PROCEEDINGS OF SPIE

Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security 2009

Belur V. Dasarathy
Editor

15–16 April 2009
Orlando, Florida, United States

Sponsored and Published by
SPIE

Volume 7344

Proceedings of SPIE, 0277-786X, v. 7344

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 Security and Assurance, and Data Networks Security 2009*, edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 7344 (SPIE, Bellingham, WA, 2009) Article CID Number.

ISSN 0277-786X
ISBN 9780819476104

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

Printed in the United States of America.

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

SPIE
Digital Library

SPIEDigitalLibrary.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

SESSION 1 INTRUSION DETECTION AND NETWORK SECURITY I

SESSION 2 INTRUSION DETECTION AND NETWORK SECURITY II

SESSION 3 DATA MINING AND CLASSIFICATION I

SESSION 4 DATA MINING AND CLASSIFICATION II

SESSION 5 MISCELLANEOUS APPLICATIONS: ISSUES AND INNOVATIONS I

SESSION 6 MISCELLANEOUS APPLICATIONS: ISSUES AND INNOVATIONS II

POSTER SESSION

Conference Committee

Symposium Chair

Ray O. Johnson, Lockheed Martin Corporation (United States)

Symposium Cochair

Michael T. Eismann, Air Force Research Laboratory (United States)

Conference Chair

Belur V. Dasarathy, Consultant, Information Fusion Technologies (United States)

Program Committee

Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (United States)
Sajid Hussain, Acadia University (Canada)
Robert S. Lynch, Jr., Naval Undersea Warfare Center (United States)
Vahid R. Riasati, Boeing Satellite Systems (United States)
John J. Salerno, Jr., Air Force Research Laboratory (United States)
Martin R. Stytz, Institute for Defense Analyses (United States)
Shusaku Tsumoto, Shimane University (Japan)

Session Chairs

1 Intrusion Detection and Network Security I
Robert S. Lynch, Jr., Naval Undersea Warfare Center (United States)
Belur V. Dasarathy, Consultant, Information Fusion Technologies (United States)

2 Intrusion Detection and Network Security II
Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (United States)
Martin R. Stytz, Institute for Defense Analyses (United States)

3 Data Mining and Classification I
Sajid Hussain, Acadia University (Canada)
Vahid R. Riasati, Boeing Satellite Systems International, Inc. (United States)

4 Data Mining and Classification II
Shusaku Tsumoto, Shimane University (Japan)
Sajid Hussain, Acadia University (Canada)

5 Miscellaneous Applications I: Issues and Innovations
Vahid R. Riasati, Boeing Satellite Systems International, Inc. (United States)
John J. Salerno, Jr., Air Force Research Laboratory (United States)

6 Miscellaneous Applications II: Issues and Innovations
John J. Salerno, Jr., Air Force Research Laboratory (United States)
Shusaku Tsumoto, Shimane University (Japan)

Introduction

This is our eleventh offering in this ongoing series on various aspects of intrusion detection and network security and knowledge discovery through data mining. We have thus far published nearly 360 papers under this series. As always, this conference is being presented in conjunction with the conference on information fusion, both under an expanded information processing related track. This is intended to recognize, exploit, and nurture the natural synergy between the two fields. The two conferences are run in sequence, rather than in parallel, to facilitate cross participation between the two research groups. In accordance with our long held principles, we at SPIE 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. Admittedly, this is not in conformity with the policy of post-conference proceedings publication followed by the majority of SPIE sister conferences being held at Orlando under the Defense and Security Symposium. Our rationale has been 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 however occasionally 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.

In line with the practice over the past few years, the size of these proceedings and the pattern of its variations, in terms of the number of papers offered over the years, are illustrated in Figure 1. We have a slight decrease over last year, which given the current economic climate is neither surprising nor a matter of concern for the long term health of this conference. It is however 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 22 presentations this year. The papers published here in these proceedings are grouped into the following six regular sessions followed by a poster session that address miscellaneous issues.

- Intrusion Detection and Network Security I & II
- Data Mining and Classification I & II
- Miscellaneous Applications: Issues and Innovations I & II

As in prior years, the global span of the conference is reflected in the authorship of the papers which are from nine (quite a few new entrants as compared to previous years, some for the first time ever, replacing others) countries namely, Austria, Brazil, Canada, China, France, Japan, Mexico, Pakistan and of course, the United States.

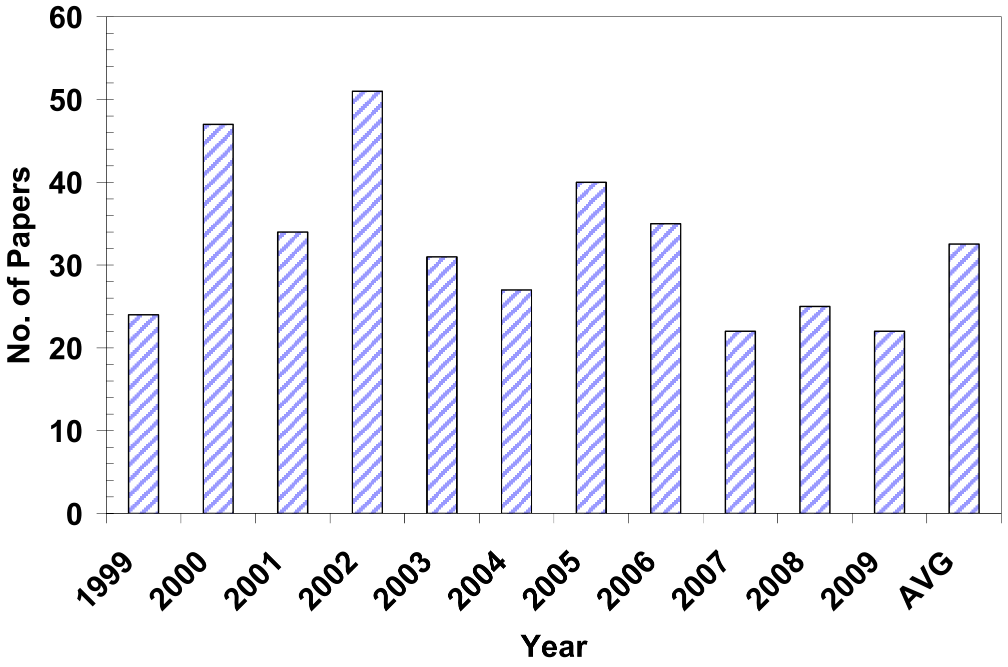

Figure 1. Number of papers published over the years in this series

We plan to continue this series in the coming year and hope to see a growth assuming that the global economy will have experienced a turn around by then. All those interested in active participation in planning and conference program development process are requested to contact me at fusion-consultant@ieee.org as early as possible, preferably during the course of the conference itself, in any case before April 30, 2009. 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 giving us the opportunity to publish their work leading 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 once again the conference program and proceedings in a timely fashion.

कायेन वाचा मनसेन्द्रियैर्वा
बुध्यात्मनावा प्रकृते स्वभावात
करोमि यद्यत सकलं परस्मै
श्रीमन्नारायणायेति समर्पयामि

"kaayena vaachaa manasendriyairvaa
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@ieee.org
http://belur.no-ip.com