PROCEEDINGS OF SPIE

Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2007

Belur V. Dasarathy
Editor

10 April 2007
Orlando, Florida, USA

Sponsored and Published by
SPIE—The International Society for Optical Engineering

Volume 6570

The International Society for Optical Engineering

Proceedings of SPIE—The International Society for Optical Engineering, 9780819466921, v. 6570

SPIE is an international technical society dedicated to advancing engineering and scientific applications of optical, photonic, imaging, electronic, and optoelectronic technologies.

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 2007*, edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 6570 (SPIE, Bellingham, WA, 2007) Article CID Number.

ISSN 0277-786X
ISBN 9780819466921

Published by
SPIE—The International Society for Optical Engineering
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone 1 360/676-3290 (Pacific Time) · Fax 1 360/647-1445
http://www.spie.org

Printed in the United States of America.

Contents

Pagination: 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.

SESSION 2 DATA MINING

SESSION 3 APPLICATIONS

SESSION 4 MISCELLANEOUS METHODS, TOPICS, AND ISSUES

POSTER SESSION

Conference Committee

Symposium Chair

John C. Carrano, Luminex Corporation (USA)

Symposium Cochair

Larry B. Stotts, DARPA (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)
Sheila B. Banks, Calculated Insight (USA)
Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (USA)
Robert S. Lynch, Jr., Naval Undersea Warfare Center (USA)
Martin R. Stytz, Institute for Defense Analyses (USA)
Shusaku Tsumoto, Shimane University (Japan)
JingTao Yao, University of Regina (Canada)

Session Chairs

1 Intrusion/Intruder Detection
Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (USA)
Belur V. Dasarathy, Consultant, Information Fusion Technologies (USA)

2 Data Mining
Robert S. Lynch, Jr., Naval Undersea Warfare Center (USA)
Thomas G. L. Allen, Air Force Research Laboratory (USA)

3 Applications
Jonathan A. Gloster, The Van Dyke Technology Group, Inc. (USA)
John J. Salerno, Jr., Air Force Research Laboratory (USA)

4 Miscellaneous Methods, Topics, and Issues
Martin R. Stytz, Institute for Defense Analyses (USA)
Shusaku Tsumoto, Shimane University (Japan)

Introduction

This is the ninth offering in our series on data mining and knowledge discovery, which has been evolving over the years and has been expanded in terms of its scope giving recognition to the dynamic nature of the information technology arena. The title was revised two 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 over 300 papers under this series. As in prior years, 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 has been our practice from the very beginning, we have pushed hard to ensure that the printed proceedings are available on-site for both of these conferences. This aids in better appreciation of the oral presentations and promotes rapid dissemination of the new developments in these areas. Admittedly, this is in contrast to the policy of post-conference proceedings publication followed by the majority of SPIE conferences. This minimizes 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 is evident from the fact that initially we had 30 abstract submissions accepted and has since whittled down by about 30% through filtering brought on by the stringent qualifying requirements of the on-site proceedings publication process.

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 regret to note that there has been a significant downturn as compared to past few years perhaps due to growing number of conferences around the world that are wholly dedicated to data mining. It is necessary for us to emphasize the intrusion detection and network security aspects in the future and find 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 seven regular sessions followed by a poster session that address miscellaneous issues.

- Intrusion/Intruder Detection
- Data Mining
- Applications
- Miscellaneous Topics

As in prior years, the global span of the conference is reflected in the authorship of the papers which are from seven different countries namely, Brazil, Canada, China, India, Japan, U.K., and of course, the USA. This has noticeably contracted in recent years by the international travel climate, both in terms of economics as well as visa issues and indeed is the main cause for the downturn in the total number of papers.

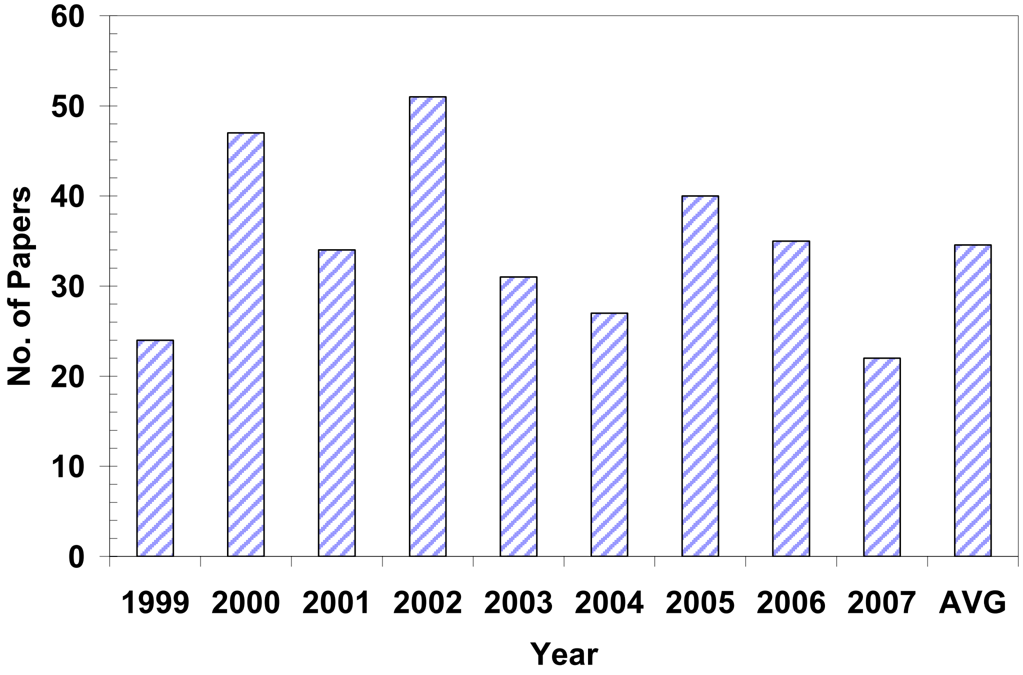

Figure 1. Number of papers published over the years in this series

We plan on continuing this series in the coming year and hope to see a growth through 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 before April 30th, 2007. 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). I 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, thanks are also due to the SPIE staff for their help in putting together the conference program and proceedings.

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@yahoo.com
http://belur.no-ip.com