarina)</i>	

## Session 3. Networks

Mobile Cloud-of-Clouds Storage Made Efficient: A Network Coding Based Approach .....	72
<i>Jiajie Shen (Fudan University), Yi Li (Fudan University), Yangfan Zhou (Fudan University), and Xin Wang (Fudan University)</i>	
Adversarially-Resistant On-Demand Topic Channels for Wireless Sensor Networks .....	83
<i>Hans Walter Behrens (Arizona State University) and K. Selçuk Candan (Arizona State University)</i>	
Secure Information Forwarding through Fragmentation in Delay-Tolerant Networks .....	93
<i>Shudip Datta (Missouri University of Science and Technology), Sanjay Madria (Missouri University of Science and Technology), James Milligan (AFRL, Rome, NY), and Mark Linderman (AFRL, Rome, NY)</i>	

## Session 4. Trusted Execution Environments

RATCHETA: Memory-Bounded Hybrid Byzantine Consensus for Cooperative Embedded Systems .....	103
<i>Wenbo Xu (Institute of Operating Systems and Computer Networks, TU Braunschweig) and Rüdiger Kapitza (Institute of Operating Systems and Computer Networks, TU Braunschweig)</i>	
MaskAI: Privacy Preserving Masked Reads Alignment using Intel SGX .....	113
<i>Christoph Lambert (SnT - University of Luxembourg), Maria Fernandes (SnT - University of Luxembourg), Jérémie Decouchant (SnT - University of Luxembourg), and Paulo Esteves-Verissimo (SnT - University of Luxembourg)</i>	
PubSub-SGX: Exploiting Trusted Execution Environments for Privacy-Preserving Publish/Subscribe Systems .....	123
<i>Sergei Arnautov (TU Dresden), Andrey Brito (Universidade Federal de Campina Grande), Pascal Felber (Université de Neuchâtel), Christof Fetzer (TU Dresden), Franz Gregor (TU Dresden), Robert Krahn (TU Dresden), Wojciech Ozga (TU Dresden), André Martin (TU Dresden), Valerio Schiavoni (Université de Neuchâtel), Fábio Silva (Universidade Federal de Campina Grande), Marcus Tenorio (Universidade Federal de Campina Grande), and Nikolaus Thümmel (TU Dresden)</i>	
Security, Performance and Energy Trade-Offs of Hardware-Assisted Memory Protection Mechanisms .....	133
<i>Christian Göttel (University of Neuchâtel), Rafael Pires (University of Neuchâtel), Isabelly Rocha (University of Neuchâtel), Sébastien Vaucher (University of Neuchâtel), Pascal Felber (University of Neuchâtel), Marcelo Pasin (University of Neuchâtel), and Valerio Schiavoni (University of Neuchâtel)</i>	

## Session 5. Fault-Tolerance

Mind the Gap: Autonomous Detection of Partitioned MANET Systems using Opportunistic Aggregation .....	143
<i>Simon Bouget (University of Rennes, Inria, CNRS, IRISA, France), Yérom-David Bromberg (University of Rennes, Inria, CNRS, IRISA, France), Hugues Mercier (University of Neuchâtel, Switzerland), Etienne Rivière (Université catholique de Louvain, Belgium), and François Taiani (University of Rennes, Inria, CNRS, IRISA, France)</i>	
DMap: A Fault-Tolerant and Scalable Distributed Data Structure .....	153
<i>Samuel Benz (Università della Svizzera Italiana (USI)) and Fernando Pedone (Università della Svizzera Italiana (USI))</i>	
Enabling State Estimation for Fault Identification in Water Distribution Systems Under Large Disasters .....	161
<i>Qing Han (University of California, Irvine), Ronald Eguchi (ImageCat Inc., CA, US), Sharad Mehrotra (University of California, Irvine), and Nalini Venkatasubramanian (University of California, Irvine)</i>	

## Session 6. Data Management and Storage

Improving Reliability of Deduplication-Based Storage Systems with Per-File Parity .....	171
<i>Suzhen Wu (Xiamen University), Huagao Luan (Xiamen University), Bo Mao (Xiamen University), Hong Jiang (University of Texas at Arlington), Gen Niu (Xiamen University), Hui Rao (Xiamen University), Fang Yu (Xiamen University), and Jindong Zhou (Xiamen University)</i>	
MuSE: Multimodal Searchable Encryption for Cloud Applications .....	181
<i>Bernardo Ferreira (DI, FCT, Universidade NOVA de Lisboa &amp; NOVA LINCS), João Leitão (DI, FCT, Universidade NOVA de Lisboa &amp; NOVA LINCS), and Henrique Domingos (DI, FCT, Universidade NOVA de Lisboa &amp; NOVA LINCS)</i>	
Héron: Taming Tail Latencies in Key-Value Stores Under Heterogeneous Workloads .....	191
<i>Vikas Jaiman (Université Grenoble Alpes, LIG; Université Catholique de Louvain), Sonia Ben Mokhtar (INSA Lyon, LIRIS, CNRS), Vivien Quéma (Université Grenoble Alpes, LIG; Grenoble, INP), Lydia Y. Chen (IBM Research – Zurich), and Etienne Rivière (Université Catholique de Louvain)</i>	

## Session 7. Blockchain and Verification - Short Papers

A Requirements-Driven Methodology for the Proper Selection and Configuration of Blockchains .....	201
<i>Mirko Staderini (University of Florence), Enrico Schiavone (University of Florence), and Andrea Bondavalli (University of Florence)</i>	
Crash-Resilient Decentralized Synchronous Runtime Verification .....	207
<i>Shokoufeh Kazemlou (McMaster University) and Borzoo Bonakdarpour (Iowa State University)</i>	
Decentralized Release of Self-Emerging Data using Smart Contracts .....	213
<i>Chao Li (University of Pittsburgh) and Balaji Palanisamy (University of Pittsburgh)</i>	

## Session 8. Consensus and State Machine Replication

Geographic State Machine Replication .....	221
<i>Paulo Coelho (Università della Svizzera italiana - Switzerland and Federal University of Uberlândia - Brazil) and Fernando Pedone (Università della Svizzera italiana - Switzerland)</i>	
Kernel Paxos .....	231
<i>Emanuele Giuseppe Esposito (Università della Svizzera italiana - Switzerland), Paulo Coelho (Università della Svizzera italiana - Switzerland and Federal University of Uberlândia - Brazil), and Fernando Pedone (Università della Svizzera italiana - Switzerland)</i>	
MDC-Cast: A Total-Order Broadcast Protocol for Multi-Datacenter Environments .....	241
<i>Mohamad-Jaafar Nehme (Université de Grenoble Alpes), Nicolas Palix (Université de Grenoble Alpes), Kamal Beydoun (Lebanese University), and Vivien Quema (Quéma - Grenoble INP)</i>	
Byzantine Agreement with Interval Validity .....	251
<i>Darya Melnyk (ETH Zurich) and Roger Wattenhofer (ETH Zurich)</i>	

## Posters and Abstracts

Dynamic Checkpoint Architecture for Reliability Improvement on Distributed Frameworks .....	261
<i>Paulo Vinicius Mendonça Cardoso (Federal University of Santa Maria) and Patrícia Pitthan de Araújo Barcelos (Federal University of Santa Maria)</i>	
Security, Performance and Energy Implications of Hardware-Assisted Memory Protection Mechanisms on Event-Based Streaming Systems .....	264
<i>Christian Göttel (University of Neuchâtel), Rafael Pires (University of Neuchâtel), Isabelly Rocha (University of Neuchâtel), Sébastien Vaucher (University of Neuchâtel), Pascal Felber (University of Neuchâtel), Marcelo Pasin (University of Neuchâtel), and Valerio Schiavoni (University of Neuchâtel)</i>	

## PhD Forum:

Collective Attestation: for a Stronger Security in Embedded Networks .....	267
<i>Ahmad Ibrahim (TU Darmstadt)</i>	
Towards Real-Time-Aware Intrusion Tolerance .....	269
<i>Christoph Lambert (University of Luxembourg), Marcus Völz (University of Luxembourg), Jérémie Decouchant (University of Luxembourg), and Paulo Esteves-Verissimo (University of Luxembourg)</i>	
Definition of an Architecture for Dynamic and Automatic Checkpoints on Apache Spark .....	271
<i>Paulo Vinicius Cardoso (Federal University of Santa Maria) and Patrícia Pitthan Barcelos (Federal University of Santa Maria)</i>	
Model-Driven Middleware to Support the Creation of Applications within Different Domains in Smart Cities .....	
<i>Paulo César Ferreira Melo (Universidade Federal de Goiás) and Fábio Moreira Costa (Universidade Federal de Goiás)</i>	

<b>Author Index</b> .....	<b>275</b>
---------------------------	------------