PROCEEDINGS OF SPIE

SPIDigitalLibrary.org/conference-proceedings-of-spie

Front Matter: Volume 6973

, "Front Matter: Volume 6973," Proc. SPIE 6973, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008, 697301 (19 March 2008); doi: 10.1117/12.795156

SPIE.

Event: SPIE Defense and Security Symposium, 2008, Orlando, Florida, United States

PROCEEDINGS OF SPIE

***Data Mining, Intrusion Detection,
Information Assurance, and
Data Networks Security 2008***

Belur V. Dasarathy
Editor

**17–18 March 2008
Orlando, Florida, USA**

Sponsored and Published by
SPIE

Volume 6973

Proceedings of SPIE, 0277-786X, v. 6973

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

The papers included 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. The papers published in these proceedings 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 this book:

Author(s), "Title of Paper," in *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008*, edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 6973 (SPIE, Bellingham, WA, 2008) Article CID Number.

ISSN 0277-786X

ISBN 9780819471642

Published by

SPIE

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

Telephone +1 360 676 3290 (Pacific Time) • Fax +1 360 647 1445

SPIE.org

Copyright © 2008, Society of Photo-Optical Instrumentation Engineers

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 copying fees. The Transactional Reporting Service base fee for this volume is \$18.00 per article (or portion thereof), which should be paid directly to the Copyright Clearance Center (CCC), 222 Rosewood Drive, Danvers, MA 01923. Payment may also be made electronically through CCC Online 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. The CCC fee code is 0277-786X/08/\$18.00.

Printed in the United States of America.

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

SPIE
Digital Library

SPIDigitalLibrary.org

Paper Numbering: Proceedings of SPIE follow an e-First publication model, with papers published first online and then in print and on CD-ROM. Papers are published as they are submitted and meet publication criteria. A unique, consistent, permanent citation identifier (CID) number is assigned to each article at the time of the first publication. Utilization of CIDs allows articles to be fully citable as soon they are published online, and connects the same identifier to all online, print, and electronic versions of the publication. SPIE uses a six-digit CID article numbering system in which:

- The first four 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. The complete citation is used on the first page, and an abbreviated version on subsequent pages. Numbers in the index correspond to the last two digits of the six-digit CID number.

Contents

vii	Conference Committee
ix	Introduction

SESSION 1 INFORMATION ASSURANCE AND SECURITY

6973 02	Integrated mandatory access control for digital data [6973-01] G. Hsieh, G. Patrick, K. Foster, G. Emamali, Norfolk State Univ. (USA); L. Marvel, Army Research Lab. (USA)
6973 03	Addressing security issues related to virtual institute distributed activities [6973-02] M. R. Stytz, Institute for Defense Analyses (USA); S. B. Banks, Calculated Insight (USA)
6973 04	An innovative middle tier design for protecting federal privacy act data [6973-03] T. G. L. Allen, AFRL/RVIS (USA)
6973 05	Mathematical model for security effectiveness figure of merit and its optimization [6973-04] S. V. Belur, J. Gloster, Van Dyke Technology Group (USA)
6973 06	Distributed intrusion detection system based on grid security model [6973-05] J. Su, Harbin Univ. of Science and Technology (China); Y. Liu, Beijing Univ. of Information and Technology (China)

SESSION 2 DATA MINING

6973 07	Is mining of knowledge possible? [6973-06] J. Brander, Interactive Engineering (Australia); A. Lupu, Scio Systems (USA)
6973 08	Application of data mining to medical risk management [6973-07] S. Tsumoto, Shimane Univ. (Japan); K. Matsuoka, Osaka Prefectural General Hospital (Japan); S. Yokoyama, Kodan Industry (Japan)
6973 09	A data mining approach to intelligent operations [6973-08] N. Memon, Aalborg Univ. (Denmark) and Hellenic American Univ. (Greece); D. L. Hicks, Aalborg Univ. (Denmark); N. Hakiolakis, Hellenic American Univ. (Greece)
6973 0A	The epidemic threshold theorem with social and contact heterogeneity [6973-09] D. Hincapié Palacio, Univ. de Antioquia (Colombia); J. Ospina Giraldo, EAFIT Univ. (Colombia); R. D. Gómez Arias, Univ. de Antioquia (Colombia)
6973 0B	Observational study of content of Hg in fog water relative to air pollution in suburbs of Nanjing [6973-10] L. Tang, S. Niu, S. Fan, X. Xu, S. Jin, J. Xu, Nanjing Univ. of Information Science and Technology (China)

SESSION 3 INTRUSION DETECTION

- 6973 0C **Intrusion signature creation via clustering anomalies** [6973-11]
G. R. Hendry, S. J. Yang, Rochester Institute of Technology (USA)
- 6973 0D **Securing MANETs with BITS!: danger theory and mission continuity** [6973-12]
M. Carvalho, Institute for Human and Machine Cognition (USA); R. Ford, W. Allen, G. Marin, Florida Institute of Technology (USA)
- 6973 0E **Virtual terrain: a security-based representation of a computer network** [6973-14]
J. Holsopple, CUBRC (USA); S. Yang, B. Argauer, Rochester Institute of Technology (USA)
- 6973 0F **VTAC: virtual terrain assisted impact assessment for cyber attacks** [6973-13]
B. J. Argauer, S. J. Yang, Rochester Institute of Technology (USA)
- 6973 0G **Usefulness of DARPA dataset for intrusion detection system evaluation** [6973-15]
C. Thomas, V. Sharma, N. Balakrishnan, Indian Institute of Science (India)

SESSION 4 MISCELLANEOUS TOPICS

- 6973 0H **Performance comparison of the automatic data reduction system (ADRS)** [6973-16]
D. Patterson, D. Turner, A. Concepcion, California State Univ., San Bernardino (USA); R. Lynch, Naval Undersea Warfare Ctr. (USA)
- 6973 0I **Two-beam coupling correlation synthetic aperture radar image recognition with power-law scattering centers pre-enhancement** [6973-17]
B. Haji-saeed, Solid State Scientific Corp. (USA); J. Khoury, C. L. Woods, Air Force Research Lab./SNHC (USA); J. Kierstead, Solid State Scientific Corp. (USA)
- 6973 0J **Adaptive Markov feature estimation and categorization using the projection-slice theorem** [6973-18]
V. R. Riasati, Boeing Satellite Systems (USA)

SESSION 5 MISCELLANEOUS APPLICATIONS

- 6973 0K **A new approach to chemical agent detection, classification, and estimation** [6973-20]
T. Qian, G. Chen, Intelligent Automation, Inc. (USA); E. Blasch, AFRL/Ryaa (USA); R. Lynch, Naval Undersea Warfare Ctr. (USA); Y. Qi, Goal Prospect Foreign Language School (China)
- 6973 0L **Using received signal strength variation for surveillance in residential areas** [6973-21]
S. Hussain, R. Peters, D. L. Silver, Acadia Univ. (Canada)
- 6973 0M **Power-law radon-transformed superimposed inverse filter synthetic discriminant correlator for facial recognition** [6973-22]
B. Haji-saeed, Solid State Scientific Corp. (USA); J. Khoury, C. L. Woods, Air Force Research Lab./SNHC (USA); J. Kierstead, Solid State Scientific Corp. (USA)
- 6973 0N **Improvement in minority attack detection with skewness in network traffic** [6973-23]
C. Thomas, N. Balakrishnan, IISc (India)

POSTER SESSION

- 6973 0O **An improved clone selection immune algorithm** [6973-24]
P. Qiao, T. Wang, J. Su, Harbin Univ. of Science and Technology (China)
- 6973 0P **An immunity-based model for dynamic distributed intrusion detection** [6973-25]
P. Qiao, T. Wang, J. Su, Harbin Univ. of Science and Technology (China)
- 6973 0Q **Research on parallel algorithm for sequential pattern mining** [6973-26]
L. Zhou, Capital Normal Univ. (China), Harbin Institute of Technology (China), and Harbin Univ. of Science and Technology (China); B. Qin, Y. Wang, Harbin Univ. of Science and Technology (China); Z. Hao, Harbin Institute of Technology (China), Harbin Univ. of Science and Technology (China), and Qiqihar Univ. (China)

Author Index

Conference Committee

Symposium Chair

Larry B. Stotts, Defense Advanced Research Projects Agency (USA)

Symposium Cochair

Ray O. Johnson, Lockheed Martin Corporation (USA)

Program Track Chair

Belur V. Dasarathy, Consultant, Information Fusion Technologies (USA)

Conference Chair

Belur V. Dasarathy, Consultant, Information Fusion Technologies (USA)

Program Committee

Thomas G. L. Allen, Air Force Research Laboratory (USA)

Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (USA)

Bahareh Haji-saeed, Solid State Scientific Corporation (USA)

Sajid Hussain, Acadia University (Canada)

Robert S. Lynch, Jr., Naval Undersea Warfare Center (USA)

Vahid R. Riasati, Boeing Satellite Systems (USA)

John J. Salerno, Jr., Air Force Research Laboratory (USA)

Martin R. Stytz, Institute for Defense Analyses (USA)

Shusaku Tsumoto, Shimane University (Japan)

Session Chairs

- 1 Information Assurance and Security
Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (USA)
Thomas G. L. Allen, Air Force Research Laboratory (USA)
- 2 Data Mining
Martin R. Stytz, Institute for Defense Analyses (USA)
Shusaku Tsumoto, Shimane University (Japan)
- 3 Intrusion Detection
John J. Salerno, Jr., Air Force Research Laboratory (USA)
Sajid Hussain, Acadia University (Canada)

- 4 Miscellaneous Topics
 Robert S. Lynch, Jr., Naval Undersea Warfare Center (USA)
 Vahid R. Riasati, Boeing Satellite Systems (USA)
- 5 Miscellaneous Applications
 Sajid Hussain, Acadia University (Canada)
 Bahareh Haji-saeed, Solid State Scientific Corporation (USA)

Introduction

With this offering, we are glad to announce that we have reached a significant milestone, namely a decade of our series on data mining knowledge discovery, which, incidentally, has expanded in scope over the years to acknowledge the dynamic nature of the information technology arena. The title was modified three years back to the current one: Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, to better reflect this expanded scope. We have thus far published nearly 350 papers under this series. As has been the practice, this conference is being presented along with the conference on Information Fusion under the common IT track. This is intended to recognize, exploit, and nurture the natural synergy between the two fields. The fact that the two conferences are run in sequence, rather than in parallel, facilitates cross participation between the two research groups. As per our long upheld principles, we have again worked hard to ensure that the printed proceedings are available on-site for both of these conferences. It is our sincere belief that this aids in better appreciation of the oral presentations and promotes rapid dissemination of the new developments in these areas. While this is not in conformity with the policy of post-conference proceedings publication followed by the majority of SPIE conferences, our aim is to minimize the risk of authors not showing up to make their promised presentations or making presentations that have not yet attained the necessary maturity or completeness by the time of the conference. This admittedly tends to reduce the number of presentations from the original expectations, which is not necessarily a negative since the average quality of the resulting presentations shows an improvement over what would be otherwise.

As has been the practice over the past few years, the variation in the size of these proceedings, in terms of the number of papers offered over the years, is illustrated in Figure 1. We have a slight increase over last year and hope this represents a turn around trend for the future. It is advisable for us in the program committee to keep emphasizing the intrusion detection and network security aspects and explore ways to reinvigorate the interest in this conference to ensure its sustainability within the SPIE context. Accordingly, ideas on how to further expand the appeal of this conference are hereby being actively sought by the organizers from the conference participants as well as the readership of these proceedings at large.

The conference has a total of 25 presentations this year. The papers published here in these proceedings are grouped into the following five regular sessions followed by a poster session that address miscellaneous issues.

- Information Assurance and Security
- Data Mining

- Intrusion Detection
- Miscellaneous Topics
- Miscellaneous Applications

As in prior years, the global span of the conference is reflected in the authorship of the papers which are from nine (a couple more than last year) different countries namely, Australia, Canada, China, Colombia, Denmark, Greece, India, Japan, and of course, USA.

Figure 1. Number of papers published over the years in this series

We hope to continue this series in the coming year and expect to see a growth based on the revamping the scope of the conference. All those interested in active participation in planning and conference program development process are requested to contact me at fusion_consultant@yahoo.com as early as possible, preferably during the course of the conference itself, in any case before March 31st, 2008. Further details regarding the call for papers and schedule for the next year will be made available in due course on the Internet at SPIE (<http://www.spie.org>) as well as my home page (<http://belur.no-ip.com>). We would like to take this opportunity to acknowledge the authors for letting us showcase their work and thereby contribute to the success of this conference. I also would like to express my thanks to the members of my program committee and the session chairs for their cooperation and support. Lastly, our thanks are

also due to the SPIE staff for their help in putting together the conference program and proceedings.

कायेन वाचा मनसेन्द्रियैर्वा
बुध्यात्मनावा प्रकृते स्वभावात्
करोमि यद्यत् सकलं परस्मै
श्रीमन्नारायणायेति समर्पयामि

"kaayena vaachaa manasendriyaiirvaa
budhyaatmanaavaa prakR^ite svabhaavaat
karomi yadyat sakalaM parasmai
shriiman naaraayaNaayeti samarpayaami"

Be it with my body, or with my mind
With words, or organs of any kind,
With my intellect, or with my soul,
Or by force of Nature pushing me to my goal,
Whatever it is, with all these I do,
Oh! Supreme Lord! I surrender to you.

Wishing you all a safe trip back home!

Belur V. Dasarathy
Fusion_consultant@yahoo.com
<http://belur.no-ip.com>